Anhang A

Glossar

A5
Stromchiffre, welche innerhalb des GSM-Standards, also im Mobilfunkbereich verwendet wird.

Advanced Encryption Standard (AES)
Der AES ist ein symmetrisches Verschlüsselungssystem mit Schlüssellängen von 128, 192 oder 256 Bits. Der AES ist im Jahr 2000 als Nachfolger des DES ausgewählt worden.

affine Abbildung
Eine Transformation, die die Multiplikation mit einer Matrix gefolgt von der Addition mit einem Vektor beinhaltet.

Algorithmus
Eindeutig bestimmtes Verfahren/Prozedur. Ein kryptographischer Algorithmus definiert eine Prozedur zur Ver- und Entschlüsselung von Daten.

Alice und Bob
Wohl die beiden bekanntesten Anwender der Kryptographie. Werden in technischen Beschreibungen die Endpunkte einer Kommunikationsverbindung oft mit A und B bezeichnet, ist es bei der Beschreibung kryptographischer Verfahren üblich, die Namen „Alice“ und „Bob“ zu verwenden. Weitere, öfters anzutreffende Personen sind: die Lauscherin Eve (von eavesdropper) und der Angreifer Mallory (von malicious).

American National Standards Institute (ANSI)
Amerikanische Organisation, die Standards für verschiedene Branchen definiert und veröffentlicht.

Angriff
Als Angriff werden alle Versuche bezeichnet, aus gegebenen Geheimtexten die Klartexte oder den zugehörigen Schlüssel mit Hilfe von kryptoanalytischen Methoden zu ermitteln.

asymmetrische Verschlüsselung
Diese Chiffrierverfahren werden auch Public-Key-Verfahren genannt. Es handelt sich um Verschlüsselungsverfahren, bei denen für die Ver- und Entschlüsselung unterschiedliche Schlüssel verwendet werden — und zwar ein öffentlicher (public) und ein geheimer (privat) Schlüssel. Die öffentlichen Schlüssel der Kommunikationsteilnehmer sind frei verfügbar. Mit dem öffentlichen Schlüssel des Empfängers läßt sich eine Nachricht zwar verschlüsseln aber nicht wieder entschlüsseln. Dazu benötigt der Empfänger den nur ihm bekannten geheimen Schlüssel. Der geheime Schlüssel ist aus dem öffentlichen Schlüssel nicht mit vertretbarem Aufwand abzuleiten.

Neben der eigentlichen Verschlüsselung von Klartexten können asymmetrische Verfahren auch zur Authentifizierung und insbesondere zur Erstellung digitaler Signaturen verwendet werden. Hier wird mit dem geheimen Schlüssel des Absenders eine Nachricht chiffriert, die nur mit dem entsprechenden öffentlichen Schlüssel des Absenders beim Adressaten entschlüsselt werden kann. Dadurch ist der Absender eindeutig identifizierbar.

Authentifizierung
Unter Authentifizierung versteht man die Feststellung der Identität einer Person, um den Zugang zu technischen Systemen zu kontrollieren. Außerdem wird die Prüfung der Authentizität von elektronischen Dokumenten als Authentifizierung bezeichnet.

Authentizität
Die Authentizität (Echtheit) eines elektronischen Dokumentes umfasst seine Integrität und seine Urheberschaft.

Baud
Anzahl der Statusveränderungen eines Mediums bei der Datenübertragung. Ein Modem mit 14 400 Baud verändert das Signal, das es an die Telefonleitung abgibt, 14 400 mal pro Sekunde.

Birthday Attack
siehe *Geburtstagsangriff*

Bit
Eine binäre Stelle, die den Wert 0 oder 1 annehmen kann.

Bletchley Park
Im 2. Weltkrieg streng abgeschirmtes Gebiet in Großbritannien, auf dem die massenhafte Dechiffrierung vor allem Enigma-verschlüsselter Nachrichten der deutschen Wehrmacht vorgenommen wurde. Anfang 1944 arbeiten bereits ca. 7 000 Menschen dort; bis zu 90 000 Nachrichten entzifferten die Mitarbeiter monatlich.

Blockchiffre
Eine Blockchiffre setzt immer auf Klartextblöcken fester Länge auf. Falls

erforderlich wird die zu verschlüsselnde Nachricht mit Füllzeichen auf ein Vielfaches der Blockgröße aufgefüllt und dann in gleichgroße Blöcke aufgeteilt. Die Verschlüsselung der Klartextblöcke erfolgt typischerweise unabhängig von der Position in der Nachricht und bei Verwendung des stets gleichen Schlüssels. Einige Varianten stellen Verknüpfungen zwischen benachbarten Blöcken her, um die Schwäche zu umgehen, dass gleiche Klartextblöcke immer zum gleichen Chiffretextblock führen könnten.

Brechen eines Verfahrens
Auffinden einer Methode, mit einem gegebenen Chiffrierverfahren verschlüsselte Nachrichten zu entziffern, ohne den geheimen Schlüssel zu kennen. Ein Verfahren gilt jedoch nicht als gebrochen, wenn die effektivste bekannte Angriffsmethode im Durchprobieren aller möglichen Schlüssel besteht.

Brute Force-Attacke
Ein Angriff auf einen kryptographischen Algorithmus, bei dem man den gesamten Schlüsselraum systematisch absucht.

Byte
Eine Gruppe von acht Bits.

CBC
siehe *Cipher Block Chaining*

CFB
siehe *Cipher Feedback*

Chiffrat
Synonym für Geheimtext.

Chiffre
Eine Chiffre ist das Verfahren, bzw. der Algorithmus zum Ver- und Entschlüsseln von Daten. Es wird weiter unterschieden in asymmetrische und symmetrische Chiffre, diese unterteilen sich wiederum in Block- und Stromchiffren.

Chosen Plaintext Attack
Bezeichnung für die Situation, dass ein Angreifer beim Angriff auf eine Chiffre in der Lage ist, den zu verschlüsselnden Text frei zu wählen.

Cipher Block Chaining (CBC)
Blockchiffriermodus, der den vorangehenden Chiffretextblock mit dem aktuellen Klartextblock kombiniert, bevor er ihn verschlüsselt; dieser Modus wird sehr häufig benutzt.

Cipher Feedback (CFB)
Blockchiffriermodus, bei dem der zuletzt verschlüsselte Chiffretextblock in die Blockchiffrierung einbezogen wird, um den Schlüssel zu erzeugen, mit dem der nächste Chiffretextblock chiffriert wird.

Ciphertext Only-Attack
siehe *Geheimtextangriff*

Data Encryption Algorithm (DEA)
Verschlüsselungsalgorithmus, der beim DES verwendet wird.

Data Encryption Standard (DES)
Symmetrisches Verschlüsselungsverfahren mit 56-Bit-Schlüssel. Im Jahr 1974 von IBM im Auftrag der US-Regierung entwickelt, anschließend von der National Security Agency (NSA) leicht modifiziert veröffentlicht und 1977 zum Standard ernannt. Ein Vorteil des DES liegt in der hohen Performance. Das Verfahren ist durch den AES ersetzt worden.

differentielle Kryptoanalyse
Angriffsmethode auf eine Chiffre. Es werden Paare von Geheimtexten untersucht, deren Klartexte bestimmte Differenzen aufweisen. Dabei geht es darum, aus den Unterschieden im Klartext auf Unterschiede im verschlüsselten Text zu stoßen und damit Rückschlüsse auf den verwendeten Schlüssel ziehen zu können.

Diffusion
Neben der Konfusion eines der beiden grundlegenden Prinzipien beim Design von Verschlüsselungsalgorithmen. Man versucht (z.B. durch Permutation, d.h. Vertauschen von Klartextteilen) die Redundanz des Klartexts über den Chiffretext zu verteilen.

digitale Signatur
Das Gegenstück zu einer handschriftlichen Unterschrift für Dokumente, die in digitaler Form vorliegen. Die digitale Signatur soll Sicherheit bei den folgenden Fragestellungen erbringen:

- Die Authentifizierung, d.h. die Sicherheit über den Absender des Dokumentes
- Die Integrität des Dokumentes soll gewährleistet werden
- Die Verbindlichkeit; d.h. der Absender soll die Erstellung nicht bestreiten können

Diese Eigenschaften können mit Hilfe asymmetrischer Verfahren erreicht werden. Mit Hilfe des geheimen Schlüssels werden Informationen erzeugt, anhand derer eine dritte Person sich unter Kenntnis des zugehörigen öffentlichen Schlüssels von der Korrektheit überzeugen kann. Für die bekannten asymmetrischen Verschlüsselungsverfahren, wie z.B. RSA, existieren Protokolle, um sie zur Erstellung von digitalen Signaturen einzusetzen.

Electronic Code Book (ECB)
Beim ECB-Modus einer Blockchiffre wird jeder Klartextblock einfach in den entsprechenden Chiffreblock verschlüsselt. Die Konsequenz ist, dass

identische Nachrichtenblöcke auch in gleiche Chiffretexte überführt werden, weshalb diese Vorgehensweise nur unter bestimmten Umständen als sicher gelten kann.

endlicher Körper
Eine mathematische Struktur mit endlich vielen Elementen, in denen die üblicherweise bekannten Rechenregeln für Addition, Subtraktion, Multiplikation und Division gelten.

Enigma
Berühmte deutsche Chiffriermaschine, mit deren Hilfe ein erheblicher Teil des deutschen Nachrichtenverkehrs (insbesondere der deutschen U-Boote) im 2. Weltkrieg chiffriert wurde.

Entropie
Die Entropie einer Nachrichtenquelle mißt die Informationen, die man durch Beobachten der Quelle durchschnittlich bekommen kann, oder umgekehrt die Unbestimmtheit, die über die erzeugte Nachricht herrscht, wenn man die Quelle nicht beobachten kann.

Entschlüsselung
Als Entschlüsselung bezeichnet man die Transformation des Geheimtextes in den Klartext. Die unbefugte Entschlüsselung wird auch als Brechen des Codes bezeichnet.

exhaustive Schlüsselsuche
Unter dem exhaustiven Durchsuchen des Schlüsselraums versteht man die Methode der Kryptonanalyse, alle Schlüssel durchzuprobieren.

Fast Encryption Algorithm (FEAL)
Blockalgorithmus, der ursprünglich als DES-Ersatz gedacht war, sich aber als unsicher herausstellte.

Federal Information Processing Standard (FIPS)
Vom NIST herausgegebene Standards, denen die Computersysteme der US-Regierung genügen sollen.

Feistel-Chiffre
Ein wesentliches Problem bei der Chiffrierung von Daten ist, dass die Verschlüsselungsfunktion umkehrbar sein muss, um eine korrekte Entschlüsselung von Texten zu ermöglichen. Bei Feistel-Chiffren wird diese Anforderung durch ein bestimmtes Design sichergestellt.

F-Funktion
Die Hauptoperation in einer Runde eines DES-ähnlichen Kryptosystems wird F-Funktion genannt. Es ist die Rolle der F-Funktion, die Daten mit den Unterschlüsseln zu mischen.

FIPS
siehe *Federal Information Processing Standard*

Geburtstagsangriff
Kryptanalytischer Angriff, der das sogenannte Geburtstagsparadox nutzt: Die Wahrscheinlichkeit, dass in einer Gruppe von 23 Personen zwei oder mehr am gleichen Tag Geburtstag haben, ist größer als 0,5!

geheimer Schlüssel
Bei symmetrischen Verschlüsselungsverfahren wird der verwendete Schlüssel auch als geheimer Schlüssel bezeichnet. Bei asymmetrischen Verschlüsselungsverfahren wird der geheime Schlüssel im Gegensatz zum öffentlichen Schlüssel vom Inhaber geheimgehalten.

Geheimtext
Der Geheimtext ist das Ergebnis der Verschlüsselung eines Dokumentes. Das unverschlüsselte Dokument bezeichnet man als Klartext.

Geheimtextangriff
Sofern für eine Kryptoanalyse nur Geheimtexte herangezogen werden, wird dies als Geheimtextangriff (engl. ciphertext-only-attack) bezeichnet. Der Angreifer muss versuchen, auf die zugehörigen Klartexte zu schließen und möglichst auch den benutzten Schlüssel bestimmen. Hierfür werden insbesondere statistische Analysen des Geheimtextes herangezogen.

Integrität
Entstammt dem lateinischen Wortschatz und ist abgeleitet von „integer“, das soviel bedeutet wie unangetastet, unverletzt, unbefleckt, rein. Der Begriff steht im Kontext der Verschlüsselung für die Unversehrtheit von kommunizierten Informationen. Dies bedeutet, dass der Informationsinhalt während eines Kommunikationsvorgangs keine Veränderung erfahren hat und damit auf Sender- und Empfängerseite absolut identisch ist.

International Data Encryption Algorithm
IDEA (International Data Encryption Algorithm) ist eine symmetrische Blockchiffre mit 64 Bit Blocklänge und einer Schlüssellänge von 128 Bit. Er wurde Anfang der 90er Jahre von X. Lai und J. Massey entwickelt. Bekannt geworden ist dieser Algorithmus vor allem durch die Verwendung innerhalb von PGP.

iteratives Kryptosystem
Ein Kryptosystem, das auf der vielfachen Iteration einer relativ schwachen Rundenfunktion basiert.

Kerckhoffs Maxime
Ein wichtiges Prinzip bei der Beurteilung von kryptographischen Algorithmen: Die Sicherheit des Verfahrens sollte nicht darauf beruhen, dass dieses geheim gehalten wird, sondern einzig und allein auf dem verwendeten Schlüssel.

Klartext
Die Original- oder Klarform verschlüsselter Daten, die durch die Benutzung eines Kryptosystems und eines Schlüssels in einen Geheimtext umgewandelt wird.

Klartextangriff
Ein Angriff der Kryptonanalyse, bei dem zusätzlich zum Geheimtext der Klartext zur Verfügung steht, wird als Klartextangriff bezeichnet.

Konfusion
Neben der Diffusion eines der beiden grundlegenden Prinzipien beim Design von Verschlüsselungsalgorithmen. Ziel ist das Verbergen von Redundanzen im Klartext. Eine Möglichkeit ist beispielsweise die Substitution von verschiedenen Klartextblöcken durch andere.

Kryptoanalyse
Abgeleitet wurde der Begriff aus dem Griechischen. Dabei steht „kryptos“ für geheim und „analyein“ für auflösen. Im ursprünglichen Sinne handelt es sich folglich um die Kunst des Auflösens von Geheimem, z.B. geheimer Schrift. Die Kryptoanalyse ist eine Teildisziplin der Kryptologie. Es handelt sich hierbei um die Kunst, Daten und Informationen aus Geheimtexten — auch ohne Kenntnis des verwendeten Schlüssels — zu rekonstruieren.

Kryptographie
Abgeleitet wurde der Begriff aus dem Griechischen. Dabei steht „kryptos“ für geheim und „graphein“ für schreiben. Im ursprünglichen Sinne handelt es sich folglich um die Kunst der Geheimschrift. Die Kryptographie ist eine Teildisziplin der Kryptologie. Es handelt sich hierbei um die Kunst, Daten und Informationen zu verschlüsseln. Das bedeutet, dass man aus einer Originalinformation, dem sogenannten Klartext, eine verschlüsselte Information, den sogenannten Chiffriertext, erzeugt. Zu diesem Zweck sind entsprechende Prozeduren, Verfahren und Systeme zu entwickeln.

Kryptologie
Kryptologie ist der Oberbegriff für Kryptographie und Kryptanalyse.

Lawineneffekt
Der Lawineneffekt (engl. avalanche effect) bezeichnet den Umstand, daß sich bei einer guten Chiffre Änderungen im Klartext möglichst schnell (innerhalb weniger Rundenfunktionen) auf den gesamten Chiffretext auswirken.

lineare Kryptoanalyse
Angriffsmethode auf eine Chiffre. Man versucht, lineare (einfache) Abhängigkeiten zwischen den Bits des Klartextes und des Chiffretextes zu entdecken und auszunutzen, um Informationen über den Schlüssel zu erhalten.

Lucifer
Verschlüsselungsverfahren, das in den 70er Jahren von IBM entwickelt wurde. Der DES basiert auf Lucifer.

Mehrfachverschlüsselung
Wiederholtes Verschlüsseln eines Textes mit dem gleichen oder mit verschiedenen Chiffrieralgorithmen. In den meisten Fällen erhöht sich dadurch vermutlich die Sicherheit. Bekanntestes Beispiel für Mehrfachverschlüsselung: Triple-DES.

National Bureau of Standards (NBS)
Das US-Institut, das den DES-Algorithmus standardisiert hat. Später wurde der Name in National Institute of Standards and Technology (NIST) umgeändert.

National Institute of Standards and Technology (NIST)
National Institute of Standards and Technology. US-amerikanisches Institut für die Technologie-Standardisierung. Vom NIST werden die FIPS-Standards herausgegeben.

National Security Agency (NSA)
Die National Security Agency ist der Geheimdienst der USA, der für geheime Informationssicherung und -beschaffung zuständig ist.

negative Mustersuche
Bei einigen Verschlüsselungsverfahren (z.B. Enigma) wird kein Zeichen in sich selbst überführt. Damit lassen sich gewisse Stellungen von Mustern im Klartext ausschließen, was manchmal schon die Kryptanalyse ermöglicht. Spielt in der klassischen Kryptologie eine Rolle; bei heutigen Algorithmen auf Grund des Lawineneffekts wahrscheinlich ohne Bedeutung.

OFB
siehe *Output Feedback*

öffentlicher Schlüssel
Ein Schlüssel des Schlüsselpaares bei asymmetrischen Verschlüsselungsverfahren, der öffentlich verteilt wird. Der öffentliche Schlüssel kann zur Chiffrierung von Daten verwendet werden, die aber nur sein Inhaber mit seinem privaten (geheimen) Schlüssel dechiffrieren kann.

One-Time-Pad
Die einzig beweisbar sichere Art der Verschlüsselung von Daten, die auf einem nur einmal verwendeten, zufälligen Schlüssel basiert, der dieselbe Länge wie der zu verschlüsselnde Klartext hat. Die Klartextbits werden mit den entsprechenden Schlüsselbits addiert (XOR), um den Chiffretext zu erhalten; nochmalige Addition der Schlüsselbits ergibt wieder den Klartext.

Operationsmodi
Art und Weise, in der Kryptosysteme genutzt werden können, um viele Klartexte zu verschlüsseln. Der einfachste Modus ist der Electronic Code Book (ECB) Modus, in dem alle Klartextblöcke in einer Nachricht separat mit demselben Schlüssel verschlüsselt werden.

Output Feedback (OFB)
Blockchiffriermodus, bei dem das Verschlüsselungsverfahren zur Erzeugung des Schlüsselstroms verwendet wird.

Parität
Unter Parität bzw. Paritätsbits versteht man Zusatzinformationen zur Sicherung der Integrität von elektronischen Dokumenten.

Plaintext
Englisch für Klartext.

Pretty Good Privacy (PGP)
Pretty Good Privacy ist ein Programm von P. Zimmermann zum Verschlüsseln und Signieren von E-Mails; vor allem durch die Verbreitung dieses Programms wurde ab ungefähr 1994 der Gebrauch von Public Key-Verfahren populär.

Primzahl
Eine natürliche Zahl, die nur durch 1 und sich selbst ohne Rest teilbar ist.

Private Key
siehe *geheimer Schlüssel*

Private-Key-Verschlüsselungsverfahren
siehe *symmetrische Verschlüsselungsverfahren*

privater Schlüssel
siehe *geheimer Schlüssel*

Produktchiffre
Da einfache Transpositions- und Substitutionschiffren für sich genommen nicht sehr sicher sind, kommen in der Praxis Varianten zum Einsatz, die schwerer zu analysierende Abbildungen erzeugen. Oft werden auch beide Chiffrearten miteinander zu den sogenannten Produktchiffren kombiniert, um die Komplexität weiter zu steigern.

Public Key
siehe *öffentlicher Schlüssel*

Public Key Kryptographie
siehe *asymmetrische Verschlüsselungsverfahren*

Public Key Infrastruktur (PKI)
Das größte Problem beim Einsatz von asymmetrischen Verschlüsselungsverfahren stellt die Authentizität von Schlüsseln dar. Dahinter verbirgt sich die Frage, wie gewährleistet werden kann, dass der vorliegende Schlüssel wirklich vom gewünschten Kommunikationspartner stammt. Eine PKI ist eine Kombination aus Hardware- und Software-Komponenten, Policen und verschiedenen Prozeduren. Sie basiert hauptsächlich auf sogenannten Zertifikaten; diese sind ihrerseits durch digitale Signaturen von einer vertrauenswürdigen Instanz beglaubigte Schlüssel der Kommunikationspartner.

Rijndael
Rijndael ist ein von Joan Daemen und Vincent Rijmen entwickeltes Verfahren zur Blockverschlüsselung, das im AES verwendet wird.

Rivest, Shamir, Adleman (RSA)
Asymmetrisches Verschlüsselungsverfahren, das Daten ver- und entschlüsseln sowie digitale Signaturen erstellen und überprüfen kann. Es ist das bekannteste asymmetrische Verschlüsselungsverfahren und trägt die Namen seiner Erfinder. Die Vermarktungsrechte des RSA-Algorithmus liegen bei der Firma RSA Data Security.

ROT13
Caesar-Verschlüsselung, bei der jeder Buchstabe durch seinen 13. Nachfolger ersetzt wird. Zweimalige Anwendung des Verfahrens liefert den Ausgangstext zurück. ROT13 soll keine kryptologische Sicherheit bieten, sondern das unerwünschte Herauslesen von Zeichenketten aus Programmtexten etwas erschweren (Anwendung in Newsreadern).

Rundenschlüssel
Rundenschlüssel sind Werte, die aus dem Chiffrierschlüssel durch Anwendung einer Schlüsselerweiterungsroutine generiert werden; sie werden bei den jeweiligen Runden der Chiffre und der inversen Chiffre angewandt.

S-Box
siehe *Substitutionsbox*

Schlüssel
Im Rahmen eines Verschlüsselungsverfahrens ist ein Schlüssel eine Information, die zur Verschlüsselung eines Klartextes bzw. zur Entschlüsselung eines Geheimtextes verwendet wird.

Schlüsselaustausch
Der Einsatz symmetrischer Chiffrierverfahren verlangt, dass sich zwei Kommunikationspartner auf einen gemeinsamen, nur ihnen bekannten Schlüssel einigen. Die Schwierigkeit dabei besteht darin, dass für den Austausch solcher Informationen heutzutage meist nur bedingt sichere Kanäle vorhanden sind. Protokolle für den Schlüsselaustausch müssen also so verfaßt sein, dass nur Informationen ausgetauscht werden, aus deren Kenntnis

kein Wissen über das eigentliche Geheimnis (den Schlüssel) resultiert. Das bekannteste derartiger Protokolle ist das sog. Diffie-Hellman-Verfahren, dessen Vorstellung 1976 als Geburtsstunde der Public Key-Kryptographie bezeichnet werden kann.

Schlüsselraum
Als Schlüsselraum bezeichnet man die Menge aller Schlüssel, mit denen ein Verschlüsselungsverfahren arbeitet.

schwache Verschlüsselung
Im Gegensatz zu starker Verschlüsselung versteht man unter schwacher Verschlüsselung Verfahren, die mit vertretbarem Aufwand durch Verfahren der Kryptoanalyse gebrochen werden können.

Secret Key
siehe *geheimer Schlüssel*

Skipjack
Von der NSA entwickelte Blockchiffrierung, die in den Capstone- und Clipper-Chips und in der Fortezza-Karte verwendet wird.

starke Verschlüsselung
Im Gegensatz zu schwacher Verschlüsselung versteht man unter starker Verschlüsselung Verfahren, die nicht mit vertretbarem Aufwand durch Verfahren der Kryptoanalyse gebrochen werden können.

Steganographie
Steganographie ist die Wissenschaft vom Verbergen von Informationen in einer anderen Information. Die versteckte Information kann nur unter Zuhilfenahme von zusätzlichen Schlüsselinformationen sichtbar gemacht werden.

Stromchiffre
Bei einer Stromchiffre wird die zu verschlüsselnde Nachricht als Datenstrom aufgefasst und zeichenweise mit einem Schlüsselstrom verknüpft. Der Schlüsselstrom ist in der Regel eine Pseudozufallsfolge, die nur mit Kenntnis des geheimen Schlüssels erzeugt werden kann. Im Gegensatz zu Blockchiffren ist die Verschlüsselung bei Stromchiffren positionsabhängig. Ein beliebiger Abschnitt eines Chiffretextes kann nicht entschlüsselt werden, ohne den vorhergehenden Teil zu entschlüsseln.

Substitutionsbox (S-Box)
Durch eine S-Box werden Eingabezeichen durch Ausgabezeichen ersetzt, die dazu benutzten Umsetzungsfunktionen haben die unterschiedlichsten Komplexitäten. In der modernen Kryptografie werden S-Boxen von vielen Verfahren eingesetzt, wobei die interne Realisierung unterschiedlich ist. Eine S-Box ist beim Data Encryption Standard nichts weiter als eine Tabelle, die durch den Eingabewert indiziert wird. Die Tabelleneinträge sind

konstant und durch den Standard definiert. In der Regel sind S-Boxen so konstruiert, dass sie leicht in Hardware zu implementieren sind.

Substitutionschiffre
Bei einer Substitutionschiffre wird ein Zeichen eines Klartextes durch ein zugeordnetes Chiffrezeichen ersetzt. Monoalphabetische Substitutionen sind sehr anfällig für Angriffe, die auf statistischen Analysen basieren. Etwas sicherer sind die polyalphabetischen Chiffren, sofern die Schlüsselwörter lang genug sind und nicht zu viele Nachrichten mit gleichem Schlüssel ausgetauscht werden.

symmetrische Chiffre
Verschlüsselungsverfahren, bei dem zur Chiffrierung und zur Dechiffrierung derselbe Schlüssel verwendet wird (oder bei dem diese zwei Schlüssel einfach voneinander ableitbar sind).

Timing Attack
Dieser Angriff basiert darauf, Rückschlüsse auf die Schlüsselgenerierung zu ziehen, in dem das zeitliche Verhalten der Verschlüsselungsprogramme analysiert wird. Einzusetzen ist diese Angriffsart bei allen Verschlüsselungsverfahren, insbesondere symmetrischen Verfahren, mit unterschiedlichem Zeitbedarf für die kryptografischen Basisoperationen. Hieraus können sich statistisch auswertbare Differenzen beispielsweise für Rotationen oder Tabellenzugriffe ergeben.

Transpositionschiffre
Mittels einer Transpositionschiffre wird ein Klartext in einen Chiffretext umgewandelt, indem nicht die einzelnen Zeichen ersetzt werden, sondern die Stellung der Zeichen zueinander, also die Anordnung der Zeichen verändert wird. Ein Beispiel für eine reine Transpositionschiffre ist die Skytala.

Triple-DES
Die Bezeichnung für Varianten des DES, welche die Probleme aufgrund der zu geringen Schlüssellänge beheben sollen; der DES-Algorithmus wird dabei dreimal hintereinander mit verschiedenen Schlüssel angewendet. Es gibt verschiedene Varianten welche sich z.B. in der Anzahl der verwendeten Schlüssel unterscheiden. Die gebräuchlichste (und auch durch ANSI standardisierte Methode) ist das EDE-Verfahren: Dabei wird mit dem ersten Schlüssel chiffriert (encrypted), mit dem zweiten Schlüssel dechiffriert (decrypted) und noch einmal mit dem ersten Schlüssel verschlüsselt (encrypted). Die effektive Schlüssellänge beträgt in diesem Fall also 112 Bit; es gibt aber auch Varianten mit 3 verschiedenen Schlüsseln, also 168 Bit Schlüssellänge.

Vernam-Chiffrierung
Chiffrierung, die zur Verschlüsselung von Fernschreiben entwickelt wurde, wobei die Datenbits mit den Schlüsselbits addiert (XOR) werden.

Verschlüsselung
: Verschlüsselung ist die Transformation einer Nachricht, Klartext genannt, in eine andere, nicht ohne zusätzliche Schlüsselinformation lesbare Nachricht, den Geheimtext.

XOR-Verknüpfung
: Rechenoperation auf Bits, bei der zwei Bits addiert werden und der Übertrag ignoriert wird.