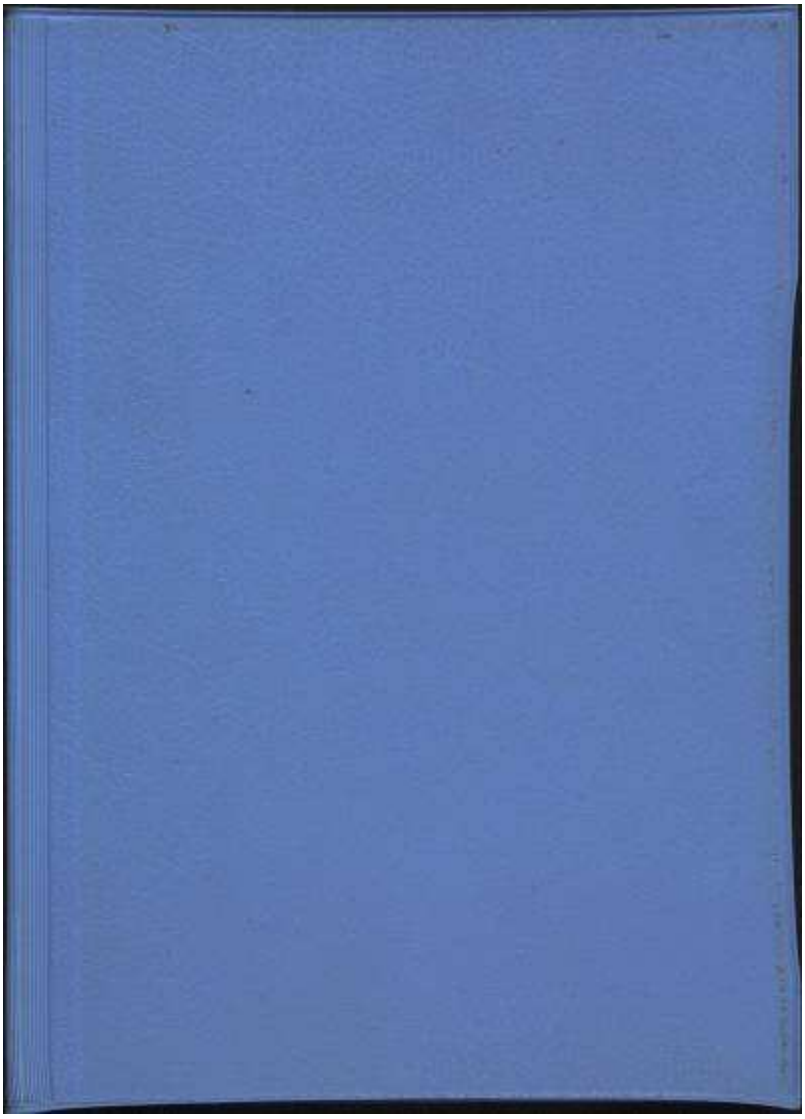


Zentrales Chiffrierorgan der DDR

Vertrauliche Verschlußsache!

VVS – ZCO/407/71

Ausfertigung 0300 *

62 Blatt

Fachbegriffe des Chiffrierwesens

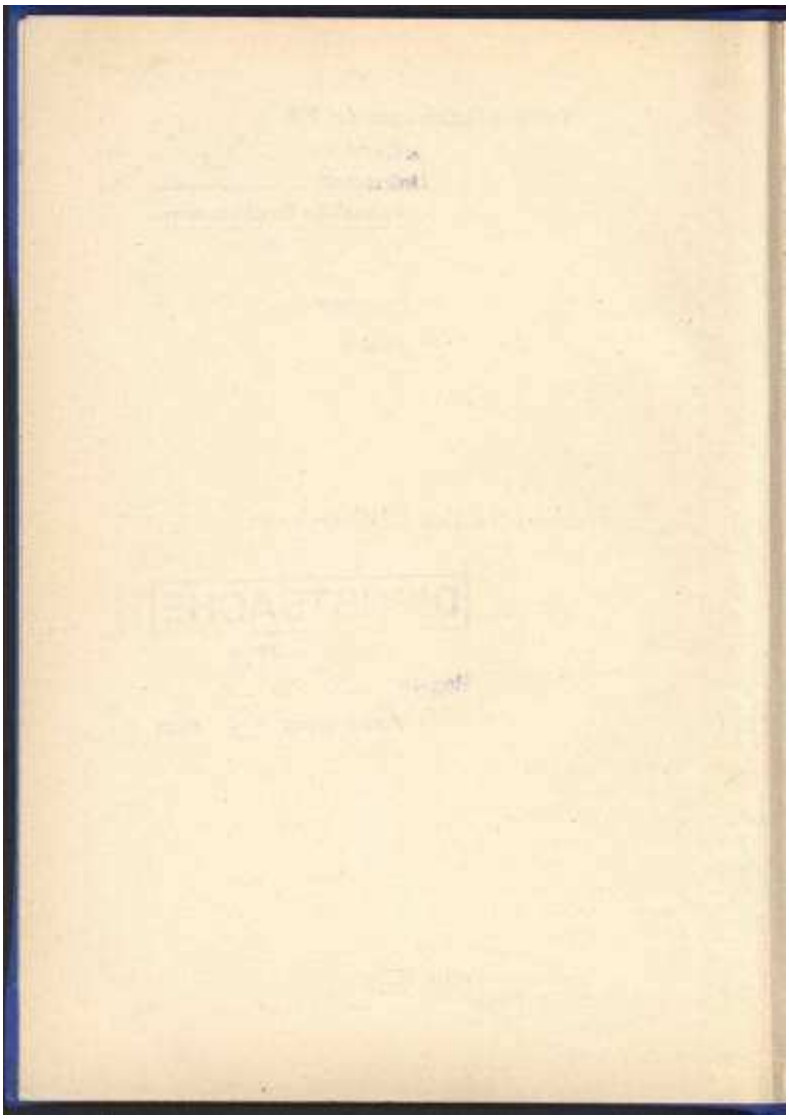
DIENSTSACHE

nachweispflichtig

Reg.-Nr. _____

Ausfertigung ___ Blatt

Berlin 1971



Inhaltsverzeichnis

Vorwort

Die Notwendigkeit einer einheitlichen, wissenschaftlich begründeten Terminologie für das Chiffrierwesen ist unbestreitbar. Die Verwendung uneinheitlicher, unklarer Fachbegriffe erschwert die gegenseitige Verständigung und die Zusammenarbeit sowohl innerhalb der DDR als auch mit anderen sozialistischen Ländern. Die Folgen sind Zeitverlust durch unnötige Auseinandersetzungen oder Unverständnis und Unterlassung notwendiger Handlungen oder sogar Mißverständnisse und Auslösung falscher Handlungen. Eine uneinheitliche Terminologie behindert auch die weitere Rationalisierung der Information und Produktion beispielsweise durch Einsatz der elektronischen Datenverarbeitung oder durch Massenfertigung einheitlicher Unterlagen anstelle verschiedener Fassungen.

Die ungerechtfertigte Verwendung bereichsinterner Fachbegriffe steht im Widerspruch zu der objektiv begründeten Forderung nach einer einheitlichen Terminologie. Unter bereichsinternen Fachbegriffen sind solche Begriffe zu verstehen, für deren Inhalt in einem bestimmten Bereich (d. h. einem Ministerium, einer Verwaltung, Abteilung oder sonstigen staatlichen oder gesellschaftlichen Institution oder Organisation) eine andere Begriffsbenennung (ein anderer Terminus) verwendet wird oder dessen Begriffsbenennung eine andere Bedeutung zugrunde gelegt ist als in anderen Bereichen. Bereichsinterne Fachbegriffe sind nur gerechtfertigt, sofern es sich um die Bezeichnung von bereichsinternen, d. h. nur in diesem Bereich vorkommenden Einrichtungen, Dienststellungen, Sachverhalten und dergleichen handelt oder wenn durch die Bezeichnung der wahre Sachverhalt gegenüber Außenstehenden verschleiert werden soll, die Bezeichnung also eine Deckbezeichnung ist.

Bereichsinterne Fachbegriffe sind zählebig. Entstanden durch Eigenschöpfung oder allzu wörtliche Übersetzung aus einer Fremdsprache in Unkenntnis des deutschen Fachausdruckes oder wegen tatsächlichen Fehlens eines solchen, finden sie in Dokumenten ihren Niederschlag und werden dadurch verbreitet und eingebürgert. Es empfiehlt sich, bei ihrer Ausmerzung so vorzugehen, daß in neu zu erarbeitenden oder zu überarbeitenden Dokumenten die einheitlichen Begriffe benutzt und ihnen die bisher gebräuchlichen bereichsinternen Begriffe in einer Übersicht oder in Klammern gegenübergestellt werden, bis sämtliche einschlägigen Dokumente überarbeitet sind. Dieser Prozeß kann sich über längere Zeit hinziehen.

Vorliegende „Fachbegriffe des Chiffrierwesens" stellen eine von Grund auf überarbeitete und wesentlich erweiterte Neufassung der im Jahre 1967 herausgegebenen „Grundbegriffe der Kryptologie" dar. Sie sollen als Grundlage für die Durchsetzung und Einhaltung einer exakten und einheitlichen Terminologie im Chiffrierwesen der DDR und als Hilfsmittel bei der Erarbeitung und dem Studium von Dokumenten des Chiffrierwesens, bei der Anleitung und Schulung von Mitarbeitern des Chiffrierwesens und bei der Abstimmung der Terminologie des Chiffrierwesens mit anderen sozialistischen Ländern dienen.

Aufgenommen wurden in erster Linie Fachbegriffe der Kryptologie und des Chiffrierwesens, die in gültigen Dokumenten und in der Praxis des Chiffrierwesens öfter verwendet werden oder zu deren besserem Verständnis beitragen können. Ferner wurde eine Anzahl solcher Begriffe aus Nachbargebieten aufgenommen, die im Chiffrierwesen öfter gebraucht werden und deren Kenntnis nicht allgemein vorausgesetzt werden kann. Synonyme wurden nur sparsam aufgenommen.

Nicht aufgenommen wurden im allgemeinen bereichsinterne Begriffe, ferner Begriffe, die in der gleichen Weise zu verstehen sind, wie sie in allgemein zugänglichen Nachschlagewerken (Duden, Meyer, Fremdwörterbuch) definiert sind sowie zusammengesetzte Begriffe, die keiner weiteren Definition bedürfen, weil ihre Bestandteile ausreichend definiert sind. Z. B. wurde „manuelles Schlüsselverfahren" nicht aufgenommen, da sein Begriffsinhalt von den Definitionen für „manuelles Verfahren" und „Schlüsselverfahren" unmißverständlich abgeleitet werden kann.

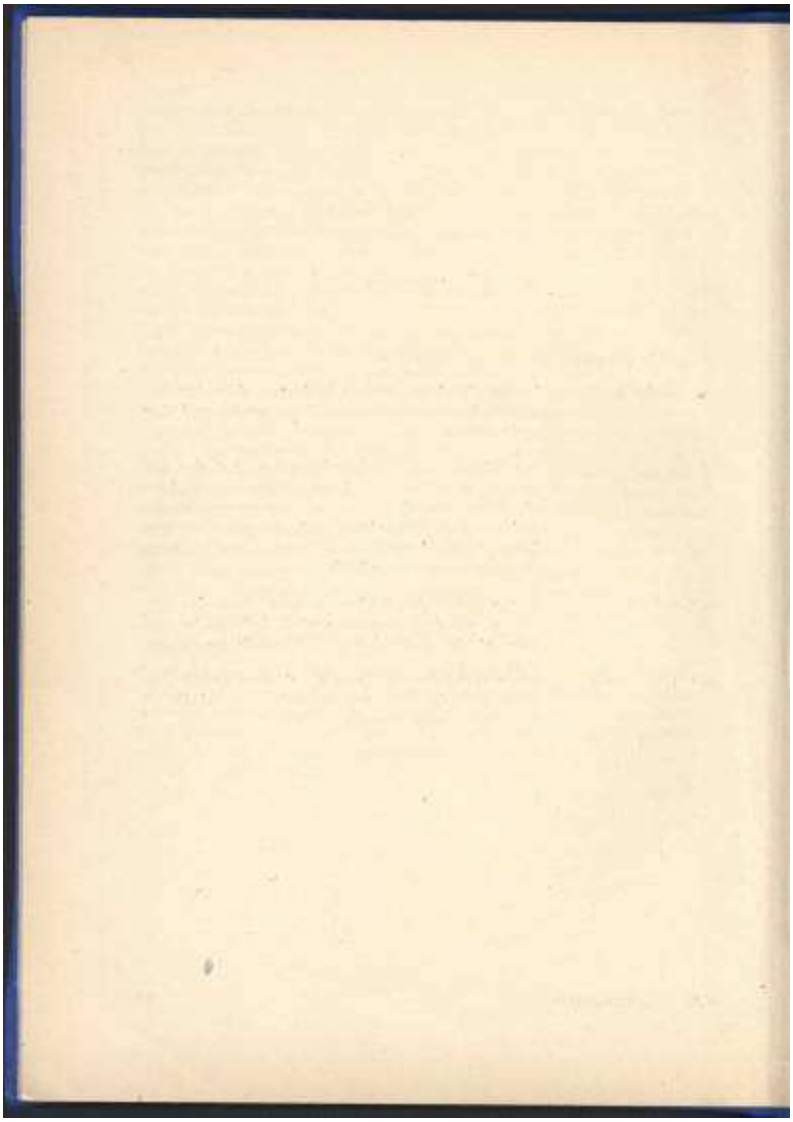
Die Terminologie des Chiffrierwesens befindet sich ebenso wie die anderer Gebiete in ständiger Entwicklung. Neue Begriffe entstehen, andere veralten oder ändern sich. Das Prinzip der Einheitlichkeit bleibt davon unberührt.

Es ist vorgesehen, zu den „Fachbegriffen des Chiffrierwesens" von Zeit zu Zeit Ergänzungen und bei Notwendigkeit eine Neufassung herauszugeben. Alle Benutzer sind aufgefordert, Hinweise für Ergänzungen, Änderungen und sonstige Verbesserungen laufend über ihre Zentralen und Leitstellen an das ZCO einzureichen.

Erläuterungen

Folgende Verweisformen werden verwendet:

+ („siehe")	innerhalb eines Artikels bedeutet, daß das folgende Wort selbständiges Stichwort ist und dort definiert ist.
+	am Schluß eines Artikels bedeutet, daß das folgende Wort selbständiges Stichwort ist bzw. die folgenden durch Komma getrennten Wörter selbständige Stichwörter sind, die mit dem hier behandelten Begriff in Beziehung stehen oder den Gegensatz dazu bilden.
s. („siehe")	verweist auf das Stichwort, unter dem der Terminus, von dem verwiesen wird, definiert ist und zum leichten Auffinden in VERSALIEN gesetzt ist.
svw. („soviel wie")	verweist auf den Terminus mit gleicher Bedeutung, unter dem die Definition zu finden ist und der im Sprachgebrauch vorzuziehen ist.



Alphabetisches Begriffsverzeichnis

abgesetzter Fernschreiber
Fernschreiber für eine Direktchiffrierverbindung, der sich außerhalb der Kontrollzone des Chiffriergerätes befindet.

abgewandeltes Alphabet
Alphabet, das aus einem vorgegebenen Alphabet durch Hinzufügung und / oder Weglassung mindestens eines Zeichens entsteht. Wenn nichts anderes angegeben, gilt das + Normalalphabet als vorgegebenes Alphabet.
+ erweitertes Alphabet, reduziertes Alphabet.

abhörsichere Leitung svw. gesicherte Leitung

Abschnittsmarkierung
Kennzeichnung eines Schlüssellochstreifenabschnittes, z. B. durch ABSCHNITTSNUMMER (lfd. Nummer des Abschnittes innerhalb des Schlüssellochstreifens) und EINLEGEMARKIERUNG (ein Symbol, das eindeutig bestimmt, wie der Abschnitt in das Gerät einzulegen ist).

Abschnittsnummer s. Abschnittsmarkierung

absendende Chiffrierstelle
Chiffrierstelle, von der ein Geheimtext ausgeht.

Absender
Person oder Stelle, die eine Nachricht verfaßt bzw. verfassen läßt und für diese verantwortlich zeichnet.

absolut irreguläre Folge
Durch wiederholte Realisierung eines Experiments mit zufälligen Ausgängen (z. B. Würfeln) entstandene Folge endlicher Länge, wobei die Realisierungen unabhängig voneinander erfolgen und die verschiedenen Ausgänge gleichwahrscheinlich sind.
+ irreguläre Folge.

absolute Frequenz svw. Frequenz

absolute Sicherheit s. Sicherheit

Abstrahlung
Emission elektromagnetischer, akustischer oder anderer Wellen.
Bei Chiffriergeräten und anderer Chiffriertechnik, Fernschreibern, Schreibmaschinen usw. tritt die Abstrahlung als unerwünschter, für die Dekryptierung nutzbarer Nebeneffekt auf.

Additionsbereich
Menge der voneinander verschiedenen Additionseinheiten, die für ein bestimmtes Additionsverfahren zugelassen sind.

Additionseinheit
Einheit der Additionsreihe.

Additionselement
Element der Additionsreihe.

Additionselementebereich
Menge der voneinander verschiedenen Additionselemente, die für ein bestimmtes Additionsverfahren zugelassen sind.

Additionsfolge
Folge von Additionselementen.

Additionsgruppe
Gruppe von Additionselementen.
+ Einsatzgruppe.

Additionsreihe
Substitutionsreihe, die zur Chiffrierung mittels + kryptographischer Addition dient.
Die Additionsreihen werden eingeteilt:
(1) nach ihrer kryptologischen Beschaffenheit in + reguläre Additionsreihen und + irreguläre Additionsreihen;
(2) nach der Art der Additionselemente in + Buchstabenadditionsreihen, + Ziffernadditionsreihen und + Zeichenadditionsreihen, unabhängig von der Gestalt der verwendeten Elemente (Zeichen), z. B. als Druckzeichen, Lochkombinationen oder Impulsfolgen (Schrittgruppen).

Additionstafel
Hilfsmittel in Tafelform zur Durchführung der kryptographischen Addition.

Additionsverfahren
Spaltenverfahren, bei dem die Substitutionsreihe als Additionsreihe benutzt wird.
Die Additionsverfahren werden eingeteilt:
(1) nach der kryptologischen Beschaffenheit der angewandten Additionsreihen in + reguläre Additionsverfahren und + irreguläre Additionsverfahren;
(2) nach der Art der verwendeten Additionselemente in + Buchstabenadditionsverfahren, + Ziffernadditionsverfahren und + Zeichenadditionsverfahren.

allgemeiner Verkehr
Chiffrierverkehr zwischen mehr als zwei Korrespondenten, wobei jeder Korrespondent gegenüber jedem anderen sowohl Absender als auch Empfänger sein kann.

Alphabet
1. Im allgemeinen Sprachgebrauch: Gesamtheit der Buchstaben eines Schriftsystems in einer bestimmten Anordnung.
+ Normalalphabet.
2. In der Kryptologie: Die Zeichen eines endlichen Zeichenbereiches in bestimmter Reihenfolge.
Die Anzahl der Zeichen wird als LÄNGE des Alphabetes bezeichnet. Die Stellenzahl eines Zeichens im Alphabet wird als dessen RANG bezeichnet. Von zwei Zeichen eines Alphabetes ist dasjenige ALPHABETISCH NIEDRIGER, das den niedrigeren Rang hat. Die Differenz der Ränge zweier Zeichen ist deren DIREKTES INTERVALL.
Spezielle Alphabete sind: + Buchstabenalphabete, + Ziffernalphabete, + Buchstaben-Ziffern-Alphabete und + Zeichenalphabete.
Die von einem vorgegebenen Alphabet abgeleiteten Alphabete werden unterschieden nach der Anordnung der Zeichen in + Standardalphabete und + Mischalphabete, nach der Abwandlung des Zeichenbereiches in + vollständige, + erweiterte, + reduzierte und + abgewandelte Alphabete, nach den Gesetzmäßigkeiten der Ableitung in + Dezimationsalphabete, + Primalphabete u. a.
+ reziproke Alphabete.

alphabetisch niedriger s. Alphabet

alphanumerische Daten s. Daten

Analyse eines Chiffrierverfahrens
Untersuchung und Einschätzung des Wertes eines Chiffrierverfahrens. Die Analyse kann sich auf alle möglichen oder auch nur bestimmte Anwendungsbedingungen und Gütefaktoren erstrecken. Sie kann auch im Hinblick auf die Eignung eines Verfahrens für einen bestimmten Anwendungsbereich durchgeführt werden.

Antifunkgegenwirkung
Teil des Funkkrieges, der auf den Schutz der eigenen Funkmittel und Funksendungen vor der gegnerischen Funkgegenwirkung gerichtet ist.
+ Funktarnung, Funktäuschung.

Anwendungsbedingungen
Gesamtheit der Gegebenheiten und Anforderungen, die bei der Auswahl eines Chiffrierverfahrens oder -mittels für einen bestimmten An-

wendungsbereich und seiner Anwendung in diesem zu beachten sind. Dazu gehören: Beschaffenheit der Nachrichten, Nachrichtendichte, Nachrichtenmittel, Übermittlungsbedingungen, Anzahl der Korrespondenten, Verkehrsart, Arbeitsbedingungen, Qualifikation und Verläßlichkeit der Chiffreure, Aufbewahrungs- und Transportbedingungen, Güteanforderungen an das Verfahren oder Mittel u. a.
Die Anforderungen, die an das Verfahren oder Mittel gestellt werden, können in einer PFLICHTENFESTLEGUNG zusammengefaßt werden.

Anwendungsbereich
Organisatorisch, territorial oder nach sonstigen Gesichtspunkten abgegrenztes Gebiet, in dem ein bestimmtes Chiffrierverfahren oder -mittel angewandt wird. Anwendungsbereiche können z. B. sein: Staaten, staatliche oder gesellschaftliche Organe und Einrichtungen, VVB oder Betriebe, Wirtschaftszweige, Waffengattungen usw.

Anwendungsvorschriften
Gesamtheit der Vorschriften, die die Anwendung von Chiffrierverfahren und -mitteln regeln.
Dazu gehören allgemeine Vorschriften über den Umgang mit Verfahren und Mitteln (Einsichtnahmeberechtigung, Nachweisführung, Aufbewahrung, Transport u. a.), + Gebrauchsanweisungen zu bestimmten Verfahren und Mitteln, + Bedienungsanweisungen zu bestimmten Chiffriergeräten, + Sicherheitsbestimmungen.

äquivalente Schlüssel
Zwei Schlüssel heißen äquivalent, wenn sie bei Anwendung auf einen beliebigen Grundtext jeweils den gleichen Geheimtext ergeben.

Arbeitsart
Art der Texteingabe oder -ausgabe bei Chiffriergeräten, z. B. manuelle oder automatische Eingabe bzw. Ausgabe auf Blatt oder Lochstreifen. + Betriebsart.

Arbeitsfeld s. Gitter

Aufdruckmarkierung
Aufgedruckte Kennzeichnung eines Schlüssellochstreifens (+ Streifenmarkierung) oder Schlüssellochstreifenabschnittes (+ Abschnittsmarkierung).

Ausbildungsnormen
Festlegung von Leistungen und Fähigkeiten, nach deren Erreichung die Ausbildung in der Anwendung bestimmter Verfahren und Mittel

sowie des Telegramm- und Codestiles als abgeschlossen betrachtet wird.
+ Übungsnormen.

Ausgangseinheit s. Substitution

Ausgangsheft s. Schlüsselheft

Ausgangskassette s. Schlüsselkassette

Ausgangspunkt s. Stoßlinienverfahren

Baud s. Telegrafiergeschwindigkeit

Bedienungsanleitung
Umfassende Beschreibung der Bedienungselemente und Bedienungsmöglichkeiten zu einem Gerät oder einer Vorrichtung, z. B. einem Chiffriergerät oder einer Chiffriervorrichtung.
+ Bedienungsanweisung.

Bedienungsanweisung
Anweisung über die Reihenfolge der Arbeitsgänge bei der Bedienung eines Gerätes oder einer Vorrichtung für einen speziellen Zweck, z. B. eines Chiffriergerätes im Rahmen eines bestimmten Chiffrierverfahrens.
+ Bedienungsanleitung.

Behelfsverfahren
Chiffrierverfahren, das behelfsmäßig oder provisorisch wegen Fehlens eines vollwertigen Chiffrierverfahrens angewandt wird.

Belegung
Anzahl der in einer Substitution einer Ausgangseinheit zugeordneten Ersatzeinheiten.
Eine Ausgangseinheit, der nur eine Ersatzeinheit zugeordnet ist, ist einfach belegt, es liegt EINFACHBELEGUNG vor; sind einer Ausgangseinheit zwei oder mehr Ersatzeinheiten zugeordnet, so liegt MEHRFACHBELEGUNG (Zweifach-, Dreifachbelegung usw.) vor.
Eine durchweg gleiche Belegung wird als HOMOGENE BELEGUNG, eine unterschiedliche als INHOMOGENE BELEGUNG bezeichnet.

Bereich
1. svw. Anwendungsbereich.
2. In Zusammensetzungen wie Elementebereich, Codegruppenbereich usw. svw. Menge.

+ Schlüsselbereich.

Betriebsart
Art der Textbearbeitung durch ein Chiffriergerät, z. B. Chiffrierung oder Dechiffrierung, Vorchiffrierung oder Direktchiffrierung.
+ Arbeitsart.

Bevollmächtigtenstelle
Nachgeordnete Stelle einer + Leitstelle, die mit bestimmten Aufgaben wie z. B. Nachweisführung und Ausgabe von Chiffriermitteln für einen Teilbereich beauftragt ist.

bidifferenter Codegruppenbereich
Codegruppenbereich, bei dem sich alle Codegruppen untereinander an mindestens zwei Stellen unterscheiden.

bidifferent-tauschfreier Codegruppenbereich
Codegruppenbereich, bei dem sich alle Codegruppen untereinander an mindestens zwei Stellen unterscheiden und keine Codegruppe durch Vertauschung zweier benachbarter Elemente in eine andere übergeht.

Bigramm s. Polygramm

Bildchiffriergerät
Chiffriergerät, das für die Chiffrierung stehender Bilder (Fotografien, Dokumente usw.) ausgelegt ist.
+ Faksimilechiffriergerät.

Bildchiffrierung
Maschinelle Chiffrierung stehender Bilder.

Bildchiffrierverfahren
Maschinelles Verfahren zur Chiffrierung stehender Bilder.

Bildtelegrafie
Übertragung von Bildern mit Halbtönen (Bildtelegrafie im engeren Sinne) oder von Schwarz-Weiß-Vorlagen (FAKSIMILETELEGRAFIE) über Kanäle.

Binärcode
Code, dessen Codeelemente Binärzeichen sind.

Binärzeichen
Jedes der Zeichen aus einem Bereich von zwei Zeichen, z. B. 0 und 1.

Blankocode
Code, in dem die Codegruppen, aber noch keine Phrasen eingetragen sind.
+ Phrasencode, Blankotafel.

Blankotafel
Codetafel, in die noch keine Phrasen eingetragen sind.

Blender
Element ohne Informationsgehalt, das zur Erhöhung der Sicherheit eines Verfahrens oder zur Täuschung des Gegners in den Text eingefügt wird.
+ Füllelement.

Blendspruch
Spruch ohne Informationsgehalt, der zur Erhöhung der Sicherheit eines Verfahrens oder zur Täuschung des Gegners abgesetzt wird.

Branchencode
Wirtschaftscode, der im Nachrichtenverkehr eines bestimmten Wirtschaftszweiges angewandt wird.

Briefverfahren
Gedecktes Verfahren, bei dem der Geheimtext in einen unverfänglichen schriftlichen Klartext, z. B. einen Brief, eingebaut wird.
Zu den Briefverfahren gehören die + Kennzeichnungsverfahren und die + Einbauverfahren.

Buchstabe s. Zeichen

Buchstabenadditionsreihe
Additionsreihe, die nur aus Buchstaben besteht.

Buchstabenadditionsverfahren
Additionsverfahren, bei dem eine Buchstabenadditionsreihe verwendet wird.

Buchstabenalphabet
Alphabet, dessen Zeichen ausschließlich Buchstaben sind.

Buchstabencode
Code, dessen Codeelemente ausschließlich Buchstaben sind.

Buchstabengruppe s. Gruppe

Buchstabentext s. Text

Buchstabenverfahren
Chiffrierverfahren, dessen Geheimelemente ausschließlich Buchstaben sind.

Buchstabenwurmverfahren
Wurmverfahren, bei dem eine Buchstabenadditionsreihe verwendet wird.

Buchstaben-Ziffern-Alphabet
Alphabet, dessen Zeichen Buchstaben und Ziffern sind.

Buchstabiersignal
Indikator, der den Anfang oder das Ende einer Buchstabierung anzeigt.

Buchstabiertafel
Codetafel, die als Klareinheiten im wesentlichen Buchstaben enthält, und zur Verschleierung von Namen und anderen buchstabenweise zu codierenden Textteilen dient.

Buchstabier- und Zahlentafel
Codetafel, die aus der Kombination einer Buchstabiertafel und einer Zahlentafel besteht.

Buchtextverfahren
Unperiodisches Additionsverfahren, bei dem die Additionsreihe aus einem in offener Sprache abgefaßten Text abgeleitet wird.

charakteristisches Polygramm s. Parallelstelle

chemisches Geheimschreibverfahren svw. Geheimschreibverfahren 1

Chiffrator
Baugruppe eines Chiffriergerätes, in der die Chiffrierung oder je nach Wahl die Chiffrierung oder Dechiffrierung realisiert wird.

Chiffre
1. svw. Chiffrierverfahren
2. svw. Geheimeinheit
3. svw. Chiffriermittel

Chiffrealphabet
Die Chiffreelemente eines Chiffreelementebereiches in bestimmter Reihenfolge.

Chiffrebereich
Menge der voneinander verschiedenen Chiffreeinheiten, die für ein Chiffreverfahren zugelassen sind.

Chiffreeinheit
Geheimeinheit bei Chiffreverfahren.

Chiffreelement
Element eines Chiffretextes.

Chiffreelementebereich
Menge der voneinander verschiedenen Chiffreelemente, die für ein Chiffreverfahren zugelassen sind.

Chiffreelementevorrat
Anzahl der Chiffreelemente eines Chiffreelementebereiches.

Chiffrefolge
Folge von Chiffreelementen.

Chiffrekomponente s. Substitution

Chiffremischtext
Geheimtext, der aus Chiffreeinheiten verschiedener Chiffreverfahren besteht.

Chiffremittel
Chiffriermittel zu Chiffreverfahren.
+ Codemittel.

Chiffretelegramm
Chiffriertes Telegramm, auch der einem chiffrierten oder zu chiffrierenden Telegramm zugrundeliegende Klartext.

Chiffretext
Geheimtext, der durch Anwendung eines Chiffreverfahrens entstanden ist.
+ Chiffremischtext.

Chiffretextlochstreifen
Lochstreifen, der Chiffretext in Form von Lochkombinationen enthält.

Chiffreur
Person, die chiffriert und dechiffriert.
Speziell: Mitarbeiter des Chiffrierdienstes, der mit der Chiffrierung und Dechiffrierung beauftragt ist.

Chiffreurmechaniker
Person, die zugleich als Chiffreur und als Chiffriermechaniker ausgebildet und tätig ist.

Chiffreverfahren
Chiffrierverfahren, bei dem die Grundeinheiten im wesentlichen von gleicher Länge und Beschaffenheit sind und keine selbständige sprachliche Bedeutung haben.
+ Codeverfahren 1.

Chiffrevorrat
Anzahl der Chiffreeinheiten eines Chiffrebereiches.

Chiffrierarbeit
Sammelbegriff für Chiffrierung, Dechiffrierung und alle damit zusammenhängenden Nebenarbeiten wie z. B. tägliche Kontrolle eines Chiffriergerätes auf einwandfreie Funktion, Registrierung entnommener Wurmtabellen, Vernichtung verbrauchter Schlüsselunterlagen usw.

Chiffrierbetriebsdienst svw. Chiffrierdienst

Chiffrier-Bevollmächtigtenstelle svw. Bevollmächtigtenstelle

Chiffrierdichte
Anzahl der in der Zeiteinheit übermittelten Geheimelemente.

Chiffrierdienst
Einrichtung des Chiffrierwesens, deren Aufgabe die Planung, Organisation, Koordinierung, Sicherstellung, Durchführung und Kontrolle des Chiffrierverkehrs in einem bestimmten Bereich ist. Organisatorisch gliedert sich ein Chiffrierdienst in der Regel in eine + Zentrale, + Leitstellen, + Bevollmächtigtenstellen und + Chiffrierstellen. + zentraler Chiffrierdienst.

chiffrieren s. Chiffrierung

Chiffrierfehler s. Verstümmelung

Chiffriergerät
Gerät, das für die vollständige oder teilweise Ausführung bestimmter Chiffrier- und/oder Dechiffrierschritte ausgelegt ist.

Die Chiffriergeräte werden eingeteilt:

(1) nach der Sicherheit in + Schlüsselgeräte, + Tarngeräte und + Verschleierungsgeräte;

(2) nach der Textart, die chiffriert wird, in + Schriftchiffriergeräte, + Datenchiffriergeräte, + Sprachchiffriergeräte, + Bildchiffriergeräte u. a.;

(3) nach der Betriebsart in + Direktchiffriergeräte und + Vorchiffriergeräte.

Bei Kombination mehrerer dieser Gesichtspunkte heißt es Schriftschlüsselgerät, Sprachverschleierungsgerät, Bilddirektchiffriergerät usw.

Chiffriergeschwindigkeit
Mittelwert für das Verhältnis der Länge eines Grundtextes zur Zeit, die zu dessen Chiffrierung (einschließlich Kenngruppenbildung usw.) benötigt wird.

Die Chiffriergeschwindigkeit wird in der Regel durch die Anzahl der Grundelemente angegeben, die durchschnittlich in einer Minute chiffriert werden können.

Chiffriergeschwindigkeitsfaktor
Gütefaktor zur Bewertung der + Chiffrier- und + Dechiffriergeschwindigkeit.

Chiffrierkanal
Kanal zwischen zwei Direktchiffriergeräten.
+ offener Kanal.

Chiffrierkorrespondent
Teilnehmer eines Chiffrierverkehrs.

Chiffrierkorrespondenz
Gesamtheit der für die Bearbeitung mit Chiffrierverfahren vorgesehenen oder mit Chiffrierverfahren bearbeiteten Nachrichten, einschließlich aller Zwischenmaterialien und der dechiffrierten Texte.

Chiffrierleitstelle svw. Leitstelle

Chiffriermaschine svw. Chiffriergerät

Chiffriermechaniker
Mechaniker, der auf dem Gebiet der Wartung und Reparatur von Chiffriertechnik tätig ist. Je nach Qualifikationsgrad werden
+ Mechaniker und + Hauptmechaniker für Chiffriertechnik unterschieden.

Chiffriermittel
Zur Anwendung eines Chiffrierverfahrens benötigte spezielle Mittel, die der Geheimhaltung unterliegen.
Dazu gehören Schlüsselunterlagen, Chiffriertechnik, Geheimcodes, Anwendungsvorschriften u. a.

Chiffriermittelfaktor
Gütefaktor zur Bewertung der physikalisch-technischen Eigenschaften der zur Benutzung eines Chiffrierverfahrens erforderlichen Chiffriermittel, wie z. B. Umfang und Format, Haltbarkeit, Anzahl, Anordnung und Unterbringung der Teile, Lesbarkeit und Übersichtlichkeit, speziell bei Chiffriergeräten auch Gewicht, Stromabhängigkeit und Stromverbrauch, Störanfälligkeit, Wartungsaufwand. Es bestehen enge Beziehungen zum + Schwierigkeitsfaktor.

Chiffriernetz
Zusammenhängendes Netz von Chiffrierverbindungen. Es kann in Teilnetze zerfallen oder selbst Teilnetz sein.

Chiffrierorgan svw. Einrichtung des Chiffrierwesens

Chiffrierraum
Raum des Chiffrierwesens, der für die Chiffrierarbeit hergerichtet ist und genutzt wird.

Chiffrierscheibe svw. Scheibe oder Schlüsselscheibe

Chiffrierschritt
Einzelner Arbeitsgang bei einer Chiffrierung, wenn sich diese aus mehreren Arbeitsgängen zusammensetzt, wie z. B. Herrichtung des Klartextes, Bildung eines Zwischentextes, Durchführung einer kryptographischen Addition, Bildung bzw. Entnahme und Einsetzung einer Kenngruppe. Analog können auch DECHIFFRIERSCHRITTE unterschieden werden.

Chiffriersignal
Indikator, der bei einem Chiffreverfahren angewandt wird.
+ Codiersignal.

Chiffrierstelle
Stelle, in der von Mitarbeitern eines Chiffrierdienstes eine oder mehrere Chiffrierverbindungen unterhalten werden.
+ motorisierte Chiffrierstation.

chiffrierte Nachricht svw. Geheimtext

Chiffriertechnik
Technik, die für den Einsatz als Chiffriermittel ausgelegt ist.

Chiffrierteil s. Substitution

chiffrierter Text svw. Geheimtext

Chiffrierung (Infinitiv: CHIFFRIEREN)
Umwandlung von Grundtext (in der Regel Klartext) in Geheimtext durch Anwendung eines Chiffrierverfahrens. (Im Sinne der Informationstheorie: Codierung zum Zweck der Geheimhaltung.) Auch zusammenfassende Bezeichnung für Chiffrierung und + Dechiffrierung. Nach der Sicherheit des angewandten Verfahrens wird unterschieden zwischen + Schlüsselung, + Tarnung und + Verschleierung, nach dem Einsatz von Chiffriertechnik zwischen + manueller, + teilmaschineller und + maschineller Chiffrierung, nach der Vollständigkeit der Chiffrierung eines Textes zwischen + Vollchiffrierung und + Teilchiffrierung.

Chiffrierunterlagen
Dokumente oder Gegenstände, die + Geheimnisse des Chiffrierwesens sind oder enthalten.
Dazu gehören:
- + Chiffriermittel;
- Zwischenmaterial, das bei der Produktion oder Anwendung von Chiffriermitteln entsteht;
- sonstige fixierte Texte (Schriftstücke, Erzeugnisse der Druck- und Reproduktionstechnik, Bilder, Tonbänder, Filme usw.) mit Informationen über Eigenschaften, Anwendungsbedingungen, Anwendungsbereiche und Anwendungsweise benutzter Chiffrierverfahren und -mittel, über Arbeitsrichtung, Arbeitsweise Arbeitsergebnisse, Struktur, Organisation, Sitz, Räumlichkeiten, Mitarbeiter, Absicherung von Einrichtungen des Chiffrierwesens u. a.

Chiffrierverbindung
Nachrichtenverbindung zur Übermittlung von Geheimtexten zwischen Korrespondenten des gleichen Schlüsselbereiches.
Nach dem angewandten Verfahren werden unterschieden:
(1) SCHLÜSSEL-, TARN- und VERSCHLEIERUNGSVERBINDUNG (je nachdem, ob ein Schlüssel-, Tarn- oder Verschleierungsverfahren angewandt wird);
(2) MANUELLE, MASCHINELLE und TEILMASCHINELLE CHIFFRIERVERBINDUNG (je nachdem, ob ein manuelles, maschinelles oder teilmaschinelles Verfahren angewandt wird);
(3) INTERN- und EXTERNVERBINDUNG (je nachdem, ob ein Intern- oder Externverfahren angewandt wird).

Chiffrierverfahren
System konstanter und variabler Vorschriften und Hilfsmittel (+ Chiffriermittel), das zur Chiffrierung (und Dechiffrierung) dient. (Im Sinne der Informationstheorie: Codierverfahren zum Zweck der Geheimhaltung.)
Die konstanten Vorschriften und Hilfsmittel bleiben ständig oder auf längere Zeit unverändert. Zu den konstanten Vorschriften gehören in der Regel Vorschriften über Herrichtung des Klartextes, Bildung des Zwischentextes, Art und Weise der Zuordnung von Klareinheiten zu Geheimeinheiten u. a., zu den konstanten Hilfsmitteln Chiffriergeräte, Schlüsselcodes, Phrasenverzeichnisse von Tarntafeln u. a. Die variablen Vorschriften und Hilfsmittel werden laufend oder in kürzeren Zeitabständen verändert oder ausgewechselt. Zu den variablen Vorschrif-

ten gehören z. B. Vorschriften über die Bildung von Additionsreihen aus vorgegebenen Unterlagen bei Mehrfachwurmverfahren oder über die Reihenfolge der Eintragung von Klareinheiten in Raster bei Transpositionsverfahren, zu den variablen Hilfsmitteln z. B. Schlüssellochstreifen, vorgedruckte Additionsreihen, Schlüsselstreifen.
Das vollständige Teilsystem der zur Umwandlung eines Textes notwendigen variablen Vorschriften und Hilfsmittel wird als SCHLÜSSEL bezeichnet.

Die Chiffrierverfahren werden eingeteilt:

(1) nach der Erkennbarkeit des Geheimtextes als solchem (d. h. als Geheimtext) in + offene Verfahren und + gedeckte Verfahren;

(2) nach der sprachlichen Beschaffenheit der Klareinheiten in + Chiffreverfahren und + Codeverfahren;

(3) nach der Grundmethode der Umwandlung in + Substitutionsverfahren und + Transpositionsverfahren;

(4) nach der Sicherheit in + Schlüsselverfahren, + Tarnverfahren und + Verschleierungsverfahren;

(5) nach der Art der angewandten Chiffriermittel in + manuelle Verfahren, + teilmaschinelle Verfahren und + maschinelle Verfahren;

(6) nach der Art der Geheimelemente in + Buchstabenverfahren, + Ziffernverfahren, + Mischverfahren und + Zeichenverfahren;

(7) nach der Länge der Grundeinheiten in + monographische Verfahren und + polygraphische Verfahren;

(8) nach der Unterschiedlichkeit der Länge der Geheimeinheiten in + gleichstellige Verfahren und + wechselstellige Verfahren;

(9) nach dem Verwendungszweck innerhalb eines Chiffrierverkehrs in + Hauptverfahren, + Zusatzverfahren, + Sonderverfahren, + Notverfahren, + Behelfsverfahren und + Ersatzverfahren;

(10) nach dem zugelassenen Benutzerkreis in + Internverfahren und + Externverfahren.

+ kombiniertes Verfahren.

Chiffrierverkehr
Nachrichtenverkehr, in dem Geheimtexte übermittelt werden.
Die potentiellen Teilnehmer eines Chiffrierverkehrs (Chiffrierkorrespondenten) bilden einen + Schlüsselbereich.

Innerhalb der einzelnen Schlüsselbereiche sind folgende VERKEHRSARTEN möglich:

- + einseitiger und + zweiseitiger Verkehr;
- + allgemeiner und + individueller Verkehr;
- + Zirkular- und + Zirkulargegenverkehr.

Chiffriervorrichtung
Nicht als selbständiges Chiffriergerät funktionsfähiger Bestandteil eines fernmeldetechnischen Systems, in dem Chiffrier- und/oder Dechiffrierschritte ablaufen.

Chiffrierwalze svw. Schlüsselwalze

Chiffrierwesen
Gesamtheit der Einrichtungen, Maßnahmen und Tätigkeiten auf den Gebieten

- Kryptologie;
- Entwicklung, Produktion und Auswertung von Chiffrierverfahren und -mitteln;
- Wartung und Reparatur von Chiffriertechnik;
- Planung, Organisation, Koordinierung, Sicherstellung, Durchführung, Absicherung und Kontrolle von Chiffrierverkehren;
- Dekryptierung.

Chiffrierzentrale svw. Zentrale

Code

1. In der Informationstheorie: Zusammenstellung von einander eindeutig umkehrbar zugeordneten Zeichenfolgen eines Alphabetes zu Zeichenfolgen des gleichen oder eines anderen Alphabetes.
2. In der Kryptologie: Zusammenstellung von einander zugeordneten Phrasen und Codegruppen, die zur Umwandlung von Klartext in Codetext und umgekehrt dient.

Die Codes werden eingeteilt:

(1) nach der Geheimhaltung, der sie unterliegen, in + Geheimcodes und + öffentliche Codes;

(2) nach der Art ihrer Verwendung als Chiffriermittel in + nichtüberschlüsselte Codes und + Schlüsselcodes;

(3) nach dem Anwendungsbereich, auf den der Phrasenbestand ausgerichtet ist, in + Militärcodes, + Verwaltungscodes, + Wirtschaftscodes, + Privatcodes, + Wettercodes u. a.;

(4) nach der Größe des Phrasenbestandes in + Kurzcodes und + Satzbücher;

(5) danach, ob die Phrasen eingetragen sind oder nicht, in + Phrasencodes und + Blankocodes;

(6) nach der Anzahl der Sprachen, in denen die Phrasen abgefaßt sind, in + einsprachige und + mehrsprachige Codes;

(7) nach der Art der Codeelemente in + Buchstabencodes, + Zifferncodes, + Mischcodes und + Zeichencodes;

(8) nach der Unterschiedlichkeit der Länge der Codegruppen in + gleichstellige und + wechselstellige Codes;

(9) nach der satztechnischen Anordnung der Phrasen und Codegruppen in + Codebücher und + Codetafeln;

(10) nach der Anzahl verschiedener Anordnungen der Phrasen in + Einfachcodes und + Mehrfachcodes;

(11) nach der Anzahl der Phrasenstellen, die den einzelnen Codegruppen zugeordnet sind, in + einstufige und + mehrstufige Codes.

Codealphabet
Die Codeelemente eines Codeelementebereiches in bestimmter Reihenfolge.

Codebuch
Code in Buchform, bei dem die Codegruppen in geschlossener Form unmittelbar neben den zugehörigen Phrasen stehen.
+ Codetafel.

Codeelement
Element eines Codetextes.

Codeelementebereich
Menge der voneinander verschiedenen Codeelemente, die für ein Codeverfahren zugelassen sind.

Codeelementevorrat
Anzahl der Codeelemente eines Codeelementebereiches.

Codefolge
Folge von Codeelementen.

Codegruppe
Die bei Codeverfahren einer Phrase zugeordnete Ersatzeinheit.
Bei nichtüberschlüsselten Geheimcodes sind die Codegruppen zugleich Geheimeinheiten, bei Schlüsselcodes Zwischeneinheiten.

Bei Tarnverfahren wird die Codegruppe als TARNGRUPPE, bei Verschleierungsverfahren als DECKBEZEICHNUNG bezeichnet. Eine aus Buchstaben bestehende Codegruppe wird auch als CODEWORT, eine aus Ziffern bestehende als CODEZAHL bezeichnet.

Codegruppenbereich
Menge der voneinander verschiedenen Codegruppen, die für ein Codeverfahren zugelassen sind.

Codegruppengleichung
Mathematische Darstellung des Bildungsgesetzes für einen Codegruppenbereich in Form einer Gleichung.

Codegruppentafel
Tabellarische Anordnung der Codeelemente eines gesicherten Codegruppenbereiches als Hilfsmittel zur Bildung der zugelassenen Codegruppen und zur Berichtigung verstümmelter Codegruppen.

Codegruppenvorrat
Anzahl der Codeguppen eines Codegruppenbereiches.

Codekomponente s. Substitution

Codemischtext
Codetext, der aus Codegruppen verschiedener Codeverfahren besteht.

Codemittel
Chiffriermittel zu Codeverfahren.
+ Chiffriermittel.

Codestil
Ausdrucksweise, die es ermöglicht, den Inhalt eines Textes mit der geringstmöglichen Anzahl von Codegruppen eines bestimmten Codes wiederzugeben.

Codetafel
Code, bei dem die Phrasen in den durch Zeilen und Spalten gebildeten Feldern von Tafeln stehen oder die Codegruppen durch Verbindung von Komponenten, z. B. den Tafel-, Zeilen- und Spaltenbezeichnungen gebildet werden.
+ Codebuch

Codetafeln, die als Chiffriermittel dienen, werden in der Regel nicht überschlüsselt. Sie werden eingeteilt:

(1) nach der Sicherheit in + Schlüsseltafeln, + Tarntafeln und verschiedene Arten von Codetafeln, die der Verschleierung dienen (+ Sprechtafel, + Buchstabiertafel, + Zahlentafel, + Buchstabier- und Zahlentafel, + Signaltafel);

(2) nach der Anzahl verschiedener Anordnungen der Phrasen in + Einfachtafeln und + Mehrfachtafeln.
+ Blankotafel.

Codetext
Text, der durch Anwendung eines Codeverfahrens entstanden ist.
+ Codemischtext.

Codeumfang
Anzahl der verschiedenen Codegruppen eines Codes, denen Phrasen zugeordnet sind.
+ Phrasenbestand.

Codeverfahren
1. Chiffrierverfahren, bei dem die Grundeinheiten im wesentlichen von unterschiedlicher Länge und Beschaffenheit sind und eine selbständige sprachliche Bedeutung haben.
   + Chiffreverfahren.
2. svw. Codierverfahren.

Codewort s. Codegruppe

Codezahl s. Codegruppe

codieren s. Codierung

Codierer
Person, die codiert und decodiert.

Codierfehler s. Verstümmelung

Codiersignal
1. Indikator, der bei einem Codeverfahren angewandt wird.
2. Chiffriersignal, das den Übergang zu Codetext anzeigt.

Codiertafel
Der Teil einer Mehrfachtafel, der zum Codieren dient.

Codierteil
Der Teil oder die Teile von Mehrfachcodes, die zum Codieren dienen.

Codierung (Infinitiv: CODIEREN)
1. In der Informationstheorie: Eindeutig umkehrbare Umwandlung von Zeichenfolgen eines Alphabetes zu Zeichenfolgen des gleichen oder eines anderen Alphabetes.

2. In der Kryptologie: Umwandlung von Grundtext (in der Regel Klartext) in Codetext durch Anwendung eines Codeverfahrens. Auch zusammenfassende Bezeichnung für Codierung und + Decodierung.

Je nach Vollständigkeit der Codierung eines Textes wird unterschieden zwischen + Vollcodierung und + Teilcodierung.

Codierverfahren
Methode der + Codierung im Sinne der Informationstheorie.

Codistik
Wissenschaft von den Codeverfahren.

Daten
Durch Zeichenfolgen eindeutig dargestellte Informationen, die eine durch Datenwörter, Datensätze und Datensatzfolgen gekennzeichnete Struktur haben.
Dabei ist ein DATENWORT, auch DATENEINHEIT genannt, eine Zeichenfolge mit selbständiger Bedeutung; miteinander verbundene und einem Ordnungsmerkmal zugeordnete Datenwörter bilden einen DATENSATZ.
NUMERISCHE DATEN bestehen nur aus Ziffern; ALPHANUMERISCHE DATEN bestehen aus Ziffern und Buchstaben.

Datenchiffriergerät
Chiffriergerät, das für die Chiffrierung von + Daten ausgelegt ist.

Datenchiffrierprogramm
Programm für eine Datenchiffrierung.

Datenchiffrierung
Chiffrierung von + Daten, besonders bei der Datenfernübertragung.

Dateneinheit s. Daten

Datenfernübertragung s. Datenübertragung

Datenfernverarbeitung
Zusammenfassender Begriff für + Datenfernübertragung und + Datenverarbeitung.

Datensatz s. Daten

Datenträger
Gegenstände, auf denen Daten zum Zwecke der Eingabe oder bei Ausgabe gespeichert werden, z. B. Lochstreifen, Lochkarten, Magnetbänder.

Datentransfer s. Datenübertragung

Datentransport s. Datenübertragung

Datenübertragung
Elektronische Übertragung von Daten über Leitungssysteme innerhalb einer Datenverarbeitungsanlage (DATENTRANSPORT oder DATENTRANSFER) oder auf größere Entfernungen nach außerhalb (DATENFERNÜBERTRAGUNG).

Datenverarbeitung
Das Erfassen, Aufbereiten, Ausgeben, Weiterleiten, Auswerten und Aufbewahren von Daten für bestimmte Zwecke (Planung, Lenkung, Analyse usw.) auf bestimmten Gebieten (Wirtschaft, Verwaltung usw.) in dauernder Wiederholung.

Datenwort s. Daten

Dechiffrator
Baugruppe eines Chiffriergerätes, in der die Dechiffrierung realisiert wird.

Dechiffreur
Person, die dechiffriert.

dechiffrieren s. Dechiffrierung

Dechiffrierfehler s. Verstümmelung

Dechiffriergeschwindigkeit
Mittelwert für das Verhältnis der Länge des Grundtextes zur Zeit, die zur Dechiffrierung des entsprechenden Geheimtextes benötigt wird. Die Dechiffriergeschwindigkeit wird in der Regel durch die Anzahl der Grundelemente angegeben, die bei der Dechiffrierung durchschnittlich in einer Minute entstehen.

Dechiffrierschritt s. Chiffrierschritt

Dechiffrierteil s. Substitution

Dechiffrierung (Infinitiv: DECHIFFRIEREN)
Rückverwandlung von Geheimtext in Grundtext (in der Regel Klartext) durch Personen, die sich offiziell im Besitz der angewandten Chiffriermittel befinden.
+ Dekryptierung.

Dechiffriervorrichtung svw. Dechiffrator

Deckbezeichnung s. Codegruppe

Decknome
Deckbezeichnung in Form eines oder mehrerer Wörter.

Decknamenverzeichnis
Zusammenstellung von einander zugeordneten Phrasen und Decknamen.

Deckzahl
Deckbezeichnung in Form einer Zahl.

Deckzahlenverzeichnis
Zusammenstellung von einander zugeordneten Phrasen und Deckzahlen.

decodieren s. Decodierung

Decodierer
Person, die decodiert.

Decodierfehler s. Verstümmelung

Decodiertafel
Der Teil einer Mehrfachtafel, der zum Decodieren dient.

Decodierteil
Der Teil oder die Teile von Mehrfachcodes, die zum Decodieren dienen.

Decodierung (Infinitiv: DECODIEREN)
Rückverwandlung von Codetext in Grundtext (in der Regel Klartext) durch Personen, die sich offiziell im Besitz des angewandten Codes befinden.

Dekombinator
Baugruppe zur Umwandlung eines Binärcodes in einen (‡)-Code.

Dekonspiration
Verstoß gegen die Regeln der konspirativen Tätigkeit (+ Konspiration), in dessen Ergebnis unbefugte Personen Kenntnis von geheimen Informationen oder Gegenständen erhalten.
+ Kompromittierung, unbefugte Offenbarung.

Dekrypteur
Person, die Dekryptierarbeiten durchführt.

Dekryptierarbeit
Bearbeitung von Chiffrierverfahren und Geheimtexten mit Methoden und Mitteln der Kryptanalysis, um die Chiffrierverfahren und die mit ihnen bearbeiteten Klartexte zu rekonstruieren.

Dekryptierbarkeit
Ein Geheimtext ist dekryptierbar, wenn er ohne vorherige Kenntnis des Schlüssels durch Anwendung von Methoden der Kryptanalysis in den Grundtext rückverwandelt werden kann.
+ Lösbarkeit.

Dekryptierdienst
Einrichtung des Chiffrierwesens, deren Aufgabe die Planung, Organisation, Koordinierung, Durchführung und Kontrolle der Dekryptierarbeit in einem bestimmten Bereich ist.

dekryptieren s. Dekryptierung

Dekryptiergerät
Gerät, das für die vollständige oder teilweise Ausführung bestimmter Dekryptierschritte ausgelegt ist.

Dekryptiermethode
System allgemeiner Arbeitsmethoden, Regeln und Vorschriften der Kryptanalysis, die zur Dekryptierung von Geheimtexten eines bestimmten Chiffrierverfahrens angewandt werden.

Dekryptiermöglichkeiten
Umstände und Bedingungen, die eine Dekryptierung allgemein oder in einem speziellen Fall ermöglichen, z. B. bei einem bestimmten Verfahren, Mittel oder Text oder bei einem bestimmten Verstoß gegen die Anwendungsvorschriften.

Dekryptierstelle
Stelle, in der von Mitarbeitern eines Dekryptierdienstes Dekryptierarbeiten durchgeführt werden.

Dekryptiertechnik
Technik, die für den Einsatz in der Dekryptierarbeit ausgelegt ist.

Dekryptierung (Infinitiv: DEKRYPTIEREN)
1. Rückverwandlung von Geheimtext in Grundtext durch Personen, die sich nicht offiziell im Besitz der angewandten Chiffriermittel befinden.
   + Dechiffrierung, Lösung, Mitlesen.
2. Einrichtung des Chiffrierwesens, deren Aufgabe die Gewinnung von Informationen über den Gegner durch Dekryptierarbeit ist.
   + Dekryptierdienst, Dekryptierstelle.

Dekryptierung eines Chiffrierverfahrens svw. Lösung eines Chiffrierverfahrens

Dezimationsalphabet
Alphabet, das aus einem vorgegebenen Alphabet entsteht, wenn aus diesem nur immer das k-te Zeichen genommen wird und die herausgenommenen Zeichen nicht weiter mitgezählt werden.
Beispiel: Das 3. Dezimationsalphabet zum Normalalphabet ist
c f i l o r u x a e j n s w b h p v d m y k z t g q .
+ Primalphabet.

Dienstgeheimnis
Geheimnisart, die nicht offenkundige Tatsachen, Gegenstände oder Nachrichten beinhaltet, die für die Sicherheit des Staates und die Tätigkeit der staatlichen und gesellschaftlichen Organe bedeutsam sind.
+ Staatsgeheimnis, Geheimhaltungsgrad.

Dienstgruppe
Einem Spruch beigefügte Gruppe, in der Angaben zur Betriebs- oder Verkehrsabwicklung enthalten sind, z. B. Dringlichkeit oder Gruppenanzahl.

diplomatischer Code
Code, der im diplomatischen Nachrichtenverkehr angewandt wird.

Direktchiffriergerät
Chiffriergerät, das für + Direktchiffrierung ausgelegt ist.
Direktchiffriergeräte können gleichzeitig für Vorchiffrierung ausgelegt sein.
+ Vorchiffriergerät, Kanalchiffriergerät.

Direktchiffrierstelle
Chiffrierstelle, in der eine oder mehrere Direktchiffrierverbindungen unterhalten werden.

Direktchiffrierung
Maschinelle Chiffrierung, bei der Chiffrierung, Übermittlung und Dechiffrierung gekoppelt sind und ohne Zwischenspeicherung des Geheimtextes praktisch gleichzeitig erfolgen. Bei TEILDIREKTCHIFFRIERUNG erfolgt entweder nur zwischen Chiffrierung und Übermittlung oder nur zwischen Übermittlung und Dechiffrierung keine Zwischenspeicherung des Geheimtextes.
+ Vorchiffrierung, Kanalchiffrierung.

Direktchiffrierverbindung
Chiffrierverbindung, die für Direktchiffrierung ausgelegt ist.

direktes Intervall s. Alphabet.

Doppelwürfelverfahren s. Würfelverfahren

Drahtaufklärung
Teil der Fernmeldeaufklärung, der auf die Erfassung und Auswertung gegnerischer Drahtnachrichtenverkehre gerichtet ist.
+ Funknachrichtenaufklärung.

Dreiergruppe s. Gruppe

Dringlichkeit
Rang einer Nachricht für Übermittlung und Zustellung.
Z. B. gelten bei der Deutschen Post folgende DRINGLICHKEITS-STUFEN (Rangstufen) für Telegramme: Nottelegramm – Blitztelegramm (Dienstvermerk: Blitz) – dringendes Telegramm (Dienstvermerk: D) – gewöhnliches Telegramm – Brieftelegramm (Dienstvermerk: LT).

Dringlichkeitsstufen s. Dringlichkeit

Duplexbetrieb
Betriebsweise des Fernmeldeverkehrs und der Datenübertragung, bei der Nachrichten gleichzeitig in beiden Richtungen übertragen werden.
+ Halbduplexbetrieb, Simplexbetrieb.

effektiver Schlüsselvorrat
Anzahl der nicht äquivalenten Schlüssel eines Schlüsselvorrates.

eigentlicher Phrasenbestand
Anzahl der Phrasenstellen eines Codes, die mit verschiedenen Phrasen besetzt sind.

Einbauverfahren
Briefverfahren, bei dem die Schriftzeichen, die den Geheimtext bilden, nicht gekennzeichnet sind, sondern durch einen zwischen den Korrespondenten verabredeten Schlüssel bestimmt werden.
+ Kennzeichnungsverfahren.

Einbruch in einen Geheimtext
Bestimmung einer Folge von Grundeinheiten ohne Kenntnis des angewandten Schlüssels.

Eineindeutigkeit
Eine Zuordnungsvorschrift von zwei Mengen A und B ist eindeutig, wenn
– jedem Element von A ein Element von B zugeordnet ist

- verschiedenen Elementen von A verschiedene Elemente von B zugeordnet sind
- jedem Element von B ein Element von A zugeordnet ist.

Zwei endliche Mengen können genau dann einander eineindeutig zugeordnet werden, wenn die Anzahl ihrer Elemente gleich ist.

Einfachbelegung s. Belegung

Einfachcode
Code, dessen Zuordnung von Phrasen und Codegruppen nur in einer Anordnung vorliegt, die sowohl zum Codieren als auch zum Decodieren dient.
+ Mehrfachcode, Einfachtafel.

einfache Verstümmelung
Verstümmelung durch Veränderung, Ausfall oder Hinzufügung eines einzigen Elementes oder Vertauschung zweier benachbarter Elemente.

einfacher Phrasencode
Code, der als Phrasen einzelne Elemente, Polygramme, Wörter, Wortfolgen, Sätze und dgl. enthält, die in beliebiger Reihenfolge zu Nachrichtentexten zusammengefügt werden können.
+ Formularcode.

einfaches Tauschverfahren s. Tauschverfahren

Einfachtafel
Codetafel, die nach dem Prinzip der Einfachcodes aufgebaut ist.
+ Mehrfachtafel.

Eingangsheft s. Schlüsselheft

Eingangskassette s. Schlüsselkassette

Eingangsschlüssel
Schlüssel, mit dem bei rekurrenten Verfahren der Textanfang chiffriert wird, bevor die rekurrente Chiffrierung einsetzt.

Einheit
Zusammenfassung von Elementen, die bei bestimmten Arbeitsgängen, z. B. Chiffrierschritten, als ein Ganzes behandelt oder gebildet wird. Im Grenzfall gleichbedeutend mit Element.
+ Additionseinheit, Chiffreeinheit, Codegruppe, Geheimeinheit, Grundeinheit, Klareinheit, Phrase, Polygramm, Zwischeneinheit.

Einlegemarkierung s. Abschnittsmarkierung

Einrichtungen des Chiffrierwesens
Dienste und Dienststellen, die mit bestimmten Aufgaben des Chiffrierwesens beauftragt sind. Dazu gehören das + Zentrale Chiffrierorgan, kryptologische Forschungs- und Entwicklungsstellen, + Chiffrierdienste, + Chiffrierstellen, + Leitstellen, + Bevollmächtigtenstellen, + Dekryptierdienste, + Dekryptierstellen, Produktionsstellen für Chiffriermittel, Reparatur- und Wartungsdienste für Chiffriertechnik u. o.
+ Räume des Chiffrierwesens.

Einsatzbedingungen svw. Anwendungsbedingungen

Einsatzgruppe
Additionsgruppe, die als erste zur Chiffrierung benutzt wird.

(n/1)-Code (Eins-aus-n-Code)
Maschinell lesbare Darstellung von n Zeichen, wobei jedem Zeichen eine eigene Informationsleitung zugeordnet ist.

einseitiger Verkehr
Chiffrierverkehr, bei dem jeder Korrespondent nur Absender oder nur Empfänger ist, z. B. einseitiger individueller Verkehr, Zirkularverkehr, Zirkulargegenverkehr.

einsprachiger Code
Code, bei dem die den einzelnen Codegruppen zugeordneten Phrasen jeweils nur in einer Sprache abgefaßt sind, unabhängig davon, ob sie verschiedenen Sprachen entnommen sind. Nach der hauptsächlich verwendeten Sprache wird unterschieden zwischen deutschsprachigen Codes usw.
+ mehrsprachiger Code.

Einstellgruppe
Gruppe, die eine bestimmte Schlüsseleinstellung anzeigt.

einstufiger Code
Code, in dem jeder Codegruppe nur eine Phrasenstelle zugeordnet ist.
+ mehrstufiger Code.

Einzelblattabsicherung
Spezielle Art der Verpackung von Schlüsselunterlagen, bei der jedes Blatt einzeln so abgedeckt ist, daß es erst nach Entfernung oder Verletzung dieser Abdeckung eingesehen werden kann.
Die Einzelblattabsicherung dient als Schutz gegen vorzeitige und unbefugte Einsichtnahme in Schlüsselunterlagen.

elektronischer Krieg svw. Funkkrieg

Element
In der Kryptologie svw. Elementarzeichen (+ Zeichen), z. B. Schriftzeichen, Lochkombination, Impulsfolge.
Nach der Stellung im Chiffrierprozeß werden unterschieden:
+ Klarelement, + Zwischenelement, + Grundelement, + Geheimelement.
+ Codeelement, Füllelement.

Elementarzeichen s. Zeichen

Elementebereich
Festgelegte Menge voneinander verschiedener Elemente.
+ Alphabet, Elementevorrat.

Elementefolge svw. Gruppe

Elementegruppe svw. Gruppe

Elementevorrat
Anzahl der Elemente eines Elementebereiches bzw. Alphabetes.

empfangende Chiffrierstelle
Chiffrierstelle, für die ein Geheimtext bestimmt ist.

Empfänger
1. Person oder Stelle, für die eine Nachricht bestimmt ist.
2. Teil einer + Kommunikationskette.

Entnahmetabelle
Tabelle, in der die Entnahme bzw. Verwendung von Schlüsselunterlagen quittiert wird.

Entstümmelung
Beseitigung einer Verstümmelung.

Entstümmelungstafel svw. Codegruppentafel

enttarnen s. Enttarnung

Enttarnung (Infinitiv: ENTTARNEN)
Dechiffrierung von Tarntext.

Entwicklung eines Chiffrierverfahrens oder Chiffriermittels
Gesamtheit aller Arbeitsgänge, die zur Herstellung eines neuen Chiffrierverfahrens oder -mittels führen, angefangen von der Auftragserteilung bis zur Freigabe der Chiffriermittel für die Produktion.

Erkennungsgruppe
Einem Spruch beigefügte Gruppe, die Angaben für die empfangende Nachrichten- oder Chiffrierstelle enthält.
Spezielle Erkennungsgruppen sind + Dienstgruppe, + Schlüsselgruppe, + Kenngruppe, + Unterscheidungsgruppe, + Kontrollgruppe.

Ersatzeinheit s. Substitution

Ersatzverfahren
Chiffrierverfahren, das als Ersatz für ein anderes, bei Einführung des Ersatzverfahrens außerkraftgesetztes Chiffrierverfahren dient.

erweitertes Alphabet
Alphabet, das aus einem vorgegebenen Alphabet durch Hinzufügung mindestens eines weiteren Zeichens entsteht.

Externmittel
Chiffriermittel zu Externverfahren.
+ Internmittel.

Externverbindung s. Chiffrierverbindung

Externverfahren
Chiffrierverfahren, das zur Benutzung außerhalb des Chiffrierdienstes freigegeben ist.
+ Internverfahren.

Fahrerchiffreur
Person, die zugleich als Chiffreur und als Fahrer einer motorisierten Chiffrierstation ausgebildet und tätig ist.

Fahrerchiffreurmechaniker
Person, die zugleich als Chiffreur, als Chiffriermechaniker und als Fahrer einer motorisierten Chiffrierstation ausgebildet und tätig ist.

Faksimilechiffriergerät
Bildchiffriergerät für Schwarz-Weiß-Vorlagen.

Faksimiletelegrafie s. Bildtelegrafie

falsches Element
Element, das in einem Text an falscher Stelle bzw. anstelle eines richtigen Elementes auftritt.
Ein falsches Element, das nicht zum zugelassenen Elementebereich gehört, wird als FREMDES ELEMENT bezeichnet.

Fehlerauswirkungen s. Verstümmelung

Fehlermöglichkeiten s. Verstümmelung

Fehlerursachen s. Verstümmelung

Feldertranspositionsverfahren
Rasterverfahren, bei dem die Felder des Rasters entsprechend einer vorgegebenen unregelmäßigen Reihenfolge verwendet werden.

Fernmeldeanlage
Technische Einrichtung zur drahtlosen oder drahtgebundenen Nachrichtenübermittlung.

Fernmeldeaufklärung
Erfassung und Auswertung fremder Fernmeldeverkehre.
+ Drahtaufklärung, Funknachrichtenaufklärung.

Fernmeldegeheimnis s. Post- und Fernmeldegeheimnis

Fernmeldemittel
Geräte und Anlagen, die zur Übertragung von Nachrichten auf elektrischem Wege, über Leitungen oder durch Funk, zwischen verschiedenen Orten ohne Rücksicht auf die Entfernung dienen.

fernmeldetechnisches System s. Kommunikationskette

Fernmeldeverkehr
Gesamtheit aller durch Fernmeldeanlagen vorgenommenen Übermittlungsprozesse.

Fernmeldewesen
Gesamtheit aller betrieblichen, technischen, technologischen sowie wirtschaftlich-organisatorischen Einrichtungen und Prozesse zum Übermitteln von Nachrichten oder anderen Informationen mit Hilfe drahtgebundener oder drahtloser Fernmeldeanlagen.

Fernschreibcode
Telegrafenalphabet für Fernschreibverkehr.

Firmencode
Wirtschaftscode, der im Nachrichtenverkehr einer bestimmten Firma angewandt wird.

Folge
Elemente einer Menge in einer bestimmten Reihenfolge, wobei die Elemente der Menge mehrfach auftreten können. Die Anzahl der Elemente einer Folge ist die LÄNGE DER FOLGE.

fördernde Redundanz s. Redundanz

Formularcode
Code, der als Phrasen vollständige Nachrichtentexte oder solche Nachrichtentexte enthält, die durch Einfügung bestimmter variabler Angaben an festgelegten Stellen zu vollständigen Nachrichtentexten ergänzbar sind. Ein in dieser Weise blattweise vorgegebener Text wird als NACHRICHTENTEXTFORMULAR bezeichnet.
+ einfacher Phrasencode, Schemaspruch.

Fortsetzungsvermerk
Indikator, der eine Fortsetzung anzeigt.

fraktionelle Substitution
Substitution, bei der Teile (Fraktionen) mehrerer Ausgangseinheiten zusammengefaßt durch eine Ersatzeinheit ersetzt werden.

fraktionelles Verfahren
Substitutionsverfahren, bei dem die Chiffrierung mittels einer oder mehrerer + fraktioneller Substitutionen erfolgt.

Freigruppe
Codegruppe eines Codegruppenbereiches, der keine Phrase zugeordnet ist, unabhängig davon, ob diese Codegruppe im Code enthalten ist oder nicht.

Freistelle
Phrasenstelle, die noch nicht mit einer Phrase besetzt ist.

fremdes Element s. falsches Element

Frequenz
Anzahl des Auftretens eines gleichen Ereignisses in einem Text, z. B. Anzahl des Auftretens des Trigramms ARN.

Frequenzanalyse
Untersuchung der Frequenz eines Textes.

Frequenzanalysis
Teil der Kryptanalysis, der sich mit der Untersuchung von Frequenzen befaßt.

Frequenzausgleich
Methode zur Verhinderung bzw. Abschwächung der Widerspiegelung der Frequenzen eines Grundtextes im Geheimtext bei Anwendung nicht absolut sicherer Chiffrierverfahren, z. B. durch mehrfache Belegung der Grundeinheiten entsprechend der durchschnittlichen Häufigkeit ihres Auftretens.

Frequenzverschleierung svw. Frequenzausgleich

Frequenzverteilung
Gesamtheit der Frequenzen aller als verschieden aufgefaßten gleichartigen Ereignisse eines Textes, z. B. aller Buchstaben oder aller Wörter eines Textes.

Füllelement
Element ohne Informationsgehalt, das in den Text eingefügt wird, um eine zweckmäßige Beschaffenheit des Textes zu erreichen, z. B. zur Auffüllung einer unvollständigen Fünfergruppe.
+ Blender.

Füllfunkspruch svw. Blendspruch

Fünferalphabet s. Telegrafenalphabet

Fünfergruppe s. Gruppe

Fünfergruppenzähler s. Gruppenzähler

Fünfschrittalphabet s. Telegrafenalphabet

Funkaufklärung
Teil des Funkkrieges, der auf die Gewinnung von Information über den Gegner durch Suchen und Abhören von Funksignalen, Standortbestimmung von Funkanlagen und Aufzeichnung und Auswertung von Funksendungen gerichtet ist.
+ Funkmeßaufklärung, Funknachrichtenaufklärung.

Funkdesinformation svw. Funktäuschung

funkelektronischer Krieg svw. Funkkrieg

Funkerchiffreur
Person, die zugleich als Funker und als Chiffreur ausgebildet und tätig ist.

Funkgegenwirkung
Teil des Funkkrieges, der auf die Vernichtung, Niederhaltung bzw. Verringerung der Wirksamkeit der gegnerischen Funkmittel gerichtet ist.
+ Funkstörung.

Funkgeheimnis
Pflicht für Funker zur Geheimhaltung der gesendeten und empfangenen Nachrichten, der Frequenzen, Rufzeichen, Sendezeiten usw. gegenüber Personen, die nicht mit der Bearbeitung dieser Nachrichten usw. beauftragt sind und für die diese Nachrichten nicht bestimmt sind.

Verbot, militärische, staatliche, kommerzielle oder sonstige Funknachrichten unbefugt aufzufangen, aufzuzeichnen oder zu verbreiten.

Funkimpulsaufklärung svw. Funkmeßaufklärung

Funkkrieg
Gesamtheit der verschiedenen Formen und Methoden des Kampfes mit den Funkmitteln des Gegners und der Gewährleistung der stabilen Arbeit eigener Funkmittel.
Der Funkkrieg umfaßt die + Funkaufklärung, die + Funkgegenwirkung und die + Antifunkgegenwirkung.

Funkmeßaufklärung
Teil der Funkaufklärung, der auf die Erfassung gegnerischer Funkmeßanlagen und -sendungen gerichtet ist.

Funknachrichtenaufklärung
Teil der Fernmeldeaufklärung ebenso wie der Funkaufklärung, der auf die Erfassung und Auswertung gegnerischer Funknachrichtenverkehre gerichtet ist.
+ Drahtaufklärung.

Funkpeilung
Teil der Funkaufklärung, dessen Aufgabe die Standortbestimmung gegnerischer Funkmittel ist.

Funkspruch
Spruch, der drahtlos durch Telegrafie oder Telefonie übermittelt wird.

Funkstörung
Einwirkung auf ein Übertragungssystem, die den richtigen Empfang von Funksignalen behindert.
Man unterscheidet natürliche und künstliche Funkstörungen. Zu den natürlichen Störungen gehören atmosphärische Störungen. Zu den künstlichen Störungen gehören unbeabsichtigte, die durch benachbarte Sender verursacht werden, sowie absichtlich erzeugte. Absichtliche Funkstörungen sind Bestandteil der + Funkgegenwirkung; sie werden unterteilt in aktive (von speziellen Störsendern erzeugte) und passive (durch Reflexion elektromagnetischer Wellen an Scheinzielen erzeugte).

Funktarnung
Maßnahmen der + Antifunkgegenwirkung zur Erschwerung der gegnerischen Funkaufklärung. Dazu gehören die Einschränkung der Sendezeiten auf ein Minimum, die Funkstille, die Verminderung der Sendeleistung, häufiger Wechsel der Arbeitsfrequenzen und Rufzeichen u. a.

Funktäuschung
Maßnahmen der + Antifunkgegenwirkung zur Täuschung des Gegners über die wahre Lage. Dazu gehören die Aussendung unwahrer Informationen, die Nachahmung von Funksignalen, die Einführung von Scheinfunkstellen, die Vortäuschung eines gesteigerten Funkbetriebes u. a.

funktionsgebundener Benutzer von Chiffrierverfahren
Person, die auf Grund ihrer Funktion zur Benutzung bestimmter Chiffrierverfahren berechtigt ist, ohne Mitarbeiter eines Chiffrierdienstes zu sein. Personen, die nur für Torn- und Verschleierungsverfahren zugelassen sind, werden auch als TARNER, solche, die auch für Schlüsselverfahren zugelassen sind, als SCHLÜSSLER bezeichnet.

Gebrauchsanweisung
Zusammenfassung der Vorschriften, die zusätzlich zu allgemeinen Vorschriften die Anwendung eines Chiffrierverfahrens oder -mittels regeln, z. B. über Herrichtung des Klartextes, Bildung von Zwischentext, Bildung und Einsetzung von Kenn- oder Schlüsselgruppen, Anwendung der Schlüsselunterlagen bei Chiffrierung und Dechiffrierung, bei maschinellen Verfahren auch über Funktionskontrolle, Inbetriebnahme und Bedienung verwendeter Geräte.
Die Gebrauchsanweisung enthält in der Regel auch die + Sicherheitsbestimmungen zum jeweiligen Verfahren.

Gedächtnisschlüssel
Schlüssel, der im Gedächtnis aufbewahrt wird.

Gedächtnisverfahren
Chiffrierverfahren, zu dessen Anwendung keine bleibenden Chiffriermittel notwendig sind.

gedeckte Führung
System von Maßnahmen zur Geheimhaltung der Führung, insbesondere der dabei zu übermittelnden Nachrichten.
Im militärischen Bereich als GEDECKTE TRUPPENFÜHRUNG bezeichnet.

gedeckte Truppenführung s. gedeckte Führung

gedeckter Geheimtext
Geheimtext, der durch Anwendung eines gedeckten Verfahrens entstanden ist und demnach nicht ohne weiteres als solcher erkennbar ist.
+ offener Geheimtext.

gedecktes Verfahren
Chiffrierverfahren, bei dessen Anwendung der Geheimtext selbst oder die Tatsache, daß eine Chiffrierung stattgefunden hat, verborgen wird. Zu den gedeckten Verfahren gehören die + Briefverfahren, die + verabredete Sprache, die + chemischen Geheimschreibverfahren und die + Mikratverfahren.
+ offenes Verfahren.

Gegenbetrieb svw. Duplexbetrieb

Geheimalphabet
Die Geheimelemente eines Geheimelementebereiches in bestimmter Reihenfolge.

Geheimbereich
Menge der voneinander verschiedenen Geheimeinheiten, die für ein Chiffrierverfahren zugelassen sind.

Geheimcode
Code, der der Geheimhaltung unterliegt.
Geheimcodes dienen in der Regel als Chiffriermittel.
+ öffentlicher Code.

geheime Nachricht
Nachricht, die als Staats- oder Dienstgeheimnis klassifiziert ist.
+ Geheimhaltungsgrad, offene Nachricht.

Geheime Verschlußsache (GVS) s. Geheimhaltungsgrad

Geheimeinheit
Einheit des Geheimtextes.

Geheimelement
Element eines Geheimtextes.
+ Chiffreelement, Codeelement, Grundelement.

Geheimelementebereich
Menge der voneinander verschiedenen Geheimelemente, die für ein Chiffrierverfahren zugelassen sind.

Geheimelementevorrat
Anzahl der Geheimelemente eines Geheimelementebereiches.

Geheimhaltung
Bewahrung von Geheimnissen vor unbefugter Offenbarung.
+ Geheimnisschutz, Sicherungstechnik.

Geheimhaltungsgrad
Kennzeichnung von Staats- und Dienstgeheimnissen nach ihrer Be-

deutung. Staatsgeheimnisse werden als GVS (Geheime Verschlußsache, höchster Geheimhaltungsgrad für Staatsgeheimnisse) oder VVS (Vertrauliche Verschlußsache), Dienstgeheimnisse als VD (Vertrauliche Dienstsache) oder NfD (Nur für den Dienstgebrauch, niedrigster Geheimhaltungsgrad) gekennzeichnet.
Von dem Geheimhaltungsgrad ist der Sicherheitsgrad des anzuwendenden Chiffrierverfahrens abhängig. Z. B. dürfen GVS nur mit Schlüsselverfahren chiffriert werden.

Geheimhaltungsstufe svw. Geheimhaltungsgrad

Geheimkomponente s. Substitution

Geheimmischtext
Geheimtext, der aus Geheimeinheiten verschiedener Chiffrierverfahren besteht.
+ Chiffremischtext, Codemischtext.

Geheimnisschutz
Staatliches und gesellschaftliches System, dessen Aufgabe der umfassende Schutz von Staats- und Dienstgeheimnissen gegen die Angriffe des Gegners und gegenüber Unbefugten ist.
Das Chiffrierwesen ist ein Teilsystem des Geheimnisschutzes.

Geheimnisse
Bedeutsame, nicht offenkundige Kenntnisse oder Gegenstände, deren Offenbarung gegen das Interesse von Personen, Personengruppen, Einrichtungen usw. verstoßen würde.
Geheimnisse, deren Wahrung im Interesse des Staates liegt, werden nach ihrer Bedeutung in die Geheimnisarten + Staatsgeheimnis und + Dienstgeheimnis eingeteilt.

Geheimnisträger
Personeller oder sachlicher Träger von Staats- oder Dienstgeheimnissen.

Geheimnisverletzung s. unbefugte Offenbarung

Geheimnisverrat s. unbefugte Offenbarung

Geheimnisverwahrung
Sicherung von gegenständlichen Geheimnissen gegen unbefugte Offenbarung durch organisatorische und technische Maßnahmen.
+ Sicherungstechnik.

Geheimschreibmittel
Die bei (chemischen) Geheimschreibverfahren zur Anwendung kom-

menden speziellen, der Geheimhaltung unterliegenden Mittel, die zur Erzeugung unsichtbarer Schriften und ihrer Sichtbarmachung dienen. Dazu gehören + Geheimtinten, Kopierpapiere, Schreibstifte u. a., die aus einer + Geheimschreibsubstanz bestehen oder mit ihr präpariert sind.

Geheimschreibsubstanz
Substanz, die zur Erzeugung unsichtbarer Schriften dient.

Geheimschreibverfahren
1. Gedecktes Verfahren, bei dem mit Hilfe einer + Geheimschreibsubstanz ein unsichtbarer Geheimtext erzeugt wird, der erst nach besonderer Behandlung wieder sichtbar wird.
2. svw. Chiffrierverfahren.

Geheimschrift
1. svw. unsichtbare Schrift.
2. svw. schriftlicher Geheimtext.

Geheimsignaltafel
Signaltafel zur Übermittlung geheimer Signale.
+ Offensignaltafel.

Geheimtext
Text, der durch Anwendung eines Chiffrierverfahrens auf einen Grundtext entstanden ist.
Nach der Art des angewandten Verfahrens werden unterschieden:
- + Schlüsseltext, + Tarntext und + Verschleierungstext;
- + Chiffretext und + Codetext;
- + offener und + gedeckter Geheimtext.

+ Geheimmischtext.

Geheimtextlochstreifen
Lochstreifen, der Geheimtext in Form von Lochkombinationen enthält.

Geheimtinte
Flüssigkeit, die zur Erzeugung unsichtbarer Schriften dient.

Geheimvorrat
Anzahl der Geheimeinheiten eines Geheimbereiches.

Geländezahl
Deckzahl für einen Kartenpunkt.

Geltungsdauer (eines Schlüssels oder einer Schlüsselserie)
Festgelegte Zeitspanne, innerhalb deren ein Schlüssel oder eine

Schlüsselserie benutzt werden darf, z. B. eine Stunde, 24 Stunden, ein Monat.
+ Geltungszeitraum.

Geltungszeitraum (eines Schlüssels oder einer Schlüsselserie)
Nach Datum und Uhrzeit festgelegter Zeitraum, während dessen ein Schlüssel oder eine Schlüsselserie zu benutzen ist, z. B. am 31. 5. 1971, 12.00–18.00 Uhr.
+ Geltungsdauer.

geringe Sicherheit s. Sicherheit

gesicherte Leitung
Leitung, die gegen das Abhören durch unbefugte Personen abgesichert ist.
Als gesicherte Leitungen gelten Leitungen, die vollständig überwacht werden oder die mit technischen Mitteln so abgesichert sind, daß der Versuch des Abhörens durch unbefugte Personen nur bei großem technischen Aufwand unbemerkt bleiben kann.

gesicherter Codegruppenbereich
Codegruppenbereich, dessen Codegruppen so ausgewählt sind, daß die Erkennung und unter Umständen auch die Berichtigung bestimmter Verstümmelungen möglich ist.
Zum Beispiel wird bei bidifferent-tauschfreien Codegruppen eine einfache Verstümmelung in der Regel als Verstümmelung erkannt; aber sie kann nicht in jedem Fall berichtigt werden, und es wird auch nicht in jedem Fall erkannt, ob es sich um eine einfache oder mehrfache Verstümmelung handelt.
+ bidifferenter, bidifferent-tauschfreier, tridifferenter Codegruppenbereich.

Gitter
Raster, der in Arbeitsfelder und Sperrfelder eingeteilt ist.
In die ARBEITSFELDER werden Elemente eingetragen, in die SPERRFELDER nicht.

Gitternetzverfahren
Verfahren der Kartencodierung, bei dem die offenen Kartenkoordinaten mit Hilfe eines einfachen Tauschverfahrens durch andere Ziffern ersetzt werden.

Gitterverfahren
Rasterverfahren, bei dem ein + Gitter als Raster verwendet wird.

gleichstelliger Code
Code, dessen Codegruppen alle die gleiche Länge haben.
+ wechselstelliger Code.

gleichstelliges Verfahren
Chiffrierverfahren, dessen Geheimeinheiten alle die gleiche Länge haben.
+ wechselstelliges Verfahren.

Großquadratverfahren
Verfahren der Kartencodierung, bei dem jeweils neun Planquadrate zu Großquadraten zusammengefaßt und diese unsystematisch numeriert werden. Die Planquadrate können nach dem +Neunersystem weiter unterteilt werden.

Grundalphabet
Die Grundelemente eines Grundelementebereiches in bestimmter Reihenfolge.

Grundbereich
Menge der voneinander verschiedenen Grundeinheiten, auf die ein bestimmtes Chiffrierverfahren anwendbar ist.

Grundeinheit
Einheit des Grundtextes.

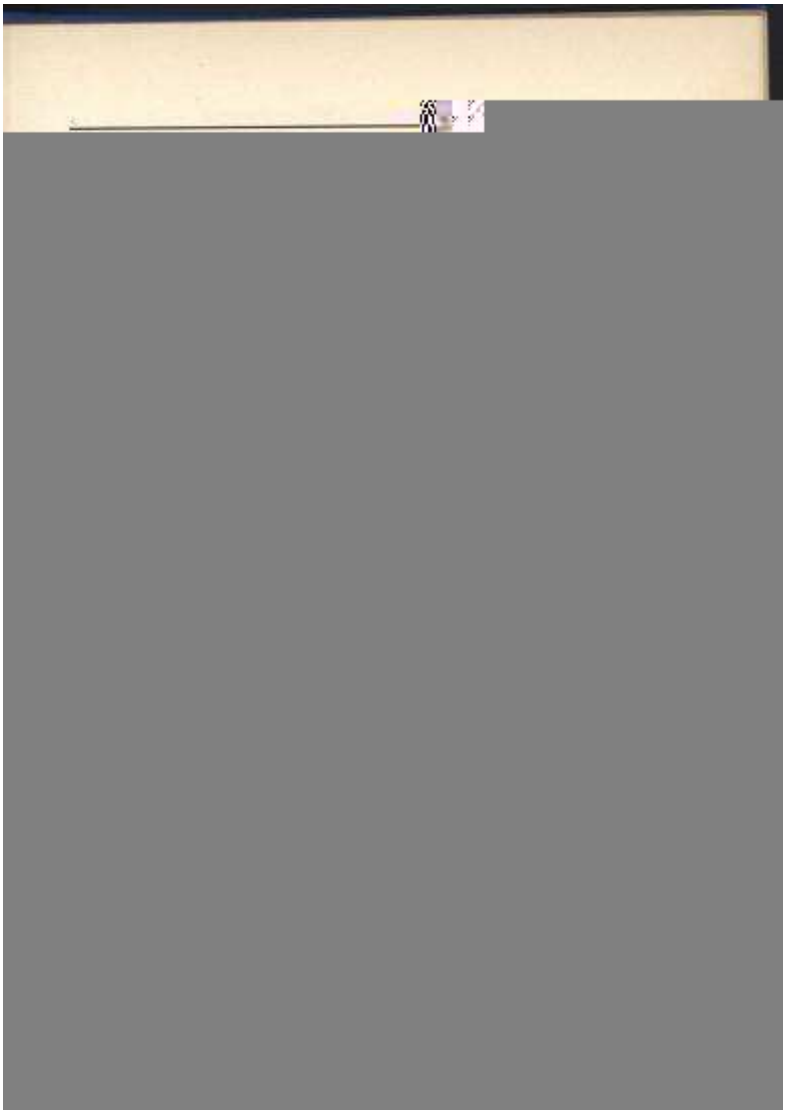
Grundelement
Element eines Grundtextes

Grundelementebereich
Menge der voneinander verschiedenen Grundelemente, auf die ein bestimmtes Chiffrierverfahren anwendbar ist.

Grundelementevorrat
Anzahl der Grundelemente eines Grundelementebereiches.

Grundtext
Text, auf den ein bestimmtes Chiffrierverfahren unmittelbar angewandt werden kann, der also nur solche Einheiten enthält, die für dieses Verfahren zugelassen sind. Der Grundtext kann Klartext, hergerichteter Klartext, Codetext oder selbst schon Geheimtext sein.

Grundtextbereich
Menge der voneinander verschiedenen Grundtexte, auf die ein bestimmtes Chiffrierverfahren anwendbar ist.
Der Grundtextbereich kann endlich oder unendlich sein.



Ideogramm
Zeichen, dem eine bestimmte Bedeutung (ein Begriff, ein Gedanke, ein Gegenstand) unabhängig von deren lautlichem Ausdruck zugeordnet ist.
Beispiele: Hieroglyphen, Zahlzeichen, Satzzeichen, aber auch Codegruppen mehrsprachiger Codes.

Idiom s. Wortfolge

Indikator
Einheit, die eine bestimmte Art oder Bildungsweise des nachfolgenden oder vorangehenden Textes anzeigt, z. B.
- Übergang zu einer anderen Textart (Klartext, Codetext, Substitutionstafeltext, Zifferntext, fremdsprachiger Text u. a.)
- Übergang zu einem anderen Verfahren (vom Hauptverfahren zum Zusatzverfahren u. a.)
- Übergang zu einem anderen Bestandteil des gleichen Verfahrens (andere Stufe bei Codeverfahren, andere Substitution bei Spaltenverfahren u. a.)
- Ersetzung einer grammatischen Form durch eine andere (Einzahl durch Mehrzahl, Vergangenheit durch Gegenwart u. a.).

Spezielle Indikatoren sind:
+ Buchstabiersignal, + Chiffriersignal, + Codiersignal, + Mehrzahlsignal, + Sprachensignal, + Trennzeichen, + Übergangssignal, + Zahlzeichen, + Irrungszeichen, + Fortsetzungsvermerk, + Wiederholungszeichen, Buchstaben- und Ziffernumschaltung bei maschinellen Verfahren.

individueller Text
Text, der in einem individuellen Verkehr übermittelt wird.
+ zirkularer Text.

individueller Verkehr
Chiffrierverkehr zwischen zwei Korrespondenten. Es wird + einseitiger und + zweiseitiger individueller Verkehr unterschieden.

Information
1. Allgemein: Zeichen(-folge), das das beim Empfänger eines gesellschaftlichen Kommunikationssystems bestehende Zeichensystem erweitert bzw. so umstrukturiert, daß die Erkenntnis oder Erkenntnisfähigkeit des Empfängers erweitert oder eine zweckmäßige Handlung ausgelöst wird.

2. Text, der Träger von Erkenntnissen, Weisungen, Erfahrungen, Auffassungen usw. ist. Gleichbedeutend mit VOLLTEXT. Die in einem Text enthaltenen Erkenntnisse usw. stellen seinen INFORMATIONSGEHALT dar.
   + Nachricht.
3. Tätigkeit, die auf die Übermittlung von Information im angeführten Sinne gerichtet ist.

Informationsquelle s. Kommunikationskette

inhomogene Belegung s. Belegung

inhomogener Text s. Text

Internationales Telegrafenalphabet s. Telegrafenalphabet

Internmittel
Chiffriermittel zu Internverfahren.
+ Externmittel.

Internverbindung s. Chiffrierverbindung

Internverfahren
Chiffrierverfahren, das nur von Angehörigen des Chiffrierdienstes angewandt werden darf.

Intervall
Abstand zweier Elemente oder Einheiten in einem Alphabet oder einem Text.

irreguläre Additionsreihe
Irreguläre Folge von Additionseinheiten.

irreguläre Folge
Durch wiederholte Realisierung eines Experimentes mit zufälligen Ausgängen (z. B. Würfeln) entstandene Folge endlicher Länge, wobei für bestimmte Zwecke die Realisierungen hinreichend unabhängig voneinander erfolgen und die verschiedenen Ausgänge hinreichend gleichwahrscheinlich sind.
Irreguläre Folgen sind auf einfache Weise nicht von + absolut irregulären Folgen zu unterscheiden.

irreguläres Additionsverfahren
Additionsverfahren, bei dem eine irreguläre Additionsreihe verwendet wird.
Die irregulären Additionsverfahren werden eingeteilt in + Wurmverfahren und + Mehrfachwurmverfahren.
+ reguläres Additionsverfahren.

Irrungszeichen
Indikator, der einen falschen Textteil anzeigt, z. B. beim Verschreiben.

isomorphe Geheimtexte
Geheimtexte, die mit verschiedenen Schlüsseln oder Verfahren hergestellt wurden, denen aber der gleiche Klartext zugrunde liegt.

isomorphe Substitution
Eineindeutige Substitution, wobei jeder Ausgangseinheit genau eine Ersatzeinheit entspricht und umgekehrt.
+ homomorphe Substitution.

ITA
Abkürzung für Internationales Telegrafenalphabet.

Kanal
Teil einer + Kommunikationskette.

Kanalchiffriergerät
Direktchiffriergerät, das für + Kanalchiffrierung ausgelegt ist.

Kanalchiffriernetz
Netz von mindestens zwei Kanalchiffrierverbindungen.

Kanalchiffrierstelle
Chiffrierstelle, in der eine oder mehrere Kanalchiffrierverbindungen unterhalten werden.

Kanalchiffrierung
Direktchiffrierung über ein zentrales Chiffriergerät mit Anschlußmöglichkeit an mehrere Nachrichtenendgeräte über spezielle teilnehmerseitige Vermittlungen.

Kanalchiffrierverbindung
Chiffrierverbindung, die für Kanalchiffrierung ausgelegt ist.

Kartencodierung
Verschleierung von Orts- und Geländeangaben mit Hilfe bestimmter Verfahren (Methoden) und Mittel. Zu den Verfahren der Kartencodierung gehören das + Kolonnenverfahren, das + Gitternetzverfahren, das + Großquadratverfahren, das + Planquadratverfahren, das + Stoßlinienverfahren, die Verwendung von Deckbezeichnungen für Geländeangaben. Die dabei angewandten Mittel werden als MITTEL DER KARTENCODIERUNG bezeichnet.

Kehralphabet s. Normalalphabet

Kenngruppe
Chiffrierte Schlüsselgruppe.

Kenngruppenabschnitt
Lochstreifenabschnitt, der Kenngruppen in Form von Lochkombinationen enthält.

Kenngruppen-Lochstreifenabschnitt svw. Kenngruppenabschnitt

Kenngruppentafel
Tabelle, die Kenngruppen enthält oder zur Bildung von Kenngruppen dient.

Kennzeichnungsverfahren
Briefverfahren, bei dem die Schriftzeichen, die den Geheimtext bilden, unauffällig gekennzeichnet sind, z. B. durch Punkte, Nadelstiche oder besondere Schreibweise.
+ Einbauverfahren.

Klaralphabet
Die Klarelemente eines Klarelementebereiches in bestimmter Reihenfolge.

Klarbereich
Menge der voneinander verschiedenen Klareinheiten, auf die ein bestimmtes Chiffrierverfahren anwendbar ist.

Klareinheit
Einheit des Klartextes.
+ Phrase.

Klarelement
Element des Klartextes.

Klarelementebereich
Menge der voneinander verschiedenen Klarelemente, auf die ein bestimmtes Chiffrierverfahren anwendbar ist.

Klarelementevorrat
Anzahl der Klarelemente eines Klarelementebereiches.

Klarfolge
Folge von Klarelementen.

Klarkomponente s. Substitution

Klartext
Text, der als solcher keine Elemente beabsichtigter Geheimhaltung

enthält, d. h. auch nicht als Träger eines + gedeckten Geheimtextes dient.
In der Kryptologie oft im Sinne von + Grundtext verwendet.

Klartextlochstreifen
Lochstreifen, der Klartext in Form von Lochkombinationen enthält.

Klarvorrat
Anzahl der Klareinheiten eines Klarbereiches.

Klassifizierung
Zuerkennung einer bestimmten Leistungsklasse auf Grund der Erfüllung bestimmter + Leistungsnormen und der Fähigkeit des Ertragens hoher physischer und psychischer Belastungen bei Vorhandensein guter politisch-moralischer und charakterlicher Eigenschaften.

Kolonnenverfahren
Verfahren der Kartencodierung, bei dem für jede Kolonne (im kartographischen Sinne, d. h. Kartenfeld von 6° Länge in der Breitenausdehnung von Pol zu Pol) eine getrennte Codierung festgelegt ist. In jeder Kolonne ist mindestens ein Ausgangsfeld festgelegt, dessen offene Koordinaten (Hochwert und Rechtswert) durch zwei beliebige dreistellige Zahlen ersetzt werden. Für jedes weitere Kartenfeld wird zu diesen Ausgangswerten ein konstanter Wert addiert oder subtrahiert (je nach Richtung). Zur annähernden Punktbestimmung können die Kartenfelder nach dem + Neunersystem weiter unterteilt werden.

Kombinator
Baugruppe eines Chiffriergerätes, in der die Umwandlung eines vorgegebenen Codes in einen Binärcode realisiert wird.

kombinierter Schlüssel
Schlüssel, dessen Teile in verschiedenen Geltungsarten oder mit verschiedener Geltungsdauer benutzt werden.

kombiniertes Verfahren
Chiffrierverfahren, bei dem nacheinander mindestens zwei wesensverschiedene Chiffrierungen angewandt werden, z. B. Transposition und Substitution oder Codeverfahren und Chiffreverfahren oder offenes und gedecktes Verfahren.

Kommunikation
1. Allgemein: Austausch von Informationen zwischen dynamischen Systemen.
2. Speziell: Austausch von Informationen (Nachrichten) zwischen Menschen.

+ Kommunikationskette.

Kommunikationskette
Folge von Systemen, zwischen denen ein Austausch von Informationen durch Signale erfolgt. Dazu gehören die INFORMATIONSQUELLE (das System, das die Informationen erzeugt), der SENDER (das System, das die Informationen in Form von Signalen emittiert), der KANAL (das System, das die Signale vom Sender zum Empfänger überträgt), der EMPFÄNGER (das System, das die übertragenen Signale aufnimmt) und die SENKE (das System, das die empfangenen Informationen auswertet).
Im Fernmeldewesen wird eine Kommunikationskette, die mindestens aus Sender, Kanal und Empfänger besteht, als FERNMELDETECHNISCHES SYSTEM bezeichnet.

Komponente s. Substitution

Kompromittierung von Chiffrierunterlagen
Kompromittierung (Bloßstellung) von Chiffrierunterlagen liegt vor, wenn unbefugte Personen infolge von Verlust, Diebstahl, Einsichtnahme, Mithören, Kopieren, Auffangen der Abstrahlung von Technik, Verrat, Verstoß gegen die Gebrauchsanweisung, unkontrollierter Beschädigung des Siegels oder der Verpackung, unbeaufsichtigtem Liegenlassen oder aus anderen Gründen vom Inhalt der Chiffrierunterlagen Kenntnis erhalten haben oder erhalten haben könnten.

Konferenzbetrieb
Nachrichtenaustausch innerhalb einer ausgewählten Gruppe von Endstellen, wobei abwechselnd jede von ihnen an alle anderen zugleich senden kann.

Konspiration
Geheimhaltung der Ziele, Kräfte, Maßnahmen, Mittel und Methoden einer Tätigkeit oder Bewegung durch Einhaltung bestimmter Verhaltensregeln (Regeln der konspirativen Tätigkeit).

Kontrollgruppe
Gruppe des Geheimtextes, die zur Kontrolle der Kenngruppe, der Richtigkeit übermittelter Codegruppen, der Vollständigkeit des Spruches und dergleichen dient.

Kontrollprogramm
Programm zur Überprüfung für die Chiffrierung wichtiger Funktionen eines Chiffriergerätes.
+ Prüfprogramm.

Kontrollschlüssel
Schlüssel, der zur Funktionskontrolle eines Chiffriergerätes benutzt wird.

Kontrollstreifen
Schlüssellochstreifen eines Kontrollschlüssels.

Kontroll- und Sicherungsvorrichtungen
Vorrichtungen an Chiffriergeräten, die den Ausfall bestimmter Geräteteile, fehlerhafte Bedienung oder fremde Zeichen im Lochstreifen signalisieren, z. B. durch Auslösung von Stopp, Aufleuchten oder Erlöschen von Kontrollampen.

Kontrollzone
Sperrzone um ein Chiffriergerät zum Schutz gegen unbefugte Einsichtnahme und die Auswertung von Abstrahlungen.

Korrespondent
Teilnehmer eines Nachrichtenverkehrs.
+ Chiffrierkorrespondent.

Kryptanalysis
Teil der Kryptologie, der sich mit der Analyse der Chiffrierverfahren und den Mitteln und Methoden zu ihrer Lösung ohne vorherige Kenntnis des Verfahrens oder des Schlüssels befaßt.
+ Frequenzanalysis

Kryptanalytiker
Person, die wissenschaftliche Arbeit auf dem Gebiet der Kryptanalysis leistet.

Kryptogramm
1. Zur Übermittlung fertiggestellter bzw. übermittelter Geheimtext.
2. svw. Geheimtext.

Kryptograph
Person, die wissenschaftliche Arbeit auf dem Gebiet der Kryptographie leistet.

Kryptographie
Teil der Kryptologie, der sich mit der Entwicklung, Herstellung und Anwendung der Chiffrierverfahren befaßt.

kryptographische Addition
Verknüpfung einer Grundeinheit mit einer Additionseinheit zu einer Geheimeinheit nach einer für alle Elemente des Grundbereichs und des Additionsbereichs definierten vorgegebenen Vorschrift, die eine

eindeutige Umkehrung (Verknüpfung einer Geheimeinheit mit einer Additionseinheit zu einer Grundeinheit) zuläßt.

kryptographisches Element svw. Element

Kryptologe
Person, die wissenschaftliche Arbeit auf dem Gebiet der Kryptologie leistet.

Kryptologie
Wissenschaft von den Chiffrierverfahren.
+ Kryptanalysis, Kryptographie.

kryptologische Sicherheit svw. Sicherheit

Kurzcode
Code geringeren Umfanges (einige Dutzend bis höchstens einige tausend Phrasen umfassend).
+ Satzbuch.

Kürzungscode svw. öffentlicher Code

Länge einer Folge s. Folge

Länge eines Alphabetes s. Alphabet

Länge eines Polygrammes s. Polygramm

Länge eines Textes
Anzahl der Elemente, Einheiten oder Gruppen eines Textes (bei Geheimtexten meist als Anzahl der Fünfergruppen angegeben).

Langzeitschlüssel
Teilsystem variabler, aber in der Regel wesentlich länger als andere Schlüsselelemente gültiger Vorschriften und Hilfsmittel, das z. B. bei Kompromittierung von Teilen eines Chiffrierverfahrens oder -gerätes verändert werden kann.
+ Chiffrierverfahren, Schlüssel.

lateinisches Quadrat
Quadratische Matrix der Seitenlänge s, besetzt mit s verschiedenen Elementen, deren jedes in jeder Zeile und jeder Spalte genau einmal vorkommt.

Laut s. Zeichen

leere Redundanz s. Redundanz

Leertext s. Text

Leerwort
Wort ohne Informationsgehalt.

Leistungsklasse
Qualifikationsgrad, der durch Erfüllung bestimmter + Leistungsnormen und den Nachweis bestimmter sonstiger Eigenschaften und Fähigkeiten erworben werden kann.
+ Klassifizierung.

Leistungsnormen
Festlegung der für den Erwerb einer + Leistungsklasse geforderten Leistungen und Fähigkeiten bei der Anwendung bestimmter Verfahren und Mittel.
Die Leistungsnormen liegen über den + Ausbildungs- und + Übungsnormen.

Leitstelle
1. Stelle, die für die Organisation und ordnungsgemäße Durchführung des Chiffrierverkehrs eines oder mehrerer Schlüsselbereiche verantwortlich ist.
2. Stelle, deren Aufgabe die Planung, Organisation, Sicherstellung und Kontrolle von Chiffrierverkehren in Bereichen ohne Chiffrierdienst, aber mit funktionsgebundenen Benutzern von Chiffriermitteln ist.

lexikographisch niedriger
Von zwei Elementefolgen ist diejenige lexikographisch niedriger, die an der ersten nicht übereinstimmenden Stelle das + alphabetisch niedrigere Element hat.

Linienbetrieb s. Lokalbetrieb

Lochband svw. Lochstreifen

Lochkombination
Zusammenfassung von Lochungen, z. B. in einem Lochstreifen, die ein Zeichen darstellt.

Lochstreifen
Datenträger in Form eines Papierstreifens. Er enthält in der Regel eine Führungsspur mit Transportlöchern und eine bestimmte Anzahl, z. B. 5 oder 8, Informationsspuren, in die Lochkombinationen entsprechend dem verwendeten Lochstreifencode parallel gelocht werden.

Lokalbetrieb
1. Betriebsart einer Fernschreibmaschine, bei der das Übertragungsnetz im Gegensatz zum LINIENBETRIEB abgeschaltet ist. Dabei

kann die Fernschreibmaschine zu Übungsschreiben oder, sofern ein Empfangslocher eingebaut ist, zum Herstellen von Lochstreifen benutzt werden.

2. Analoge Betriebsart eines Direktchiffriergerätes, bei der die Chiffrierung (Vorchiffrierung) oder Dechiffrierung unter Abschaltung des Übertragungsnetzes erfolgt.

Lösbarkeit
Ein Chiffrierverfahren ist lösbar, wenn Dekryptiermethoden existieren, mit deren Hilfe Geheimtexte dieses Verfahrens in Grundtext umgewandelt werden können.
+ Dekryptierbarkeit.

Lösung eines Chiffrierverfahrens
Entwicklung von Dekryptiermethoden zu einem Verfahren, mit deren Hilfe ein beliebiger Geheimtext dieses Verfahrens in Grundtext umgewandelt werden kann.
Die Entwicklung von Dekryptiermethoden, mit deren Hilfe Geheimtexte eines Verfahrens nur unter bestimmten zusätzlichen Bedingungen in Grundtext umgewandelt werden können, wird als TEILLÖSUNG EINES CHIFFRIERVERFAHRENS bezeichnet.

manuelle Chiffrierung
Chiffrierung durch Anwendung eines manuellen Verfahrens oder der manuellen Vorschriften und Hilfsmittel eines teilmaschinellen Verfahrens.
+ maschinelle Chiffrierung.

manuelle Chiffrierverbindung s. Chiffrierverbindung

manuelles Chiffriermittel
Alle Chiffriermittel zu manuellen Chiffrierverfahren und die Chiffriermittel zu teilmaschinellen Verfahren, die zur manuellen Anwendung vorgesehen sind.

manuelles Verfahren
Chiffrierverfahren, bei dem ohne Chiffriergeräte chiffriert und dechiffriert wird.
Manuelle Verfahren, bei denen einfache mechanische Chiffriermittel wie z. B. Schieber oder Scheibe angewandt werden, werden auch als MECHANISCHE VERFAHREN bezeichnet.
+ maschinelles Verfahren.

Marinecode
Militärcode, der im Nachrichtenverkehr der Seestreitkräfte angewandt wird.

maschinelle Chiffrierung
Chiffrierung durch Anwendung eines maschinellen Verfahrens oder der maschinellen Vorschriften und Hilfsmittel eines teilmaschinellen Verfahrens.
Nach der Textart wird unterschieden zwischen + Schriftchiffrierung + Datenchiffrierung, + Sprachchiffrierung und + Bildchiffrierung, nach der Betriebsart zwischen + Vorchiffrierung und + Direktchiffrierung.
+ manuelle Chiffrierung.

maschinelle Chiffrierverbindung s. Chiffrierverbindung

maschinelles Verfahren
Chiffrierverfahren, bei dem mit Chiffriergeräten chiffriert und dechiffriert wird.
Die maschinellen Verfahren werden nach der zu chiffrierenden Textart eingeteilt in + Schriftchiffrierverfahren, + Sprachchiffrierverfahren und Bildchiffrierverfahren.
+ manuelles Verfahren.

Matrix
System von m mal n Größen, das in einem rechteckigen Schema von m Zeilen und n Spalten angeordnet ist. Die m mal n Größen nennt man die Elemente der Matrix.

Mechaniker für Chiffriertechnik
Chiffriermechaniker, der berechtigt ist, bestimmte Chiffriertechnik, z. B. ein Chiffriergerät, in Baugruppen zu zerlegen, wieder zusammenzubauen und kleinere Fehler selbständig zu beheben.

mechanisches Verfahren s. manuelles Verfahren

Mehrfachbelegung s. Belegung

Mehrfachcode
Code, dessen Zuordnung von Phrasen und Codegruppen in mehreren Anordnungen vorliegt, die entweder zum Codieren oder zum Decodieren dienen.
Je nach Anzahl der Anordnungen werden unterschieden: + Zweifachcode, Dreifachcode usw.
+ Einfachcode.

mehrfaches Tauschverfahren s. Tauschverfahren

Mehrfachtafel
Codetafel, die nach dem Prinzip der Mehrfachcodes aufgebaut ist.
+ Einfachtafel, Stellencodetafel.

Mehrfachwurmverfahren
Irreguläres Additionsverfahren, bei dem die Additionsreihe oder Folgen daraus mehrfach benutzt werden.
+ Wurmverfahren.

mehrsprachiger Code
Code, bei dem die den einzelnen Codegruppen zugeordneten Phrasen in zwei oder mehr Sprachen abgefaßt sind.
Nach der Anzahl der verschiedenen Sprachen wird unterschieden zwischen zweisprachigen, dreisprachigen Codes usw., nach den Sprachen selbst zwischen deutsch-russischen, russisch-polnisch-deutschen Codes usw.
+ einsprachiger Code.

mehrstufiger Code
Code, bei dem mindestens einer Codegruppe mehr als eine Phrasenstelle zugeordnet ist. Je nach Anzahl der zugeordneten Phrasenstellen handelt es sich um einen zweistufigen, dreistufigen Code usw.
+ einstufiger Code, Stellencode.

Mehrstufigkeit
Zuordnung von mehr als einer Phrasenstelle zu einer Codegruppe in einem Code.
Jede dieser Zuordnungen wird als + Stufe bezeichnet.

Mehrzahlsignal
Indikator, der anzeigt, daß von einer bestimmten Phrase die Mehrzahl zu bilden ist.

Menge
Zusammenfassung bestimmter, wohlunterschiedener Objekte (Elemente unserer Anschauung oder unseres Denkens) zu einem Ganzen.

Mikratverfahren
Gedecktes Verfahren, bei dem der Text zum Zwecke der Verbergung fotografisch extrem verkleinert wird.

Militärcode
Code, der im militärischen Nachrichtenverkehr angewandt wird.
+ Marinecode.

Mindestsicherheit
Sicherheitsgrad, der als Minimum gefordert oder garantiert wird.

Mischalphabet
Alphabet, in dem die Zeichen nicht in der gewöhnlichen oder genau umgekehrten Reihenfolge stehen.
+ Standardalphabet.

Mischcode
Code, dessen Codeelemente Buchstaben und Ziffern sind.

Mischgruppe s. Gruppe

Mischtext
Text, der teils aus Klartext, teils aus Geheimtext besteht.

Mischverfahren
Chiffrierverfahren, dessen Geheimelemente Buchstaben und Ziffern sind.
+ Buchstabenverfahren, Ziffernverfahren, steganographisches Verfahren.

Mitarbeiter des Chiffrierdienstes
Person, die in einem Chiffrierdienst tätig ist.
Mitarbeiter des Chiffrierdienstes gelten als + Geheimnisträger und unterliegen den für diese geltenden Bestimmungen. Nach dem Umfang ihrer Tätigkeit im Chiffrierdienst wird zwischen + hauptamtlichen und + nebenamtlichen Mitarbeitern des Chiffrierdienstes, nach ihrer Tätigkeitsrichtung zwischen + Chiffreuren, + Chiffriermechanikern u. a. unterschieden.

Mitlesen
Dekryptieren bei Kenntnis der angewandten Chiffriermittel.

Mittel der gedeckten Führung svw. Chiffriermittel

Mittel der Kartencodierung s. Kartencodierung

mittlere Sicherheit s. Sicherheit

Monatsschlüssel s. Zeitschlüssel

monoalphabetisches Verfahren svw. Tauschverfahren

monographisches Verfahren
Chiffrierverfahren, dessen Grundeinheiten einzelne Elemente sind.
+ polygraphisches Verfahren.

Morsealphabet s. Telegrafenalphabet

motorisierte Chiffrierstation
Kraftfahrzeug, das als mobile Chiffrierstelle eingerichtet ist.

Nachricht
1. svw. Information
2. Information, die im Prozeß der zwischenmenschlichen + Kommunikation auftritt.
+ Spruch.

Nachrichtenbeförderung
Beförderung von Nachrichten, die an Gegenstände gebunden sind (z. B. Briefe) vom Absender zum Empfänger.
+ Nachrichtenübermittlung.

Nachrichtendichte
Nachrichtenmenge innerhalb eines bestimmten Zeitraumes.

Nachrichtenfluß
Verteilung der in einem Nachrichtenverkehr übermittelten Nachrichten nach Zeit, Menge, Inhalt, Korrespondenten usw.

Nachrichtenkanal svw. Kanal

Nachrichtennetz
Zusammenhängendes Netz von Nachrichtenverbindungen. Es kann in Teilnetze zerfallen oder selbst Teilnetz sein.
+ Chiffriernetz.

Nachrichtenstelle
Stelle, in der eine oder mehrere Nachrichtenverbindungen unterhalten werden.

Nachrichtentextformular s. Formularcode.

Nachrichtenübermittlung
Übermittlung von Nachrichten, die nicht an einen Gegenstand gebunden sind (z. B. Ferngespräche, Fernschreiben, Telegramme), mit Fernmeldeanlagen.
+ Nachrichtenbeförderung.

Nachrichtenverbindung
Verbindung zur Übermittlung von Nachrichten zwischen zwei Korrespondenten.
+ Chiffrierverbindung, Nachrichtennetz.

Nachrichtenverkehr
Austausch von Nachrichten zwischen dafür zuständigen Stellen.
+ Chiffrierverkehr, Kommunikation, Korrespondent.

nebenamtlicher Mitarbeiter des Chiffrierdienstes
Person, die eine Hauptfunktion außerhalb des Chiffrierdienstes ausübt und zusätzlich als Mitarbeiter des Chiffrierdienstes tätig ist.
+ hauptamtlicher Mitarbeiter des Chiffrierdienstes.

Neunersystem
Methode zur Einteilung von Quadraten in jeweils neun kleinere Quadrate, die in bestimmter Reihenfolge numeriert sind, z. B.
1 2 3
8 9 4
7 6 5
Das Neunersystem dient bei der Kartencodierung zur genaueren Bestimmung von Kartenpunkten.

Neunerunterteilung svw. Neunersystem

NfD s. Geheimhaltungsgrad

nichtüberschlüsselter Code
Code, der als Chiffriermittel dient, wobei der Codetext zugleich Geheimtext ist und als solcher übermittelt wird.
+ Schlüsselcode.

Normalalphabet
Gesamtheit der Buchstaben eines Schriftsystems in der gewöhnlichen Reihenfolge, insbesondere die 26 Buchstaben des lateinischen Alphabetes in der Reihenfolge
a b c d e f g h i j k l m n o p q r s t u v w x y z.
Die Umkehrung des Normalalphabetes z y x . . . c b a wird als KEHRALPHABET bezeichnet. Der Rang eines Buchstabens im Normalalphabet wird als dessen NORMALRANG bezeichnet, z. B. hat der Buchstabe f den Normalrang 6.

Normalfrequenz
Grenzwert der relativen Frequenz eines Ereignisses bei stetiger Erweiterung des untersuchten Textes.

Normalrang s. Normalalphabet

Notverfahren
Chiffrierverfahren, das bei Ausfall des Hauptverfahrens angewandt wird.
Im Gegensatz zu Behelfsverfahren dienen als Notverfahren oft Chiffrierverfahren, die keine geringere Sicherheit als das Hauptverfahren besitzen.
Beispiel: Überlagerung eines maschinellen mit einem manuellen Schlüsselverfahren, das bei Ausfall der Chiffriertechnik als Notverfahren dient.

numerische Daten s. Daten

Nur für den Dienstgebrauch (NfD) s. Geheimhaltungsgrad

offene Nachricht
Nachricht, die nicht als + geheime Nachricht klassifiziert ist.

offener Geheimtext
Geheimtext, der durch Anwendung eines offenen Verfahrens entstanden ist und demnach ohne weiteres als Geheimtext erkennbar ist.
+ gedeckter Geheimtext.

offener Kanal
Kanal, der nicht + Chiffrierkanal ist (unabhängig davon, in welchem Maße über ihn chiffrierte Nachrichten übermittelt werden).

offener Text svw. Klartext

offenes Verfahren
Chiffrierverfahren, bei dessen Anwendung ein offener Geheimtext erzeugt wird.
+ gedecktes Verfahren.

Offensignaltafel
Signaltafel zur Übermittlung offener Signale.
+ Geheimsignaltafel.

öffentlicher Code
Code, der nicht der Geheimhaltung unterliegt.
Öffentliche Codes können auch in Verbindung mit Chiffrierverfahren als Mittel der Textkürzung und Zwischentextbildung dienen, ohne selbst Chiffriermittel zu sein.
+ Geheimcode.

off-line-Chiffrierung svw. Vorchiffrierung

on-line-Chiffrierung svw. Direktchiffrierung

Ordnungswort
Wort, unter dem eine Wortfolge im Phrasenverzeichnis eingeordnet wird.

Als Ordnungswörter werden in der Regel verwendet:

a) das erste Wort der Wortfolge,

b) das Stichwort, d. h. wesentlichste Wort der Wortfolge,

c) ein Schlagwort, d. h. ein Begriff, der einen engeren oder weiteren Sachinhalt bezeichnet.

Beispiel: Die Wortfolge „leichtes Maschinengewehr" wird eingeordnet unter „leichtes" (erstes Wort), „Maschinengewehr" (Stichwort), „Infanteriewaffen" (engeres Schlagwort) oder „Waffen und Geräte" (weiteres Schlagwort).

Parallelstelle
Wiederholung eines Ereignisses in einem Text oder in verschiedenen Texten, die bestimmten gleichen Bedingungen unterliegen. In der Praxis werden unter Parallelstellen hauptsächlich Wiederholungen von Polygrammen verstanden. Das sich wiederholende Polygramm wird als CHARAKTERISTISCHES POLYGRAMM bezeichnet.

Pentagramm s. Polygramm

periodische Additionsreihe
Additionsreihe, in der sich mindestens eine Teilfolge der Additionselemente periodisch wiederholt. Eine spezielle Form der periodischen Additionsreihen ist die REINPERIODISCHE ADDITIONSREIHE, die durch ständige Wiederholung einer Folge von Additionselementen entsteht.

periodische Additionsverfahren
Additionsverfahren, bei dem eine periodische Additionsreihe verwendet wird.
Eine spezielle Form der periodischen Additionsverfahren ist das REINPERIODISCHE ADDITIONSVERFAHREN, bei dem eine reinperiodische Additionsreihe benutzt wird.

Pflichtenfestlegung s. Anwendungsbedingungen

phasengleiche Geheimtexte
Geheimtexte, die stückweise mit der gleichen Substitutionsreihe gebildet wurden.

Phrase
Grundeinheit bei Codeverfahren.
Phrasen sind im allgemeinen von unterschiedlicher Länge und Beschaffenheit, z. B. Buchstaben, Ziffern, Satzzeichen, Polygramme, Wörter und Wortfolgen, Sätze und Satzfolgen.

Phrasenbestand
Anzahl der in einem Code mit Phrasen besetzten Phrasenstellen.
+ eigentlicher Phrasenbestand.

Phrasencode
Code, in dem außer den Codegruppen auch die Phrasen eingetragen sind.
Der Begriff Phrasencode wird im allgemeinen anstelle des einfachen Begriffes Code nur dann verwendet, wenn der Gegensatz zu einem + Blankocode hervorgehoben werden soll. Die Phrasencodes werden eingeteilt in + einfache Phrasencodes und + Formularcodes.

Phrasenstelle
Stelle in einem Code, an der innerhalb einer Stufe eine Phrase oder auch mehrere gegeneinander austauschbare Phrasen untergebracht werden können.
+ Freistelle.

Phrasenstreifen
Streifen, der mit Phrasen beschriftet ist, z. B. bei Codetafeln.
+ Schlüsselstreifen.

Phrasentafel
Der Teil einer Codetafel, in dem die Phrasen stehen.

Phrasenteil svw. Phrasenverzeichnis

Phrasenverzeichnis
Der Teil eines Codes, der die Phrasen enthält.

Phrasenvorrat
Gesamtzahl der Phrasenstellen eines Codes, die bei gegebenem Codegruppenvorrat unter Berücksichtigung der Belegung und der Anzahl der Stufen möglich ist.

Phrasenzeile svw. Phrasenstreifen.

Planquadratverfahren
Verfahren der Kartencodierung, bei dem die Planquadrate in unsystematischer Weise numeriert sind, wodurch in der Regel auch ein Decodierteil erforderlich wird.

polyalphabetisches Verfahren svw. Spaltenverfahren

Polygramm
Zusammenfassung von zwei oder mehr unmittelbar aufeinanderfolgenden Elementen, die in bestimmter Hinsicht als Einheit betrachtet werden.
Nach der Anzahl der Elemente (LÄNGE DES POLYGRAMMS) werden unterschieden: BIGRAMM (Länge 2), TRIGRAMM (Länge 3), TETRAGRAMM (Länge 4), PENTAGRAMM (Länge 5) usw.
+ Gruppe.

polygraphisches Verfahren
Chiffrierverfahren, dessen Grundeinheiten aus zwei oder mehr Elementen bestehen.
+ monographisches Verfahren.

Polyphone
Verschiedene Geheimeinheiten, denen die gleiche Klareinheit zugeordnet ist, z. B. bei Mehrfachbelegung.
+ Homophon.

Post- und Fernmeldegeheimnis
Pflicht für Mitarbeiter und Beauftragte der Post, den Inhalt von Postsendungen und Nachrichten geheimzuhalten.
+ Funkgeheimnis.

Primalphabet
Alphabet, das aus einem vorgegebenen Alphabet der Länge n entsteht, wenn aus diesem nur immer das k-te Zeichen (k zu n teilerfremd) genommen wird und die herausgenommenen Zeichen weiter mitgezählt werden.
Beispiel: Das 3. Primalphabet zum Normalalphabet ist
c f i l o r u x a d g j m p s v y b e h k n q t w z.
+ Dezimationsalphabet.

Privatcode
Code, der im privaten Nachrichtenverkehr angewandt wird.

Produktionsfehler s. Verstümmelung

Programm
Festgelegter Ablauf von Arbeitsgängen.

Prüfprogramm
Programm für die Überprüfung sämtlicher Funktionen eines Chiffriergerätes.
+ Kontrollprogramm.

Q-Code
International vereinbarter Code des Funkverkehrs, der als Phrasen häufig vorkommende Betriebsmitteilungen, Fragen und Antworten enthält, denen als Codegruppen dreistellige Buchstabengruppen zugeordnet sind, deren erster Buchstabe durchweg das beim Morsen leicht erkennbare Q ist, z. B. QSL = Empfangsbestätigung. Die Codegruppen werden als Q-GRUPPEN bezeichnet.

Q-Gruppe s. Q-Code

quasiabsolute Sicherheit s. Sicherheit

Rang eines Elementes s. Alphabet

Raster
Geometrische Figur, die zur Ausführung einer Transposition dient. Die häufigste Form des Rasters ist das Rechteck; seltener treten Kreis, Dreieck, Trapez oder andere Figuren auf.
+ Gitter, Matrix.

Rasterverfahren
Transpositionsverfahren, bei dem die Transposition mit Hilfe eines + Rasters erfolgt. Zu den Rasterverfahren gehören die + Würfelverfahren, die + Feldertranspositionsverfahren und die + Gitterverfahren.

Räume des Chiffrierwesens
Räume, die für bestimmte Zwecke des Chiffrierwesens genutzt werden und in der Regel bestimmten Sicherungsvorschriften entsprechen müssen. Dazu gehören + Chiffrierräume, Werkstätten für die Produktion von Chiffriermitteln und die Reparatur von Chiffriertechnik, Lagerräume für Chiffriermittel u. a.

Redewendung s. Wortfolge

Redundanz
Der Teil einer Information, der keine Information trägt und daher weggelassen werden könnte, ohne daß ein Informationsverlust einträte.
Es ist zu unterscheiden zwischen FORDERNDER REDUNDANZ, die dazu dient, bei Ausfall von Teilen der Information die ursprüngliche Information wiederherzustellen, z. B. bei + gesicherten Codegruppenvorräten, und LEERER REDUNDANZ, die nicht diesem Zweck dient.

reduziertes Alphabet
Alphabet, das aus einem vorgegebenen Alphabet durch Weglassung mindestens eines Zeichens entsteht.

reguläre Additionsreihe
Additionsreihe, die nicht die Bedingung der + irregulären Additionsreihe erfüllt.
Die regulären Additionsreihen werden nach ihrer kryptologischen Beschaffenheit eingeteilt in + periodische Additionsreihen und + unperiodische Additionsreihen.

reguläres Additionsverfahren
Additionsverfahren, bei dem eine reguläre Additionsreihe benutzt wird.
Die regulären Additionsverfahren werden nach der mathematisch-

kryptologischen Beschaffenheit der benutzten Additionsreihen eingeteilt in + periodische Additionsverfahren und + unperiodische Additionsverfahren.

reinperiodische Additionsreihe s. periodische Additionsreihe
reinperiodisches Additionsverfahren s. periodisches Additionsverfahren

rekurrentes Verfahren
Unperiodisches Additionsverfahren, bei dem die auf den + Eingangsschlüssel folgenden Substitutionen von den vorangegangenen Klareinheiten, Geheimeinheiten oder Substitutionen abhängig sind.

relative Frequenz
Prozentuale Frequenz eines Ereignisses, z. B. Anzahl des Auftretens des Buchstaben A bezogen auf 100 Buchstaben eines Textes.

Reparaturdienst
Einrichtung des Chiffrierwesens, deren Aufgabe die Reparatur und Wartung von Chiffriertechnik in einem bestimmten Bereich ist.

reziproke Alphabete
Zwei Alphabete des gleichen Elementebereiches, zwischen denen folgende Beziehung besteht: Haben die Elemente E_i im ersten und E_k im zweiten Alphabet den gleichen Rang, so haben auch die Elemente E_k im ersten und E_i im zweiten Alphabet den gleichen Rang.

Richtungsbetrieb svw. Simplexbetrieb

Richtungspunkt s. Stoßlinienverfahren

Route
Reihenfolge des Eintragens der Elemente in die Felder eines Rasters oder ihres Ablesens.

Rückfrage
Anfrage der empfangenden Nachrichten- oder Chiffrierstelle bei der absendenden Nachrichten- oder Chiffrierstelle zwecks Klärung eines nicht verstandenen Textteiles oder Spruches.
Im Chiffrierverkehr gelten zum Schutz gegen Kompromittierung für Form und Inhalt von Rückfragen und Rückantworten bestimmte Vorschriften.

Satzbuch
Code größeren Umfanges (einige tausend bis einige hunderttausend Phrasen umfassend).
+ Kurzcode.

Scheibe
Mechanisches Hilfsmittel zur Durchführung einer Substitution, wobei die Komponenten kreisförmig gegeneinander drehbar sind.
+ Schieber.

Schemaspruch
Spruch in festgelegter Form und/oder Reihenfolge der Teile.
+ Formularcode.

Schieber
Mechanisches Hilfsmittel zur Durchführung einer Substitution, wobei die Komponenten geradlinig gegeneinander verschiebbar sind.
+ Scheibe.

Schiffahrtscode
Verkehrscode, der im Nachrichtenverkehr der Schiffahrt angewandt wird.

Schlüssel
Vollständiges Teilsystem der zur Chiffrierung eines Textes notwendigen variablen Vorschriften und Hilfsmittel eines Chiffrierverfahrens.
Nach der Geltungsart werden unterschieden: + Textschlüssel, + Zeitschlüssel, + Zeittextschlüssel und + kombinierter Schlüssel.
+ Chiffrierverfahren, Schlüsselunterlagen.

Schlüsselbereich
Gesamtheit der gleichzeitigen Benutzer der gleichen Schlüsselunterlagen zum gleichen Verfahren.

Schlüsselcode
Code, der als Chiffriermittel dient, wobei der Codetext nur Zwischentext ist, der erst nach Überschlüsselung mit einem Chiffreverfahren zum Geheimtext wird.
Als Schlüsselcodes können nicht nur Geheimcodes, sondern auch öffentliche Codes verwendet werden, wenn die geforderte Sicherheit durch das zur Überschlüsselung benutzte Verfahren allein gewährleistet wird.
+ nichtüberschlüsselter Code.

Schlüsseleinstellung
Einstellung bzw. Zusammenstellung der Schlüsselelemente eines Schlüssels zu einem bestimmten Schlüssel.
+ Einstellgruppe.

Schlüsselelement
Bestandteil eines Schlüssels.

Schlüsselgerät
Chiffriergerät, das eine Geheimhaltung bearbeiteter Nachrichten für einige Tage bis unbegrenzte Zeit gewährleistet.

schlüsselgleiche Geheimtexte
Geheimtexte, die durch Anwendung des gleichen Schlüssels entstanden sind.

Schlüsselgruppe
Gruppe, die den verwendeten Schlüssel oder Teile davon anzeigt.
+ Kenngruppe.

Schlüsselgruppentafel
Tabelle, die Schlüsselgruppen enthält oder zur Bildung von Schlüsselgruppen dient.

Schlüsselheft
Heftförmig verpackte Schlüsselunterlagen, z. B. Wurmtabellenheft, Schlüssellochstreifenheft.
Ein Schlüsselheft, das zur Chiffrierung dient, wird als AUSGANGSHEFT, eines, das zur Dechiffrierung dient, als EINGANGSHEFT bezeichnet.

Schlüsselkassette
Kassette, die zur Aufnahme von Schlüsselunterlagen dient.
Eine Schlüsselkassette, die zur Chiffrierung dient, wird als AUSGANGSKASSETTE, eine, die zur Dechiffrierung dient, als EINGANGSKASSETTE bezeichnet.

Schlüssellochkarte
Lochkarte, die einen Schlüssel oder Teile davon enthält.

Schlüssellochstreifen
Lochstreifen, der Schlüssel oder Teile davon in Form von Lochkombinationen enthält.
Der Schlüssellochstreifen kann in Abschnitte (SCHLÜSSELLOCHSTREIFENABSCHNITTE) eingeteilt sein, die durch + Aufdruckmarkierungen gekennzeichnet sind.

Schlüssellochstreifenabschnitt s. Schlüssellochstreifen

Schlüssellochstreifenheft
Schlüssellochstreifen in Verpackung aus Papier, Karton oder Weichplaste.

Schlüssellochstreifenkassette
Kassette, die zur Aufnahme von Schlüssellochstreifen dient.

Schlüsselmittel
Chiffriermittel zu Schlüsselverfahren.

schlüsseln s. Schlüsselung

Schlüsselreihe
Elementefolge, die als Schlüssel oder zur Bildung eines Schlüssels dient. Besteht sie aus einem Wort, so wird sie als SCHLÜSSELWORT bezeichnet; besteht sie aus einer Ziffernfolge, so wird sie als SCHLÜSSELZAHL bezeichnet; besteht sie aus einer Wortfolge oder einem Satz, so wird sie als SCHLÜSSELSATZ bezeichnet.

Schlüsselrekonstruktion
Bestimmung vollständiger Schlüssel, einzelner Schlüsselelemente oder äquivalenter Schlüssel eines Chiffrierverfahrens mit Hilfe von Methoden der Kryptanalysis.

Schlüsselsatz s. Schlüsselreihe

Schlüsselscheibe
Scheibenförmiger Bauteil eines Chiffriergerätes, der als Schlüsselelement dient.
+ Scheibe, Schlüsselscheibensatz.

Schlüsselscheibenblock
Teil eines Schlüsselscheibensatzes, der aus einer Zusammenfassung mehrerer Schlüsselscheiben besteht.

Schlüsselscheibensatz
Zusammenfassung einer bestimmten Anzahl von Schlüsselscheiben zu einem Schlüsselelement.
+ Schlüsselscheibenblock.

Schlüsselserie
Zusammenfassung einer Anzahl verschiedener Schlüssel, die für den zusammenhängenden Gebrauch im gleichen Anwendungsbereich bestimmt sind.

Schlüsselserienwechsel
Übergang von einer Schlüsselserie zu einer anderen.

Schlüsselstreifen
Streifen, der mit einem Schlüssel oder Teilen davon beschriftet ist, z. B. bei Codetafeln.
+ Phrasenstreifen, Spaltenstreifen, Zeilenstreifen, Tornstreifen.

Schlüsseltabelle
Schlüssel oder Teile davon in Tabellenform.
+ Schlüsseltafel.

Schlüsseltafel
Codetafel, die als Schlüsselmittel dient.

Schlüsseltext
Geheimtext, der durch Anwendung eines Schlüsselverfahrens entstanden ist.

Schlüsseltextverfahren
Transpositionsverfahren, bei dem die Transposition mit Hilfe einer + Schlüsselreihe erfolgt.

Schlüsselung (Infinitiv: SCHLÜSSELN)
Chiffrierung durch Anwendung eines Schlüsselverfahrens.

Schlüsselunterlagen
Unterlagen, die Schlüssel oder Teile von Schlüsseln enthalten.

Schlüsselverbindung s. Chiffrierverbindung

Schlüsselverfahren
Chiffrierverfahren, das eine Geheimhaltung für mehrere Tage bis unbegrenzte Zeit gewährleistet.

Schlüsselvorrat
Anzahl der nach den festgelegten Bildungsgesetzen möglichen Schlüssel zu einem Chiffrierverfahren.
+ effektiver Schlüsselvorrat.

Schlüsselwalze
Schlüsselscheibensatz, der auf einer Achse befestigt ist.

Schlüsselwechsel
Übergang von einem Schlüssel zu einem anderen Schlüssel durch Ersetzung aller bzw. einzelner bisher benutzter Schlüsselelemente durch zum gleichartigen Gebrauch bestimmte neue Schlüsselelemente.

Schlüsselwort s. Schlüsselreihe

Schlüsselzahl s. Schlüsselreihe

Schlüßler s. funktionsgebundener Benutzer

Schriftchiffriergerät
Chiffriergerät, das für die elementeweise Chiffrierung von schriftlichen Texten ausgelegt ist.

Schriftchiffrierung
Maschinelle Chiffrierung schriftlicher Texte.

Schriftchiffrierverfahren
Maschinelles Verfahren zur Chiffrierung schriftlicher Texte.

Schriftzeichen s. Zeichen

Schrittgeschwindigkeit svw. Telegrafiergeschwindigkeit

Schrittgruppe
Impulsfolge, die ein Zeichen darstellt.

Schwierigkeitsfaktor
Gütefaktor zur Bewerwertung der Schwierigkeit der Handhabung eines Chiffrierverfahrens, d. h. der für die Erlernung und ständige Beherrschung des Verfahrens erforderlichen Kenntnisse, Fähigkeiten und Fertigkeiten und des dazu benötigten Zeitaufwandes.

selbständiger Chiffrierdienst s. zentraler Chiffrierdienst.

Sender s. Kommunikationskette

Senke s. Kommunikationskette

Sicherheit eines Chiffrierverfahrens
Mittlerer Widerstand, den die Geheimtexte eines Chiffrierverfahrens der Dekryptierung entgegensetzen. Die Sicherheit ist häufig für verschiedene Sprüche, mitunter sogar für verschiedene Grundeinheiten innerhalb eines Spruches verschieden.
Die Sicherheit ist die wesentlichste Eigenschaft von Chiffrierverfahren; von ihr hängt es ab, in welchem Grade der eigentliche Zweck der Anwendung eines Chiffrierverfahrens, die Geheimhaltung von Information, erfüllt wird.
Bei der Unterscheidung von Sicherheitsgraden wird von folgenden Voraussetzungen ausgegangen:

- Alle Anwendungsvorschriften, die Einfluß auf die Sicherheit haben, werden von den Benutzern streng eingehalten.
- Andererseits verfügt der Dekrypteur über gute Kenntnisse, Erfahrungen und Fähigkeiten auf dem Gebiet der Dekryptierung und alle notwendigen technischen Hilfsmittel; er kennt das angewandte Verfahren und die allgemeine Beschaffenheit der Schlüsselunterlagen, aber nicht die konkret benutzten Schlüsselunterlagen; er besitzt mit dem Verfahren chiffrierte Texte in dem für die Dekryptierung notwendigen Umfang.

Unter diesen Voraussetzungen können folgende SICHERHEITSGRADE unterschieden werden:

(1) ABSOLUTE SICHERHEIT
das Verfahren ist weder theoretisch noch praktisch dekryptierbar;

(2) QUASIABSOLUTE SICHERHEIT
das Verfahren ist theoretisch dekryptierbar, aber diese Möglichkeit ist in der Praxis nicht realisierbar;

(3) HOHE SICHERHEIT
das Verfahren hat die Sicherheit eines weder absolut sicheren noch quasiabsolut sicheren + Schlüsselverfahrens;
(4) MITTLERE SICHERHEIT
das Verfahren hat etwa die Sicherheit eines + Tarnverfahrens;
(5) GERINGE SICHERHEIT
das Verfahren hat etwa die Sicherheit eines + Verschleierungsverfahrens.

Die Begriffe hohe, mittlere und geringe Sicherheit haben nur relativen Charakter. Die Sicherheit von Verfahren dieser Sicherheitsgrade kann je nach Anwendungsvorschriften, z. B. Begrenzung der für einen Schlüssel zugelassenen Textmenge, oder Anwendungsbedingungen, z. B. benutzte Nachrichtenmittel, erheblichen Schwankungen unterliegen.
+ Dekryptierbarkeit, Mindestsicherheit

Sicherheitsbestimmungen (zu Chiffrierunterlagen)
Bestimmungen über den Schutz gegen Kompromittierung und über Maßnahmen bei Kompromittierung von Chiffrierunterlagen.

Sicherheitsfaktor
Faktor zur Bewertung der + Sicherheit eines Chiffrierverfahrens

Sicherheitsgrad s. Sicherheit

Sicherheitsüberprüfung (von Personen)
Überprüfung von Personen, die als Geheimnisträger vorgesehen sind, auf politische, charakterliche und sonstige Eignung.

Sicherungsmittel
Sammelbegriff für alle Mittel, die dazu dienen, Geheimnisse gegen unbefugte Kenntnisnahme, Kopierung, Veränderung, Zerstörung oder Wegnahme zu sichern.
Dazu gehören + Chiffriermittel und + Sicherungstechnik.

Sicherungstechnik
Technische Vorrichtungen, Mittel und Anlagen, die dazu dienen, Gegenstände gegen unbemerkte und unbefugte Einsichtnahme, Kopierung, Veränderung, Zerstörung oder Wegnahme zu sichern. Dazu gehören z. B. Fenstergitter, Sicherheitsschlösser, Panzerschränke, Raumschutzanlagen.

Sicherungsvorrichtung s. Kontroll- und Sicherungsvorrichtungen

Siebeneralphabet s. Telegrafenalphabet

Siebenschrittalphabet s. Telegrafenalphabet

Signal
Materielle Gestalt eines Zeichens.

Signalcode svw. Zeichencode

Signaltafel
Codetafel (in der Regel geringen Umfanges) zur schnellsten Übermittlung einzelner kurzer Signale.
+ Geheimsignaltafel, Offensignaltafel.

Silbenverständlichkeit s. Verständlichkeitsfaktor

Simplexbetrieb
Betriebsweise des Fernmeldeverkehrs und der Datenübertragung, bei der Nachrichten oder Daten in nur einer Richtung übertragen werden.
+ Duplexbetrieb, Halbduplexbetrieb.

Sondersprechtafel
Sprechtafel für eine einmalige Aktion.

Sonderverfahren
Chiffrierverfahren, das anstelle des Hauptverfahrens angewandt wird, wenn bestimmte Nachrichten nur einem enger begrenzten Personenkreis als den Benutzern des Hauptverfahrens zugänglich sein sollen.

Sonderzeichen s. Zeichen

Spaltenstreifen
Horizontaler Schlüsselstreifen bei Codetafeln, der die Spaltenbezeichnungen enthält.
+ Zeilenstreifen.

Spaltentransposition s. Würfelverfahren

Spaltentranspositionsverfahren svw. Würfelverfahren

Spaltenverfahren
Substitutionsverfahren, bei dem die Chiffrierung mittels mehrerer Substitutionen erfolgt.
Zu den Spaltenverfahren gehören u. a. die + rekurrenten Verfahren und die + Additionsverfahren.
+ Tauschverfahren.

Sperrfeld s. Gitter

Sperrzone svw. Kontrollzone

Spezialproduktionstechnik
Spezialtechnik, die für die Produktion von Chiffriermitteln ausgelegt ist.
+ Zufallsgenerator.

Spezialtechnik
Technik, die speziell für Einrichtungen, Maßnahmen und Tätigkeiten des Chiffrierwesens ausgelegt ist, z. B. Chiffriertechnik, Dekryptiertechnik, Spezialproduktionstechnik.

Sprachchiffriergerät
Chiffriergerät, das für die Chiffrierung von gesprochenen Texten ausgelegt ist.

Sprachchiffrierung
Maschinelle Chiffrierung gesprochener Texte.

Sprachchiffrierverfahren
Maschinelles Verfahren zur Chiffrierung gesprochener Texte.

Sprachensignal
Indikator, der den Übergang zu einer anderen Sprache anzeigt.

sprachliches Zeichen s. Zeichen

Sprachtrakt
Die Baugruppe eines Sprachchiffriergerätes, die die Chiffrierung bzw. Dechiffrierung der Sprache realisiert.

Sprechtafel
Codetafel, die zur Verschleierung einzelner geheimzuhaltender Begriffe dient, aber auch mit anderen Verschleierungsmitteln wie Buchstabier- und Zahlentafeln, Decknamen- und Deckzahlenverzeichnissen, Mitteln der Kartencodierung kombiniert sein kann.
+ Sondersprechtafel.

Spruch
Nachricht, die über Fernmeldemittel übermittelt wird.
Der Spruch gliedert sich in der Regel in SPRUCHKOPF (Absender, Empfänger, Datum, Uhrzeit, Dringlichkeitsvermerk u. a.) SPRUCHTEXT (die eigentliche Information) und SPRUCHENDE (weitere Angaben zur Betriebs- und Verkehrsabwicklung).
+ Funkspruch.

Spruchende s. Spruch

Spruchkopf s. Spruch

Spruchlänge
Anzahl der Elemente oder Gruppen (meist Fünfergruppen) eines Spruches.

Spruchschlüssel s. Textschlüssel

Spruchtext s. Spruch

Staatsgeheimnis
Höchste Geheimnisart, die nicht offenkundige Tatsachen, Gegenstände oder Nachrichten beinhaltet, die für den Schutz und die Stärkung der Staatsmacht der Deutschen Demokratischen Republik sowie für die Festigung der sozialistischen Staatengemeinschaft von entscheidender Bedeutung sind.
+ Dienstgeheimnis, Geheimhaltungsgrad.

Standardalphabet
Alphabet, das mit einem anderen Zeichen beginnt als ein vorgegebenes Alphabet, in dem aber im übrigen die Zeichen in der gewöhnlichen oder genau umgekehrten Reihenfolge stehen.
+ Mischalphabet.

steganographisches Verfahren svw. Zeichenverfahren

Stellencode
Mehrstufiger Code, bei dem im wesentlichen durch die Stellung des Codeelementes bzw. der Codegruppe im Codetext festgelegt ist, aus welcher Stufe die zugeordnete Phrase zu entnehmen ist.

Stellencodetafel
Mehrfachtafel, die nach dem Prinzip des Stellencodes aufgebaut ist.

Stereotype
Textteile, die in einem Nachrichtenverkehr häufig in unveränderter Form vorkommen.
Sie treten besonders in Routinemeldungen wie z. B. „Keine Vorkommnisse", bei Unterschriften u. dgl. auf und begünstigen die Dekryptierung.

Stoß svw. Stoßlinie

Stoßlinie s. Stoßlinienverfahren

Stoßlinienverfahren
Verfahren der Kartencodierung, das auf der Anwendung einer Stoßlinie beruht. Die STOSSLINIE ist eine Linie, die als Strahl von einem festgelegten Kartenpunkt, dem AUSGANGSPUNKT, über einen anderen festgelegten Kartenpunkt, den RICHTUNGSPUNKT, verläuft.
Die Deckbezeichnung für einen Kartenpunkt, die in diesem Fall als STOSSLINIENWERT bezeichnet wird, wird gebildet aus der Entfernung des Kartenpunktes senkrecht zur Stoßlinie (in mm) und von da zum Ausgangspunkt sowie einer weiteren Ziffer zur Kennzeichnung, ob sich der Kartenpunkt links oder rechts von der Stoßlinie befindet.

Zu einer Karte können gleichzeitig auch mehrere Stoßlinien verwendet werden. In diesem Fall ist die Bezeichnung der verwendeten Stoßlinie in den Stoßlinienwert einzubeziehen.

Stoßlinienwert s. Stoßlinienverfahren

Streifenmarkierung
Kennzeichnung eines Schlüssellochstreifens, z. B. durch Typ-, Serien- und Exemplarnummer.

Stufe
Eine bestimmte Zuordnung von Codegruppen zu Phrasenstellen bei mehrstufigen Codes.

Stundenschlüssel s. Zeitschlüssel

substituieren s. Substitution

Substitution (Infinitiv: SUBSTITUIEREN)

1. Eine der beiden Grundmethoden der Textumwandlung bei Anwendung eines offenen Chiffrierverfahrens, wobei die Einheiten eines Textes durch andere Einheiten ersetzt werden.
   + Transposition.
2. Zuordnung von Einheiten (AUSGANGSEINHEITEN) zu anderen Einheiten (ERSATZEINHEITEN).
   Die beiden Teile der Zuordnung werden als KOMPONENTEN der Substitution bezeichnet. Stehen in einer Komponente Klareinheiten, so wird diese als KLARKOMPONENTE bezeichnet; stehen in einer Komponente Zwischeneinheiten, so wird diese als ZWISCHENKOMPONENTE bezeichnet; stehen in einer Komponente Codegruppen, so wird diese als CODEKOMPONENTE bezeichnet; stehen in einer Komponente Geheimeinheiten, so wird diese als GEHEIMKOMPONENTE (bei Chiffreverfahren auch als CHIFFREKOMPONENTE) bezeichnet.
   Liegt eine Zuordnung von Klareinheiten zu Geheimeinheiten bzw. Codegruppen in zwei verschiedenen Anordnungen vor, von denen die erste zum leichteren Auffinden der Klareinheiten beim Chiffrieren (Codieren) nach diesen, die zweite zum leichteren Auffinden der Geheimeinheiten (Codegruppen) beim Dechiffrieren (Decodieren) nach diesen geordnet ist, so wird die erste Anordnung als CHIFFRIERTEIL bzw. + Codierteil, die zweite Anordnung als DECHIFFRIERTEIL bzw. + Decodierteil bezeichnet.
   Die Substitutionen werden eingeteilt in + isomorphe, + homomorphe und + fraktionelle Substitutionen.
   + Belegung, Code, Substitutionstafel.

3. Die Ersetzung von Einheiten durch andere aufgrund der festgelegten Zuordnung.

Substitutionsprogramm
Programm eines Chiffriergerätes, das eine bestimmte Substitution realisiert.

Substitutionsreihe
Reihenfolge der Verwendung der Substitutionen bei Spaltenverfahren.

Substitutionsschaltung
Schaltung zur Realisierung einer bestimmten Substitution.

Substitutionstafel
Anordnung einer oder mehrerer Substitutionen in Tafelform.

Substitutionsverfahren
Chiffrierverfahren, bei dem der Text durch Substitution umgewandelt wird.
Die Substitutionsverfahren werden eingeteilt in + Tauschverfahren, + Spaltenverfahren und + fraktionelle Verfahren.
+ Transpositionsverfahren.

sympathetische Tinte svw. Geheimtinte

Synchronbetrieb
Betriebsart von Kanalchiffriergeräten, bei der Sende- und Empfangsgerät selbständig synchron getaktet werden.
Der Synchronbetrieb bietet den Vorteil, daß bei kurzzeitiger Unterbrechung der Übertragung die nachfolgende Information nicht unklar wird.

Synonym
Wort mit gleicher oder ähnlicher Bedeutung wie ein anderes Wort, z. B. Telefon und Fernsprecher.
+ Homonym.

Tagesschlüssel s. Zeitschlüssel

Tarnelement
Element eines Tarntextes.

tarnen s. Tarnung

Tarner s. funktionsgebundener Benutzer

Tarngerät
Chiffriergerät, das eine Geheimhaltung bearbeiteter Nachrichten für mehrere Stunden gewährleistet.

Tarngruppe s. Codegruppe

Tarnmittel
Chiffriermittel zu Tarnverfahren.

Tarnname svw. Deckname

Tarnseite s. Tarnstreifen

Tarnserie
Spezielle Bezeichnung für Schlüsselserie bei Tarntafeln.

Tarnstreifen
Schlüsselstreifen zu Tarntafeln. Bei mehrseitigen Tarnstreifen werden die einzelnen Seiten als TARNSEITEN bezeichnet.

Tarntafel
Codetafel, die als Tarnmittel dient.

Tarntext
1. Geheimtext, der durch Anwendung eines Tarnverfahrens entstanden ist.
2. Scheinbar harmloser Text, der bei gedeckten Verfahren einen Geheimtext enthält oder überdeckt.

Tarnung (Infinitiv: TARNEN)
Chiffrierung durch Anwendung eines Tarnverfahrens.

Tarnverbindung s. Chiffrierverbindung

Tarnverfahren
Chiffrierverfahren, das eine Geheimhaltung für mehrere Stunden gewährleistet.

Tarnzahl svw. Deckzahl

tauschfreier Codegruppenbereich
Codegruppenbereich, bei dem keine Codegruppe durch Vertauschung zweier benachbarter Elemente in eine andere Codegruppe des gleichen Codegruppenbereiches übergeht.

Tauschverfahren
Substitutionsverfahren, bei dem die Chiffrierung mittels einer einzigen Substitution erfolgt.
Die Tauschverfahren werden eingeteilt in EINFACHE TAUSCHVERFAHREN, bei denen eine + isomorphe Substitution angewandt wird, und MEHRFACHE TAUSCHVERFAHREN, bei denen eine + homomorphe Substitution angewandt wird.
+ Spaltenverfahren.

technische Beschreibung
Umfassende Darstellung der physikalischen Eigenschaften (Abmessungen, Gewicht usw.), des Aufbaues, der Wirkungsweise und der Verwendungsmöglichkeiten eines Gerätes oder einer Anlage.

technische Nachrichtenmittel svw. Fernmeldemittel

teilchiffrieren s. Teilchiffrierung

Teilchiffrierung (Infinitiv: TEILCHIFFRIEREN)
Chiffrierung, bei der nur Teile eines Grundtextes chiffriert werden.

teilcodieren s. Teilcodierung

Teilcodierung (Infinitiv: TEILCODIEREN)
Codierung, bei der nur Teile eines Grundtextes codiert werden.

Teildirektchiffrierung s. Direktchiffrierung

Teillösung eines Chiffrierverfahrens s. Lösung eines Chiffrierverfahrens

teilmaschinelle Chiffrierung
Chiffrierung, bei der innerhalb eines Schlüsselbereiches mindestens ein Korrespondent mit und mindestens ein Korrespondent ohne Chiffriertechnik chiffriert bzw. dechiffriert.

teilmaschinelle Chiffrierverbindung s. Chiffrierverbindung

teilmaschinelles Verfahren
Chiffrierverfahren, bei dessen Anwendung mindestens ein Korrespondent mit und mindestens ein Korrespondent ohne Chiffriergerät chiffriert bzw. dechiffriert.

Telefonie
Übertragung von (gesprochener) Sprache mittels Wechselströmen über Draht oder Funk.

Telegrafenalphabet
Zuordnung von Schriftzeichen zu Impulsfolgen zwecks telegrafischer Übertragung.
Im MORSEALPHABET sind den Schriftzeichen Kombinationen von Punkten und Strichen (kurzen und langen Impulsen) zugeordnet. Zur Unterscheidung der einzelnen Zeichen und Wörter sind folgende Vereinbarungen getroffen: Die Einheit ist der Punkt; ein Strich = 3 Punktlängen; Abstand zwischen zwei Impulsen eines Schriftzeichens = 1 Punktlänge, zwischen zwei Schriftzeichen = 3 Punktlängen, zwischen zwei Wörtern = 5 Punktlängen.
Im Drahtfernschreibverkehr wird das INTERNATIONALE TELEGRAFENALPHABET Nr. 2 verwendet, auch FONFERALPHABET oder FÜNF-

SCHRITTALPHABET genannt. In ihm gibt es nur Punkte. Der Einzelschritt besteht aus „Strom" oder „kein Strom". Jedem Zeichen ist eine Kombination von 5 Einzelschritten zugeordnet. Insgesamt gibt es 32 Kombinationen, von denen 23 doppelt belegt sind.
Das Internationale Telegrafenalphabet Nr. 2 wurde 1929 von den Postverwaltungen aller Länder der Erde als verbindlich angenommen. Für Mehrfachtelegrafen wurde das INTERNATIONALE TELEGRAFENALPHABET Nr. 1 gewählt.
Im Funkfernschreibverkehr wird das SIEBENERALPHABET oder SIEBENSCHRITTALPHABET von van Duuren verwendet. Jede der 35 Kombinationen besteht aus 7 Einzelschritten, von denen jeweils drei Stromschritte und vier kein-Strom-Schritte sind. Dadurch können Verstümmelungen bis zu einem bestimmten Grade erkannt und berichtigt werden.
Das INTERNATIONALE TELEGRAFENALPHABET Nr. 5 ist ebenfalls ein Siebeneralphabet, bei dem aber alle 128 Kombinationen ausgenutzt werden. Es wurde für erweiterte Aufgaben der Fernschreibtechnik, besonders bei der Datenübertragung, geschaffen.
Beim Hell-Schreiber wird das TELEGRAFENALPHABET VON HELL verwendet, wobei die Schriftzeichen in Form von Rasterpunkten dargestellt werden. Der Raster besteht aus 7 Zeilen und 7 Spalten, also 49 Rasterpunkten.

Telegrafie
Nachrichtenübermittlung mittels Stromimpulsen über Draht oder Funk.
+ Bildtelegrafie.

Telegrafiergeschwindigkeit
Anzahl der kürzesten in einem System vorkommenden Telegrafierimpulse je Zeiteinheit.
Maßeinheit: 1 Baud = 1 Impuls pro Sekunde.

Telegramm
Nachricht, die telegrafisch übermittelt und dem Empfänger schriftlich ausgehändigt wird.

Telegrammstil
Ausdrucksweise, die jedes überflüssige Wort vermeidet.
+ Codestil.

tetradifferenter Codegruppenbereich
Codegruppenbereich, bei dem sich alle Codegruppen untereinander an mindestens vier Stellen unterscheiden.

Tetragramm s. Polygramm

Text

1. Im allgemeinen Sprachgebrauch: Folge von Schriftzeichen mit Informationsgehalt.
2. In der Kryptologie: Zusammenstellung von Elementen bzw. Zeichen, unabhängig von deren Beschaffenheit, der Art ihrer Verkettung und ihrem Informationsgehalt. Wesentlich ist nur, daß die Elemente isoliert und als Bestandteil eines + Alphabetes identifiziert werden können.
   Nach der Stellung im Chiffrierprozeß werden unterschieden:
   + Klartext, + Zwischentext und + Geheimtext.
   + Grundtext, Mischtext.
   Nach der Verschiedenartigkeit der im Text auftretenden Elemente wird unterschieden zwischen HOMOGENEM TEXT, in dem nur gleichartige Elemente auftreten (z. B. nur Buchstaben im BUCHSTABENTEXT, nur Ziffern im ZIFFERNTEXT), und INHOMOGENEM TEXT, in dem verschiedenartige Elemente auftreten (z B. Buchstaben, Ziffern und Satzzeichen).
   Nach dem Informationsgehalt wird unterschieden zwischen VOLLTEXT (Text mit Informationsgehalt) und LEERTEXT (Text ohne Informationsgehalt, z. B. in Blendsprüchen).

Textarten s. Text

Textschlüssel
Geltungsart eines Schlüssels, bei der eine maximale Textmenge (Anzahl Sprüche, Gruppen oder Elemente) festgelegt ist, die mit dem Schlüssel bearbeitet werden darf.
Ein Textschlüssel, mit dem jeweils nur ein Spruch chiffriert werden darf, wird als SPRUCHSCHLÜSSEL bezeichnet.

Transmitter
Lochstreifenlesende Baugruppe eines Chiffriergerätes.

transponieren s. Transposition

Transposition (Inifinitiv: TRANSPONIEREN)

1. Eine der beiden Grundmethoden der Textumwandlung bei Anwendung eines offenen Chiffrierverfahrens, wobei die Einheiten eines Textes umgeordnet werden, selbst aber unverändert bleiben. + Substitution.
2. Die Umordnung von Einheiten eines Textes.

Transpositionsverfahren
Chiffrierverfahren, bei dem der Text durch + Transposition umgewandelt wird.

Die Transpositionsverfahren werden eingeteilt in + Rasterverfahren und + Schlüsseltextverfahren.
+ Substitutionsverfahren.

Trennzeichen
Indikator, der anzeigt, daß bestimmte Textteile (Elemente, Wörter, Zahlen, sonstige Elementefolgen) zu trennen sind.

tridifferenter Codegruppenbereich
Codegruppenbereich, bei dem sich alle Codegruppen untereinander an mindestens drei Stellen unterscheiden.

Trigramm s. Polygramm

typisiertes Gefechtsdokument
Nachrichtentextformular in militärischen Bereichen.

Übergangssignal
Indikator, der bei mehrstufigen Verfahren den Übergang zu einer anderen Stufe anzeigt.

Übermittlungsfehler s. Verstümmelung

überschlüsseln s. Überschlüsselung

überschlüsselter Code svw. Schlüsselcode

Überschlüsselung (Infinitiv: ÜBERSCHLÜSSELN)
Nochmalige Chiffrierung eines bereits chiffrierten Textes zur Erhöhung der Sicherheit, wobei in der Regel ein anderes Verfahren angewandt wird als bei der vorangegangenen Chiffrierung.

Übertragungskanal svw. Kanal

Übungsnormen
Festlegung von über den + Ausbildungsnormen liegenden Leistungen und Fähigkeiten bei der Anwendung bestimmter Verfahren und Mittel.
+ Leistungsnormen.

Umschreibung
Bezugnahme der Teilnehmer eines Nachrichtenverkehrs auf ihnen bekannte Dinge in einer solchen Weise, daß dritte Personen den konkreten Inhalt nicht erfassen können.
Die Umschreibung ist keine Form der Chiffrierung.

Umsetztafel svw. Substitutionstafel

unbefugte Offenbarung (von Geheimnissen)
Preisgabe von Geheimnissen an unbefugte Personen. Bei fahrlässiger Preisgabe handelt es sich im wesentlichen um GEHEIMNISVERLETZUNG (vgl. StGB § 246), bei vorsätzlicher Preisgabe um GEHEIMNISVERRAT (vgl. StGB § 245).

unbefugte Person
Person, die vom Standpunkt des Urhebers, Aufbewahrers oder Vermittlers einer Information oder eines Gegenstandes davon keine Kenntnis erhalten soll.

unperiodische Additionsreihe
Reguläre Additionsreihe, die nicht periodisch ist.

unperiodisches Additionsverfahren
Additionsverfahren, bei dem eine unperiodische Additionsreihe benutzt wird.
Zu den unperiodischen Additionsverfahren gehören die + Buchtextverfahren und die + rekurrenten Verfahren.

Unterscheidungsgruppe
Einem Spruch beigefügte Gruppe, die bestimmte Unterscheidungsmerkmale mitteilt, z. B. die Kennzeichnung des Spruches als Zirkularspruch.

VD s. Geheimhaltungsgrad

verabredete Sprache
Gedecktes Verfahren, bei dem für bestimmte Ausdrücke der offenen Sprache eine geheime Bedeutung verabredet wird.

Verfahren svw. Chiffrierverfahren

Verkehr s. Chiffrierverkehr, Nachrichtenverkehr

Verkehrsarten s. Chiffrierverkehr

Verkehrscode
Wirtschaftscode, der im Nachrichtenverkehr des Verkehrswesens angewandt wird.
+ Schiffahrtscode.

Verknüpfung svw. kryptographische Addition

Verknüpfungsprogramm
Programm eines Chiffriergerätes, das eine bestimmte Verknüpfung realisiert.

Verknüpfungsschaltung
Schaltung eines Chiffriergerätes, die eine bestimmte Verknüpfung realisiert.

Verlängerungsfaktor
Gütefaktor zur Bewertung des Verhältnisses der Länge des Geheimtextes zur Länge des dazugehörenden Grundtextes.

verschleiern s. Verschleierung

Verschleierung (Infinitiv: VERSCHLEIERN)
Chiffrierung durch Anwendung eines Verschleierungsverfahrens, wobei in der Regel nur eine Teilchiffrierung erfolgt.

Verschleierungsgerät
Chiffriergerät, das für bearbeitete Nachrichten das unmittelbare Mitverstehen Unbefugter verhindert.

Verschleierungsmittel
Chiffriermittel zu Verschleierungsverfahren.

Verschleierungstext
Geheimtext, der durch Anwendung eines Verschleierungsverfahrens entstanden ist.

Verschleierungsverbindung s. Chiffrierverbindung

Verschleierungsverfahren
Chiffrierverfahren, das nur das unmittelbare Mitverstehen unbefugter Personen verhindert.

verschlüsseln svw. schlüsseln

Verschlüsselung svw. Schlüsselung

Verständlichkeitsfaktor
Gütefaktor zur Bewertung der Verständlichkeit eines chiffriert übermittelten Textes beim Empfänger (Dechiffreur). Er ist besonders bei der Sprachchiffrierung und bei der Anwendung mehrsprachiger Codes von Bedeutung. Bei der Sprachchiffrierung kann er als Prozentsatz der richtig verstandenen Wörter (WORTVERSTÄNDLICHKEIT) oder Silben (SILBENVERSTÄNDLICHKEIT) angegeben werden. Bei der Anwendung mehrsprachiger Codes kommt es in erster Linie auf die Übersetzungsgenauigkeit an.

Verstümmelung
Fehlerhafte Veränderung eines Textes durch Auftreten nicht eindeutig erkennbarer, falscher oder zusätzlicher Elemente, Ausfall oder

Vertauschung von Elementen. Alle diese Veränderungen stellen FEHLERMÖGLICHKEITEN dar.
Verstümmelungen können bei der Produktion von Chiffriermitteln (PRODUKTIONSFEHLER), bei der Chiffrierung bzw. Codierung (CHIFFRIER- bzw. CODIERFEHLER), bei der Übermittlung (ÜBERMITTLUNGSFEHLER) oder bei der Dechiffrierung bzw. Decodierung (DECHIFFRIER- bzw. DECODIERFEHLER) auftreten.
FEHLERURSACHEN können subjektiver oder objektiver Art sein. Subjektive Fehlerursachen sind z. B. Verlesen, Verschreiben, Verhören oder Versprechen (bei Diktat oder telefonischer Übermittlung), Rechenfehler bei der kryptographischen Addition; objektive Fehlerursachen sind z. B. technische Störungen bei der maschinellen Produktion, Chiffrierung, Übermittlung oder Dechiffrierung, atmosphärische Störungen bei Funkübermittlung. FEHLERAUSWIRKUNGEN können sein, daß der Text unverständlich oder unvollständig wird oder einen falschen Sinn erhält, demzufolge notwendige Handlungen unterbleiben oder erst mit Verspätung durchgeführt werden können oder sogar falsche Handlungen ausgelöst werden.

Verstümmelungsfaktor
Gütefaktor zur Bewertung der Fehlermöglichkeiten und Fehlerauswirkungen bei der Chiffrierung.
Übermittlung und Dechiffrierung.

Vertrauliche Dienstsache (VD) s. Geheimhaltungsgrad

Vertrauliche Verschlußsache (VVS) s. Geheimhaltungsgrad

Verwaltungscode
Code, der im Nachrichtenverkehr des Staats- und Verwaltungsdienstes angewandt wird.
+ diplomatischer Code.

Vierergruppe s. Gruppe

vollchiffrieren s. Vollchiffrierung

Vollchiffrierung (Infinitiv: VOLLCHIFFRIEREN)
Chiffrierung, bei der ein Grundtext vollständig chiffriert wird.

vollcodieren s. Vollcodierung

Vollcodierung (Infinitiv: VOLLCODIEREN)
Codierung, bei der ein Grundtext vollständig codiert wird.

vollständiges Alphabet
Alphabet, das den gleichen Zeichenbereich wie ein vorgegebenes Alphabet umfaßt.

Volltext s. Text, Information

Vollwort
Wort, das für die Erhaltung des Sinns und vollständigen Inhalts des Klartextes wesentlich ist.

Vorchiffriergerät
Chiffriergerät, das für + Vorchiffrierung ausgelegt ist.
+ Direktchiffriergerät.

Vorchiffrierung
Maschinelle Chiffrierung, bei der sowohl zwischen Chiffrierung und Übermittlung als auch zwischen Übermittlung und Dechiffrierung eine Zwischenspeicherung des Geheimtextes erfolgt.
+ Direktchiffrierung.

Vorrat
In Zusammensetzungen wie Elementevorrat, Codegruppenvorrat usw. svw. Anzahl der Elemente usw. des jeweiligen Bereiches.
(In der Literatur vielfach auch gleichbedeutend mit Bereich.)

VVS s. Geheimhaltungsgrad

Wechselbetrieb svw. Halbduplexbetrieb

wechselstelliger Code
Code, dessen Codegruppen verschiedene Länge haben.
+ gleichstelliger Code.

wechselstelliges Verfahren
Chiffrierverfahren, dessen Geheimeinheiten verschiedene Länge haben.
+ gleichstelliges Verfahren.

Weiterleitung
Übermittlung eines Spruches von einem Schlüsselbereich in einen anderen, wobei er von einer als Verbindungsglied dienenden Chiffrierstelle dechiffriert und neu chiffriert werden muß.

Wettercode
Code, der im Nachrichtenverkehr des meteorologischen Dienstes angewandt wird.

Wiederholungszeichen
Indikator, der eine Wiederholung anzeigt.

Wirtschaftscode
Code, der im Nachrichtenverkehr der Wirtschaft angewandt wird.
+ Handelscode, Branchencode, Firmencode, Verkehrscode.

Wochenschlüssel s. Zeitschlüssel

Wort

1. In der Kybernetik: Folge von Zeichen, die in einem bestimmten Zusammenhang als eine Einheit betrachtet wird.
2. In der Linguistik: Laut- oder Buchstabenkomplex (im Grenzfall auch ein einzelner Laut oder Buchstabe), der als kleinster selbständiger sprachlicher Bedeutungsträger auftritt. In diesem Sinne ist das Wort gleichzeitig ein + Zeichen. Die Anzahl der Elemente eines Wortes ist die WORTLÄNGE.
   + Homonym, Synonym, Leerwort, Vollwort.

Wortfolge

Folge von zwei oder mehr Wörtern.
Eine semantisch nicht auflösbare Wortfolge wird als WORTVERBINDUNG, REDEWENDUNG oder IDIOM bezeichnet. Eine Wortverbindung wie z. B. „einen Streit vom Zaune brechen" läßt sich in eine fremde Sprache nicht Wort für Wort, sondern nur als Sinnganzes übersetzen.

Wortlänge s. Wort

Wortverbindung s. Wortfolge

Wortverständlichkeit s. Verständlichkeitsfaktor

Würfelverfahren

Rasterverfahren, bei dem der Grundtext zeilenweise in einen Raster eingetragen und nach Permutation der Spalten (SPALTENTRANSPOSITION) spaltenweise abgelesen wird.
Bei Wiederholung dieses Vorganges (mit anderem Raster und anderer Spaltentransposition) handelt es sich um ein DOPPELWÜRFELVERFAHREN.

Wurm svw. irreguläre Additionsreihe

Wurmgruppe

Gruppe von Elementen einer irregulären Additionsreihe.

Wurmtabelle

Zusammenfassung einer Anzahl von Wurmgruppen in Tabellenform.

Wurmtabellenheft

Zusammenfassung einer bestimmten Anzahl von Wurmtabellen in Heftform.

Wurmtabellenkassette

Kassette, die zur Aufnahme von Wurmtabellen dient.

Wurmverfahren
Irreguläres Additionsverfahren, bei dem die Additionsreihe nur einmal benutzt wird.
Nach der Art der Additionselemente wird unterschieden zwischen + Buchstabenwurmverfahren und + Ziffernwurmverfahren.
+ Mehrfachwurmverfahren.

Zahlensignal
Indikator, der den Anfang oder das Ende von Zahlen anzeigt.

Zahlentafel
Codetafel, die zur Verschleierung von Ziffern und Zahlen dient.

Zeichen
1. Einheit aus einer materiellen Gestalt und einer Bedeutung.
Die materielle Gestalt wird als ZEICHENTRÄGER oder SIGNAL bezeichnet und kann u.a. ein Schriftzeichen, ein Bild, ein Laut, eine Lochung, ein Impuls oder eine Folge von solchen sein. Die wichtigsten Zeichen sind die SPRACHLICHEN ZEICHEN, mit deren Hilfe die Menschen Informationen austauschen. Dazu gehören die LAUTE (Lautzeichen) und die SCHRIFTZEICHEN; beide können zum Zweck der maschinellen Verarbeitung oder technischen Übertragung in Lochkombinationen, Impulsfolgen usw. umgeformt werden.
Die Schriftzeichen werden eingeteilt in BUCHSTABEN, ZIFFERN und SONDERZEICHEN (Satzzeichen und andere Sonderzeichen). Als ELEMENTARZEICHEN werden die kleinsten, als Einheit von Bedeutung und Signal nicht weiter zerlegbaren Zeichen verstanden, z. B. die verschiedenen Schriftzeichen (nicht die einzelnen Striche, aus denen sie zusammengesetzt sind) oder die verschiedenen Impulsfolgen des Morsealphabetes (nicht deren einzelne Impulse).
In der Kryptologie werden die Elementarzeichen als KRYPTOGRAPHISCHE ELEMENTE oder kurz ELEMENTE bezeichnet.
+ Alphabet, Text.
2. Zeichen, das nicht Buchstabe oder Ziffer ist.
+ Zeichenalphabet, Zeichencode, Zeichentext, Zeichenverfahren.

Zeichenadditionsreihe
Additionsreihe, unter deren Additionselementen mindestens ein von Buchstaben oder Ziffern verschiedenes Zeichen auftritt.

Zeichenadditionsverfahren
Additionsverfahren, bei dem eine Zeichenadditionsreihe verwendet wird.

Zeichenalphabet
Alphabet, das mindestens ein von Buchstaben oder Ziffern verschiedenes Zeichen enthält.

Zeichenbereich
Festgelegte Menge voneinander verschiedener Zeichen.

Zeichencode
Code, unter dessen Codeelementen mindestens ein von Buchstaben oder Ziffern verschiedenes Zeichen auftritt.

Zeichengruppe s. Gruppe

Zeichentext
Text, unter dessen Elementen mindestens ein von Buchstaben oder Ziffern verschiedenes Element auftritt.

Zeichenträger svw. Signal

Zeichenverfahren
Chiffrierverfahren, unter dessen Geheimelementen mindestens ein von Buchstaben oder Ziffern verschiedenes Zeichen auftritt.

Zeichenvorrat
Anzahl der Zeichen eines Zeichenbereiches bzw. Zeichenalphabetes.

Zeilenstreifen
Vertikaler Schlüsselstreifen bei Codetafeln, der die Zeilenbezeichnungen enthält.
+ Spaltenstreifen.

Zeitschlüssel
Geltungsart eines Schlüssels, bei der eine maximale Geltungsdauer festgelegt ist, innerhalb deren der Schlüssel beliebig oft benutzt werden darf. Je nachdem, ob die Geltungsdauer nach Stunden, Tagen, Wochen oder Monaten bemessen ist, werden unterschieden: STUNDENSCHLÜSSEL, TAGESSCHLÜSSEL, WOCHENSCHLÜSSEL, MONATSSCHLÜSSEL.
+ Langzeitschlüssel.

Zeittextschlüssel
Geltungsart eines Schlüssels, bei der sowohl eine maximale Textmenge als auch eine maximale Geltungsdauer festgelegt ist.

Zentrale
Leitendes Organ eines Chiffrierdienstes.

zentraler Chiffrierdienst
In einem größeren Bereich mit mehreren unabhängig voneinander bestehenden Chiffrierdiensten, die in diesem Fall als SELBSTÄNDIGE CHIFFRIERDIENSTE bezeichnet werden, der Chiffrierdienst, der mit der Abwicklung der Chiffrierkorrespondenz der Leitung des jeweiligen Bereiches und der nicht durch selbständige Chiffrierdienste erfaßten Bereichsteile, ggf. auch mit bestimmten Aufgaben der Anleitung, Koordinierung usw. des Chiffrierwesens im Gesamtbereich beauftragt ist.

zentrales Chiffrierorgan
Einrichtung des Chiffrierwesens, deren Aufgabe die zentrale Planung, Organisation, Sicherstellung, Anleitung und Kontrolle des Chiffrierwesens eines Staates ist.

Ziffer s. Zeichen

Ziffernadditionsreihe
Additionsreihe, die nur aus Ziffern besteht.

Ziffernadditionsverfahren
Additionsverfahren, bei dem eine Ziffernadditionsreihe verwendet wird.

Ziffernalphabet
Alphabet, dessen Zeichen ausschließlich Ziffern sind.
Ein ZIFFERNMISCHALPHABET ist ein Ziffernalphabet, dessen Ziffern nicht in der natürlichen Reihenfolge stehen.

Zifferncode
Code, dessen Codeelemente ausschließlich Ziffern sind.

Zifferngruppe s. Gruppe

Ziffernmischalphabet s. Ziffernalphabet

Ziffertext s. Text

Ziffernverfahren
Chiffrierverfahren, dessen Geheimelemente ausschließlich Ziffern sind.
+ Buchstabenverfahren, Zeichenverfahren.

Ziffernwurmverfahren
Wurmverfahren, dessen Additionselemente Ziffern sind.

zirkularer Text
Text, der in einem Zirkularverkehr übermittelt wird.
+ individueller Text.

Zirkulargegenverkehr
Chiffrierverkehr zwischen mehr als zwei Korrespondenten, wobei ein Korrespondent nur Empfänger ist und alle anderen Korrespondenten nur Absender sind.
+ Zirkularverkehr.

Zirkularverkehr
Chiffrierverkehr zwischen mehr als zwei Korrespondenten, wobei ein Korrespondent nur Absender ist und alle anderen Korrespondenten nur Empfänger sind.
+ Zirkulargegenverkehr.

Zufallsgenerator
Gerät, das für die Produktion irregulärer Folgen ausgelegt ist.

Zusatzverfahren
Chiffrierverfahren, das zusätzlich zum Hauptverfahren entweder in Verbindung mit diesem oder neben diesem zur rationelleren Chiffrierung oder zur Erhöhung der Sicherheit des Hauptverfahrens angewandt wird.
Beispiel: Tarntafel als Hauptverfahren zur Meldung besonderer Vorkommnisse. Sprechtafel als Zusatzverfahren für immer wiederkehrende stereotype Routinemeldungen.

Zweiergruppe s. Gruppe

Zweifachcode
Mehrfachcode mit einem Codierteil und einem Decodierteil.

zweiseitiger Verkehr
Chiffrierverkehr, bei dem beide Seiten sowohl Absender als auch Empfänger sind, z. B. zweiseitiger individueller Verkehr, allgemeiner Verkehr.

Zwischeneinheit
Einheit des Zwischentextes.

Zwischenelement
Element des Zwischentextes.

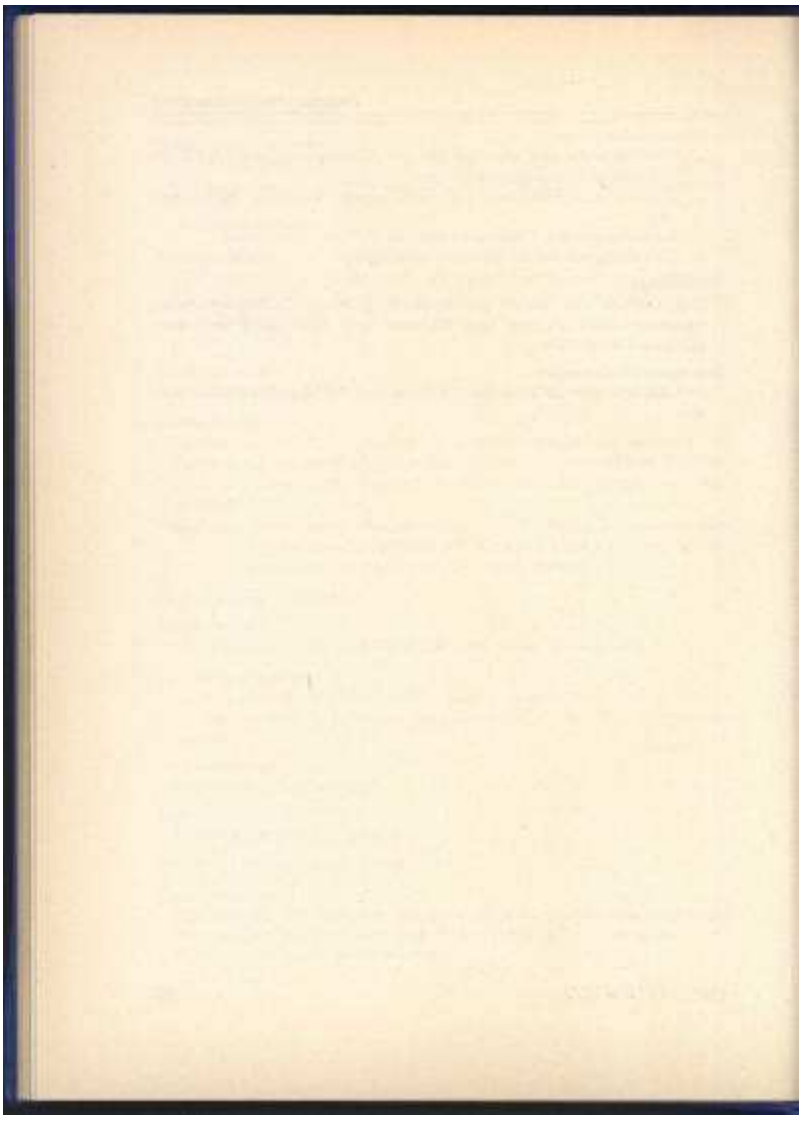
Zwischenkomponente s. Substitution

Zwischenmaterial
Materialien, die bei der Bearbeitung von Chiffrierunterlagen als Zwischenprodukte anfallen und Rückschlüsse auf die entsprechenden Chiffrierunterlagen selbst zulassen.

Dazu gehören u. a.
- Zwischentexte und sonstige bei der Chiffrierung und Dechiffrierung anfallende Aufzeichnungen;
- Notizen und Entwürfe zu Entwicklungen, Analysen, Weisungen usw.;
- Korrekturabzüge, Fehldrucke usw. zu Chiffrierunterlagen;
- Zwischenprodukte zu Schlüsselunterlagen.

Zwischentext
Zwischenform des Textes bei Anwendung eines Chiffrierverfahrens zwischen ursprünglichem Text (Klartext bzw. Grundtext) und endgültigem Geheimtext.

Zwischentextlochstreifen
Lochstreifen, der Zwischentext in Form von Lochkombinationen enthält.



Begriffsgruppen

Additionsverfahren

Additionsbereich
Additionseinheit
Additionselement
Additionselementebereich
Additionsfolge
Additionsgruppe
Additionsreihe
Additionstafel
Additionsverfahren
Buchstabenadditionsreihe
Buchstabenadditionsverfahren
Buchstabenwurmverfahren
Buchtextverfahren
Einsatzgruppe
irreguläre Additionsreihe
irreguläres Additionsverfahren
kryptographische Addition
Mehrfachwurmverfahren
periodische Additionsreihe
periodisches Additionsverfahren
reguläre Additionsreihe
reguläres Additionsverfahren
reinperiodische Additionsreihe
reinperiodisches Additionsverfahren
unperiodische Additionsreihe
unperiodisches Additionsverfahren
Verknüpfung
Wurm
Wurmgruppe
Wurmtabelle
Wurmtabellenheft
Wurmtabellenkassette
Wurmverfahren
Zeichenadditionsreihe
Zeichenadditionsverfahren
Ziffernadditionsreihe
Ziffernadditionsverfahren
Ziffernwurmverfahren

Alphabete

abgewandeltes Alphabet
Alphabet
alphabetisch niedriger
Buchstabenalphabet
Buchstaben-Ziffern-Alphabet
Chiffrealphabet
Codealphabet
Dezimationsalphabet
direktes Intervall
erweitertes Alphabet
Fernschreibcode
Fünferalphabet
Fünfschrittalphabet
Geheimalphabet
Grundalphabet
Internationales
Telegrafenalphabet
Intervall
ITA
Kehralphabet
Klaralphabet
Länge eines Alphabetes
Mischalphabet
Morsealphabet
Normalalphabet
Normalrang
Primalphabet
Rang eines Elementes
reduziertes Alphabet
reziproke Alphabete
Siebeneralphabet
Siebenschrittalphabet
Standardalphabet
Telegrafenalphabet
vollständiges Alphabet
Zeichenalphabet
Ziffernalphabet
Ziffernmischalphabet

Chiffrierverfahren allgemein (Einteilung, Anwendung)

Anwendungsbedingungen
Anwendungsbereich
Anwendungsvorschriften
Bedienungsanleitung
Bedienungsanweisung
Behelfsverfahren
Bereich
Buchstabenverfahren
Chiffre
Chiffreverfahren
Chiffrierverfahren
Codeverfahren
Einsatzbedingungen
Entwicklung eines Chiffrierverfahrens
Ersatzverfahren
Externverfahren
Gebrauchsanweisung
Gedächtnisverfahren
gedecktes Verfahren
Geheimschreibverfahren
gleichstelliges Verfahren
Hauptverfahren
Internverfahren
kombiniertes Verfahren
manuelles Verfahren
maschinelles Verfahren
mechanisches Verfahren
Mischverfahren
monographisches Verfahren
Notverfahren
offenes Verfahren
polygraphisches Verfahren
Schlüsselverfahren
Sicherheitsbestimmungen
Sonderverfahren
steganographisches Verfahren
Substitutionsverfahren
Tarnverfahren
technische Beschreibung
teilmaschinelles Verfahren
Transpositionsverfahren
Verfahren
Verschleierungsverfahren
wechselstelliges Verfahren
Zeichenverfahren
Ziffernverfahren
Zusatzverfahren

Chiffrierverkehr

absendende Chiffrierstelle
allgemeiner Verkehr
Blendspruch
Chiffretelegramm
Chiffrierdichte
Chiffrierkanal
Chiffrierkorrespondent
Chiffrierkorrespondenz
Chiffriernetz
Chiffrierverbindung
Chiffrierverkehr
Direktchiffrierverbindung
einseitiger Verkehr
empfangende Chiffrierstelle
Erkennungsgruppe
Fehlerauswirkungen
Fehlermöglichkeiten
Fehlerursachen
Füllfunkspruch
individueller Text
individueller Verkehr
Internverbindung
Kanalchiffriernetz
Kanalchiffrierverbindung
Kontrollgruppe
manuelle Chiffrierverbindung
maschinelle Chiffrierverbindung
Schlüsselbereich
Schlüsselverbindung
Tornverbindung
teilmaschinelle Chiffrierverbindung
Unterscheidungsgruppe
Verkehr
Verkehrsarten
Verschleierungsverbindung
Weiterleitung
Zirkulargegenverkehr
Zirkularverkehr
zweiseitiger Verkehr

Codeverfahren (außer Kartencodierung)

Belegung
bidifferenter
  Codegruppenbereich
bidifferent-tauschfreier
  Codegruppenbereich
Blankocode
Blankotafel
Branchencode
Buchstabencode
Buchstabiertafel
Buchstabier- und Zahlentafel
Code
Codealphabet
Codebuch
Codeelement
Codeelementebereich
Codeelementevorrat
Codefolge
Codegruppe
Codegruppenbereich
Codegruppengleichung
Codegruppentafel
Codegruppenvorrat
Codekomponente
Codemischtext
Codemittel
Codestil
Codetafel
Codetext
Codeumfang
Codeverfahren
Codewort
Codezahl
codieren
Codierer
Codierfehler
Codiersignal
Codiertafel
Codierteil
Codierung
Codistik
Deckbezeichnung
Deckname
Decknamenverzeichnis
Deckzahl
Deckzahlenverzeichnis
decodieren
Decodierer
Decodierfehler
Decodiertafel
Decodierteil
Decodierung
diplomatischer Code
eigentlicher Phrasenbestand
Einfachcode
einfacher Phrasencode
Einfachtafel
einsprachiger Code
einstufiger Code
Entstümmelungstafel
enttarnen
Enttarnung
Firmencode
Formularcode
Freigruppe
Freistelle
Geheimcode
Geheimsignaltafel
gesicherter
  Codegruppenbereich
gleichstelliger Code
Handelscode
Kurzcode
Kürzungscode
Marinecode
Mehrfachcode
Mehrfachtafel
mehrsprachiger Code

mehrstufiger Code
Mehrstufigkeit
Militärcode
Mischcode
Nachrichtentextformular
nichtüberschlüsselter Code
Offensignaltafel
öffentlicher Code
Ordnungswort
Phrase
Phrasenbestand
Phrasencode
Phrasenstelle
Phrasenstreifen
Phrasentafel
Phrasenteil
Phrasenverzeichnis
Phrasenvorrat
Phrasenzeile
Privatcode
Q-Code
Q-Gruppe
Satzbuch
Schemaspruch
Schiffahrtscode
Schlüsselcode
Schlüsseltafel
Signalcode
Signaltafel
Sondersprechtafel
Spaltenstreifen
Sprechtafel
Stellencode
Stellencodetafel
Stufe
Tarnelement
tarnen
Tarngruppe
Tarnname
Tarnseite
Tarnserie
Tarnstreifen
Tarntafel
Tarntext
Tarnzahl
tauschfreier
Codegruppenbereich
teilcodieren
Teilcodierung
tetradifferenter
Codegruppenbereich
tridifferenter
Codegruppenbereich
typisiertes Gefechtsdokument
überschlüsselter Code
Verkehrscode
Verwaltungscode
vollcodieren
Vollcodierung
wechselstelliger Code
Wettercode
Wirtschaftscode
Zahlentafel
Zeichencode
Zeilenstreifen
Zifferncode
Zweifachcode

Datenverarbeitung

alphanumerische Daten
Binärcode
Binärzeichen
Daten
Dateneinheit
Datenfernübertragung
Datenfernverarbeitung
Datensatz
Datenträger
Datentransfer
Datentransport
Datenübertragung
Datenverarbeitung
Datenwort
(¦)-Code (Eins-aus-n-Code)
Lochband
Lochkombination
Lochstreifen
numerische Daten
Programm

Einheiten, Gruppen (außer Indikatoren)

Additionseinheit
Additionsgruppe
Ausgangseinheit
Bigramm
Buchstabengruppe
Chiffre
Chiffreeinheit
Codegruppe
Codewort
Codezahl
Deckbezeichnung
Deckname
Deckzahl
Dienstgruppe
Einheit
Einsatzgruppe
Einstellgruppe
Elementegruppe
Erkennungsgruppe
Ersatzeinheit
Freigruppe
Fünfergruppe
Geheimeinheit
Geländezahl
Grundeinheit
Gruppe
Homophon
Ideogramm
Kenngruppe
Klareinheit
Kontrollgruppe
Länge eines Polygramms
Leerwort
lexikographisch niedriger
Lochkombination
Mischgruppe
Pentagramm
Phrase
Polygramm
Polyphone
Q-Gruppe
Schlüsselgruppe
Schlüsselwort
Schlüsselzahl
Schrittgruppe
Stoßlinienwert
Tarngruppe
Tarnname
Tarnzahl
Tetragramm
Trigramm
Unterscheidungsgruppe
Vierergruppe
Vollwort
Wort
Wortlänge
Wortverbindung
Wurmgruppe
Zeichengruppe
Zifferngruppe
Zweiergruppe
Zwischeneinheit

Einrichtungen, Räume

Bevollmächtigtenstelle
Chiffrierbetriebsdienst
Chiffrier-Bevollmächtigtenstelle
Chiffrierdienst
Chiffrierleitstelle
Chiffrierorgan
Chiffrierraum
Chiffrierstelle
Chiffrierzentrale
Dekryptierdienst
Dekryptierstelle
Dekryptierung
Direktchiffrierstelle
Einrichtungen des Chiffrierwesens
Kanalchiffrierstelle
Leitstelle
motorisierte Chiffrierstation
Räume des Chiffrierwesens
Reparaturdienst
selbständiger Chiffrierdienst
Zentrale
zentraler Chiffrierdienst
zentrales Chiffrierorgan

Elemente, Zeichen allgemein

Additionselement
Binärzeichen
Blender
Buchstabe
Chiffreelement
Codeelement
Daten
Element
Elementarzeichen
falsches Element
fremdes Element
Füllelement
Geheimelement
Grundelement
Ideogramm
Information
Klarelement
kryptographisches Element
Laut
Rang eines Elementes
Schriftzeichen
Signal
Sonderzeichen
sprachliches Zeichen
Tarnelement
Zeichen
Ziffer
Zwischenelement

Folgen, Reihen

absolut irreguläre Folge
Additionsfolge
Additionsreihe
Buchstabenadditionsreihe
Chiffrefolge
Codefolge
Elementefolge
Folge
irreguläre Additionsreihe
irreguläre Folge
Klarfolge
Länge einer Folge
periodische Additionsreihe
reguläre Additionsreihe
reinperiodische Additionsreihe
Wortfolge
Wortverbindung
Ziffernadditionsreihe

Funkkrieg, Fernmeldeaufklärung

Antifunkgegenwirkung
Drahtaufklärung
elektronischer Krieg
Fernmeldeaufklärung
Funkaufklärung
Funkdesinformation
funkelektronischer Krieg
Funkgegenwirkung
Funkimpulsaufklärung
Funkkrieg
Funkmeßaufklärung
Funknachrichtenaufklärung
Funkpeilung
Funkstörung
Funktarnung
Funktäuschung

Gedeckte Verfahren

Briefverfahren
chemisches Geheimschreibverfahren
Einbauverfahren
gedecktes Verfahren
Geheimschreibmittel
Geheimschreibsubstanz
Geheimschreibverfahren
Geheimtinte
Kennzeichnungsverfahren
Mikratverfahren
sympathetische Tinte
Tarntext
verabredete Sprache

Geheimnisschutz

abhörsichere Leitung
Chiffrierwesen
Dekonspiration
Dienstgeheimnis
Fernmeldegeheimnis
Funkgeheimnis
gedeckte Führung
gedeckte Truppenführung
geheime Nachricht
Geheime Verschlußsache
Geheimhaltung
Geheimhaltungsgrad
Geheimhaltungsstufe
Geheimnisschutz
Geheimnisse
Geheimnisträger
Geheimnisverletzung
Geheimnisverrat
Geheimnisverwahrung
gesicherte Leitung
GVS
Kompromittierung von Chiffrierunterlagen
Konspiration
Kryptanalysis
Kryptographie
Kryptologie
NfD
Nur für den Dienstgebrauch
Post- und Fernmeldegeheimnis
Sicherheitsbestimmungen
Sicherheitsüberprüfung
Sicherungsmittel
Sicherungstechnik
Sicherungsvorrichtung
Staatsgeheimnis
unbefugte Offenbarung
unbefugte Person
VD
Vertrauliche Dienstsache
Vertrauliche Verschlußsache
VVS

Güte

absolute Sicherheit
Analyse eines Chiffrierverfahrens
Chiffriergeschwindigkeit
Chiffriergeschwindigkeitsfaktor
Chiffriermittelfaktor
Dechiffriergeschwindigkeit
Dekryptierbarkeit
geringe Sicherheit
Güte
Gütefaktor
hohe Sicherheit
kryptologische Sicherheit
Mindestsicherheit
mittlere Sicherheit
quasiabsolute Sicherheit
Schwierigkeitsfaktor
Sicherheit eines Chiffrierverfahrens
Sicherheitsfaktor
Sicherheitsgrad
Silbenverständlichkeit
Verlängerungsfaktor
Verständlichkeitsfaktor
Verstümmelungsfaktor
Wortverständlichkeit

Indikatoren

Buchstabiersignal
Chiffriersignal
Codiersignal
Fortsetzungsvermerk
Indikator
Irrungszeichen
Mehrzahlsignal
Sprachensignal
Trennzeichen
Übergangssignal
Wiederholungszeichen
Zahlensignal

Informations- und Kommunikationstheorie

Code
Codierung
Codierverfahren
Empfänger
fernmeldetechnisches System
fördernde Redundanz
Information
Informationsquelle
Kanal
Kommunikation
Kommunikationskette
leere Redundanz
Nachricht
Redundanz
Sender
Senke
Signal
Zeichen
Zeichenträger

Kartencodierung

Ausgangspunkt
Geländezahl
Gitternetzverfahren
Großquadratverfahren
Kartencodierung
Kolonnenverfahren
Mittel der Kartencodierung
Neunersystem
Neunerunterteilung
Planquadratverfahren
Richtungspunkt
Stoß
Stoßlinie
Stoßlinienverfahren
Stoßlinienwert

Kryptanalysis, Dekryptierung

absolute Frequenz
Analyse eines Chiffrierverfahrens
charakteristisches Polygramm
Dekrypteur
Dekryptierarbeit
Dekryptierbarkeit
Dekryptierdienst
dekryptieren
Dekryptiergerät
Dekryptiermethode
Dekryptiermöglichkeiten
Dekryptierstelle
Dekryptiertechnik
Dekryptierung
Einbruch
Frequenz
Frequenzanalyse
Frequenzanalysis
Frequenzausgleich
Frequenzverschleierung
Frequenzverteilung
Kryptanalysis
Lösbarkeit
Lösung
Mitlesen
Normalfrequenz
Parallelstelle
phasengleiche Geheimtexte
relative Frequenz
schlüsselgleiche Geheimtexte
Schlüsselrekonstruktion
Teillösung eines Chiffrierverfahrens

Linguistik

Alphabet
Buchstabe
Homonym
Ideogramm
Idiom
Intervall
Laut
Leerwort
Ordnungswort
Redewendung
Schriftzeichen
Sonderzeichen
sprachliches Zeichen
Synonym
Telegrammstil
Text
Umschreibung
Vollwort
Wort
Wortfolge
Wortlänge
Wortverbindung

Maschinelle Verfahren

abgesetzter Fernschreiber
Abschnittsmarkierung
Abschnittsnummer
Abstrahlung
Arbeitsart
Aufdruckmarkierung
Bedienungsanleitung
Bedienungsanweisung
Betriebsart
Bildchiffriergerät
Bildchiffrierung
Bildchiffrierverfahren
Chiffrator
Chiffretextlochstreifen
Chiffriergerät
Chiffrierkanal
Chiffriermaschine
Chiffriertechnik
Chiffriervorrichtung
Chiffrierwalze
Datenchiffriergerät
Datenchiffrierprogramm
Datenchiffrierung
Dechiffrator
Dechiffriervorrichtung
Dekombinator
Direktchiffriergerät
Direktchiffrierung
Einlegemarkierung
Faksimilechiffriergerät
Fünfergruppenzähler
Geheimtextlochstreifen
Gruppenzähler
Kanalchiffriergerät
Kanalchiffrierung
Kenngruppenabschnitt
Kenngruppen-Lochstreifenabschnitt
Klartextlochstreifen
Kombinator
Kontrollprogramm
Kontrollschlüssel
Kontroll- und Sicherungsvorrichtungen
Kontrollzone
Linienbetrieb
Lokalbetrieb
maschinelle Chiffrierung
maschinelles Verfahren
off-line-Chiffrierung
on-line-Chiffrierung
Prüfprogramm
Schlüsselgerät
Schlüssellochkarte
Schlüssellochstreifen
Schlüssellochstreifenabschnitt
Schlüssellochstreifenheft
Schlüssellochstreifenkassette
Schlüsselscheibe
Schlüsselscheibenblock
Schlüsselscheibensatz
Schlüsselwalze
Schriftchiffriergerät
Schriftchiffrierung
Schriftchiffrierverfahren
Sicherungsvorrichtung
Sperrzone
Sprachchiffriergerät
Sprachchiffrierung
Sprachchiffrierverfahren

Sprachtrakt
Streifenmarkierung
Substitutionsprogramm
Substitutionsschaltung
Synchronbetrieb
Tarngerät
technische Beschreibung
Teildirektchiffrierung
teilmaschinelle Chiffrierung
teilmaschinelles Verfahren
Transmitter
Verknüpfungsprogramm
Verknüpfungsschaltung
Verschleierungsgerät
Vorchiffriergerät
Vorchiffrierung
Zwischentextlochstreifen

Mengen, Bereiche, Vorräte (außer Alphabeten)

Additionsbereich
Additionselementebereich
Bereich
bidifferenter
  Codegruppenbereich
bidifferent-tauschfreier
  Codegruppenbereich
Chiffrebereich
Chiffreelementebereich
Chiffreelementevorrat
Chiffrevorrat
Codeelementebereich
Codeelementevorrat
Codegruppenbereich
Codegruppenvorrat
effektiver Schlüsselvorrat
eigentlicher Phrasenbestand
Elementebereich
Elementevorrat
Geheimbereich
Geheimelementebereich
Geheimelementevorrat
Geheimvorrat
gesicherter
  Codegruppenbereich
Grundbereich
Grundelementebereich
Grundelementevorrat
Grundtextbereich
Grundtextvorrat
Klarbereich
Klarelementebereich
Klarelementevorrat
Klarvorrat
Menge
Phrasenbestand
Phrasenvorrat
Schlüsselvorrat
tauschfreier
  Codegruppenbereich
tetradifferenter
  Codegruppenbereich
tridifferenter
  Codegruppenbereich
Vorrat
Zeichenbereich
Zeichenvorrat

abhörsichere Leitung
Absender
Baud
Bildtelegrafie
Dienstgruppe
Dringlichkeit
Dringlichkeitsstufen
Duplexbetrieb
Empfänger
Faksimiletelegrafie
Fernmeldeanlage
Fernmeldegeheimnis
Fernmeldemittel
fernmeldetechnisches System
Fernmeldeverkehr
Fernmeldewesen
Fernschreibcode
Fünferalphabet
Fünfschrittalphabet
Funkgeheimnis
Funkspruch
Funkstörung
Gegenbetrieb
gesicherte Leitung
Halbduplexbetrieb
Internationales Telegrafenalphabet
ITA
Kanal
Kommunikation
Kommunikationskette
Konferenzbetrieb
Kontrollgruppe
Korrespondent
Linienbetrieb
Lokalbetrieb
Morsealphabet
Nachricht
Nachrichtenbeförderung
Nachrichtendichte
Nachrichtenfluß
Nachrichtenkanal
Nachrichtennetz
Nachrichtenstelle
Nachrichtenübermittlung
Nachrichtenverbindung
Nachrichtenverkehr
offene Nachricht
offener Kanal
Post- und Fernmeldegeheimnis
Q-Code
Q-Gruppe
Richtungsbetrieb
Rückfrage
Schrittgeschwindigkeit
Schrittgruppe
Sender
Siebeneralphabet
Siebenschrittalphabet
Simplexbetrieb
Spruch
Spruchende
Spruchkopf
Spruchlänge
Spruchtext
technische Nachrichtenmittel
Telefonie
Telegrafenalphabet
Telegrafie
Telegrafiergeschwindigkeit
Telegramm
Übermittlungsfehler
Übertragungskanal
Unterscheidungsgruppe
Verkehr
Verstümmelung

Personen, Ausbildung

Ausbildungsnormen
Chiffreur
Chiffreurmechaniker
Chiffriermechaniker
Codierer
Dechiffreur
Decodierer
Dekrypteur
Fahrerchiffreur
Fahrerchiffreurmechaniker
Funkerchiffreur
funktionsgebundener Benutzer von Chiffriermitteln
hauptamtlicher Mitarbeiter des Chiffrierdienstes
Hauptmechaniker
Klassifizierung
Kryptanalytiker
Kryptograph
Kryptologe
Leistungsklasse
Leistungsnormen
Mechaniker
Mitarbeiter des Chiffrierdienstes
nebenamtlicher Mitarbeiter des Chiffrierdienstes
Schlüßler
Tarner
Übungsnormen

Schlüssel und Schlüsselunterlagen

Abschnittsmarkierung
Abschnittsnummer
Additionsreihe
Additionstafel
äquivalente Schlüssel
Aufdruckmarkierung
Ausgangsheft
Ausgangskassette
Chiffrierscheibe
effektiver Schlüsselvorrat
Eingangsheft
Eingangskassette
Eingangsschlüssel
Einlegemarkierung
Einsatzgruppe
Einstellgruppe
Einzelblattabsicherung
Entnahmetabelle
Erkennungsgruppe
Gedächtnisschlüssel
Geltungsdauer
Geltungszeitraum
Kenngruppe
Kenngruppenabschnitt
Kenngruppen-
Lochstreifenabschnitt
Kenngruppentafel
kombinierter Schlüssel
Kontrollschlüssel
Langzeitschlüssel
Monatsschlüssel
Schlüssel
Schlüsselbereich
Schlüsseleinstellung
Schlüsselelement
Schlüsselgruppe
Schlüsselgruppentafel
Schlüsselheft
Schlüsselkassette
Schlüssellochkarte
Schlüssellochstreifen
Schlüssellochstreifenabschnitt
Schlüssellochstreifenheft
Schlüssellochstreifenkassette
Schlüsselreihe
Schlüsselsatz
Schlüsselscheibe
Schlüsselscheibenblock
Schlüsselscheibensatz
Schlüsselserie
Schlüsselserienwechsel
Schlüsselstreifen
Schlüsseltabelle
Schlüsselunterlagen
Schlüsselvorrat
Schlüsselwalze
Schlüsselwechsel
Schlüsselwort
Schlüsselzahl
Spaltenstreifen
Spruchschlüssel
Streifenmarkierung
Stundenschlüssel
Tagesschlüssel
Tarnseite
Tarnserie
Tarnstreifen
Textschlüssel
Wochenschlüssel
Wurmtabelle
Wurmtabellenheft
Wurmtabellenkassette
Zeilenstreifen
Zeitschlüssel
Zeittextschlüssel

Spezialtechnik

Bildchiffriergerät
Chiffrator
Chiffriergerät
Chiffriermaschine
Chiffrierscheibe
Chiffriertechnik
Chiffriervorrichtung
Chiffrierwalze
Datenchiffriergerät
Dechiffrator
Dechiffriervorrichtung
Dekombinator
Dekryptiergerät
Dekryptiertechnik
Direktchiffriergerät
Faksimilechiffriergerät
Kanalchiffriergerät
Kombinator
Scheibe
Schlüsselgerät
Schlüsselscheibe
Schlüsselscheibenblock
Schlüsselscheibensatz
Schlüsselwalze
Schriftchiffriergerät
Spezialproduktionstechnik
Spezialtechnik
Sprachchiffriergerät
Sprachtrakt
Tarngerät
Verschleierungsgerät
Vorchiffriergerät
Zufallsgenerator

Substitutionsverfahren (außer Additionsverfahren)

Ausgangseinheit
Belegung
Chiffrekomponente
Chiffrierscheibe
Chiffrierteil
Dechiffrierteil
Einfachbelegung
einfaches Tauschverfahren
Eingangsschlüssel
Ersatzeinheit
fraktionelle Substitution
fraktionelles Verfahren
Geheimkomponente
homogene Belegung
homomorphe Substitution
Homophon
inhomogene Belegung
isomorphe Substitution
Klarkomponente
Komponente
Mehrfachbelegung
mehrfaches Tauschverfahren
monoalphabetisches Verfahren
polyalphabetisches Verfahren
Polyphone
rekurrentes Verfahren
Scheibe
Schieber
Spaltenverfahren
substituieren
Substitution
Substitutionsreihe
Substitutionstafel
Substitutionsverfahren
Tauschverfahren
Umsetztafel
Zwischenkomponente

Tätigkeiten

Bildchiffrierung
Chiffrierarbeit
chiffrieren
Chiffrierfehler
Chiffrierschritt
Chiffrierung
codieren
Codierfehler
Codierung
Datenchiffrierung
dechiffrieren
Dechiffrierfehler
Dechiffrierschritt
Dechiffrierung
decodieren
Decodierfehler
Decodierung
Dekryptierarbeit
dekryptieren
Dekryptierung
Direktchiffrierung
einfache Verstümmelung
Entstümmelung
enttarnen
Enttarnung
Entwicklung
Fehlerauswirkungen
Fehlermöglichkeiten
Fehlerursachen
Herrichtung des Klartextes
Kanalchiffrierung
Lösung
manuelle Chiffrierung
maschinelle Chiffrierung
mitlesen
off-line-Chiffrierung
on-line-Chiffrierung
Produktionsfehler
schlüsseln
Schlüsselung
Schriftchiffrierung
Sprachchiffrierung
substituieren
Substitution
tarnen
Tarnung
teilchiffrieren
Teilchiffrierung
teilcodieren
Teilcodierung
Teildirektchiffrierung
Teillösung
teilmaschinelle Chiffrierung
transponieren
Transposition
Übermittlungsfehler
überschlüsseln
Überschlüsselung
verschleiern
Verschleierung
verschlüsseln
Verschlüsselung
Verstümmelung
vollchiffrieren
Vollchiffrierung
vollcodieren
Vollcodierung
Vorchiffrierung

Texte

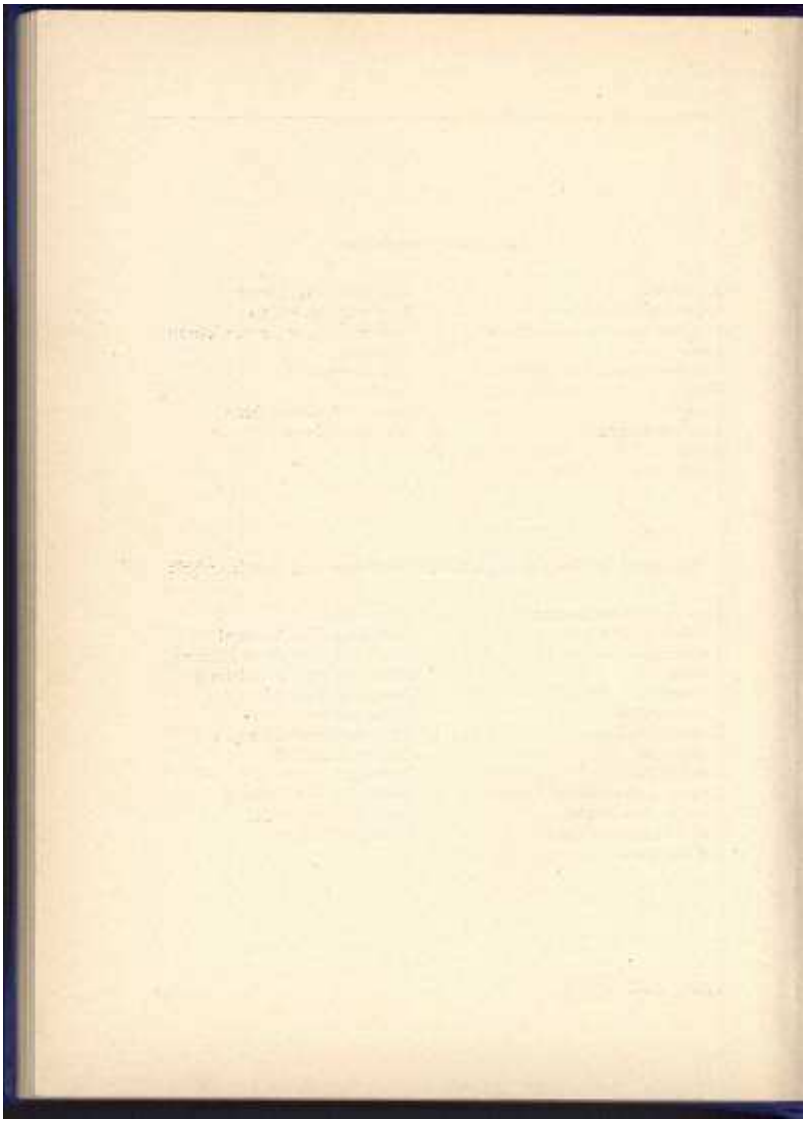
Blendspruch
Buchstabentext
Chiffremischtext
Chiffretext
chiffrierte Nachricht
chiffrierter Text
Codemischtext
Codetext
Füllfunkspruch
Funkspruch
gedeckter Geheimtext
Geheimmischtext
Geheimschrift
Geheimtext
Grundtext
hergerichteter Klartext
homogener Text
individueller Text
Information
inhomogener Text
isomorphe Geheimtexte
Klartext
Kryptogramm
Länge eines Textes
Leertext
Mischtext
Nachricht
offene Nachricht
offener Geheimtext
offener Text
phasengleiche Geheimtexte
Schemaspruch
schlüsselgleiche Geheimtexte
Schlüsseltext
Spruch
Spruchende
Spruchkopf
Spruchlänge
Spruchtext
Stereotype
Tarntext
Text
Textarten
Verschleierungstext
Volltext
Zeichentext
Zifferntext
zirkularer Text
Zwischentext

Transpositionsverfahren

Arbeitsfeld
Doppelwürfelverfahren
Feldertranspositionsverfahren
Gitter
Gitterverfahren
Matrix
Raster
Rasterverfahren
Route
Schlüsseltextverfahren
Spaltentransposition
Spaltentranspositionsverfahren
Sperrfeld
transponieren
Transposition
Transpositionsverfahren
Würfelverfahren

Unterlagen (außer Codes, Schlüsselunterlagen und Spezialtechnik

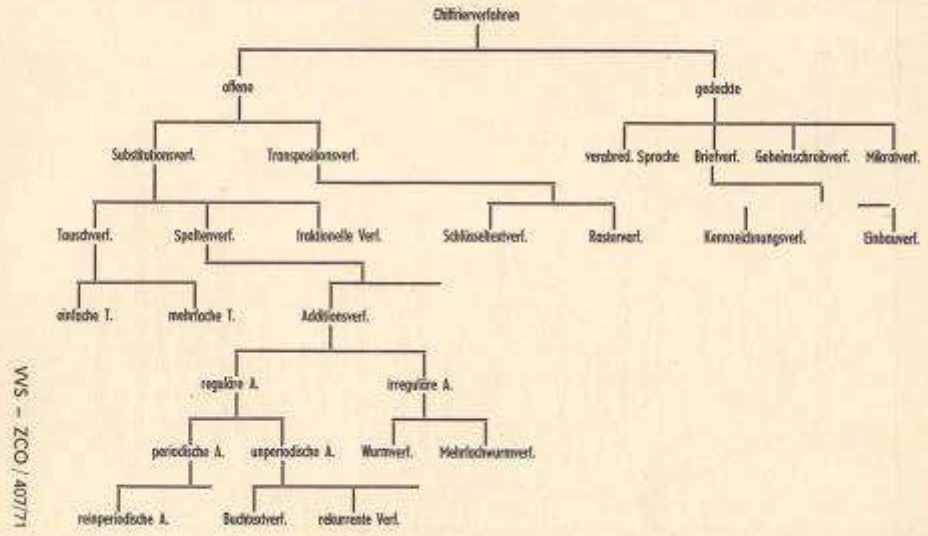
Anwendungsvorschriften
Bedienungsanleitung
Bedienungsanweisung
Chiffre
Chiffremittel
Chiffriermittel
Chiffrierunterlagen
Codemittel
Externmittel
Gebrauchsanweisung
Geheimschreibmittel
Geheimschreibsubstanz
Geheimtinte
Internmittel
manuelles Chiffriermittel
Mittel der gedeckten Führung
Mittel der Kartencodierung
Pflichtenfestlegung
Schlüsselmittel
Sicherheitsbestimmungen
Substitutionstafel
Tarnmittel
technische Beschreibung
Verschleierungsmittel
Zwischenmaterial



Systematische Übersicht der Begriffsgruppen

1. **Geheimnisschutz**
2. **Chiffrierwesen, Kryptologie**
2.1. **Allgemeine Grundlagen**
2.1.1. Einrichtungen, Räume
2.1.2. Personen, Ausbildung
2.1.3. Tätigkeiten
2.1.4. Unterlagen (außer Codes, Schlüsselunterlagen und Spezialtechnik)
2.1.5. Schlüssel und Schlüsselunterlagen
2.1.6. Spezialtechnik
2.1.7. Zeichen und Texte
2.1.7.1. Elemente, Zeichen allgemein
2.1.7.2. Einheiten, Gruppen
2.1.7.2.1. Indikatoren
2.1.7.3. Mengen, Bereiche, Vorräte
2.1.7.3.1. Alphabete
2.1.7.4. Folgen, Reihen
2.1.7.5. Texte
2.2. **Chiffrierverfahren, Kryptographie**
2.2.1. Chiffrierverfahren allgemein
2.2.1.1. Güte
2.2.2. Transpositionsverfahren
2.2.3. Substitutionsverfahren
2.2.3.1. Additionsverfahren
2.2.4. Codeverfahren
2.2.4.1. Kartencodierung
2.2.5. Maschinelle Verfahren
2.2.6. Gedeckte Verfahren
2.3. **Kryptanalysis, Dekryptierung**
3. **Nachbargebiete**
3.1. Datenverarbeitung
3.2. Funkkrieg, Fernmeldeaufklärung
3.3. Informations- und Kommunikationstheorie
3.4. Linguistik
3.5. Nachrichtenwesen

122 Systematische Teilübersicht der Chiffrierverfahren



Gebräuchliche Abkürzungen

AAS	=	Arbeitsartenschalter
AR	=	Additionsreihe
BA	=	Bedienungsanweisung
BAS	=	Betriebsartenschalter
Bu	=	Übergang zu Buchstabentext
Chi-	=	Chiffrier–
CT	=	Chiffretext
CS	=	Übergang zu Code (Codiersignal)
DFÜ	=	Datenfernübertragung
DG	=	Dienstgruppe
GA	=	Gebrauchsanweisung
GT	=	Geheimtext
hKT	=	hergerichteter Klartext
KG	=	Kenngruppe
KSV	=	Kontroll- und Sicherungsvorrichtung(en)
KT	=	Klartext
MCS	=	motorisierte Chiffrierstation
NZ	=	Neue Zeile
SAI	=	Schulungsanleitung
SCD	=	selbständiger Chiffrierdienst
SG	=	Schlüsselgruppe
SiT	=	Signaltafel
SpT	=	Sprechtafel
SRA	=	Streifenrißanzeige
SuT	=	Übergang zu Substitutionstafel
TT	=	Tarntafel
UG	=	Unterscheidungsgruppe
WR/ZL	=	Wagenrücklauf und Zeilenvorschub
WS	=	Wiederholungssignal
ZCD	=	Zentraler Chiffrierdienst
ZCO	=	Zentrales Chiffrierorgan
Zi	=	Übergang zu Ziffern- und Zeichentext
ZS	=	Zahlensignal
ZwR	=	Zwischenraum
ZwT	=	Zwischentext
32.	=	32. Kombination des ITA 2