

# **Glossar der wichtigsten Fachbegriffe der Kryptografie**

## **Hinweis**

Im folgenden werden eine ganze Reihe wichtiger Fachbegriffe aus der Kryptologie jeweils kurz erklärt. Die einzelnen Begriffe werden aber nur kurz erläutert, um sie in einem Textzusammenhang besser verstehen zu können. Für eine ausführliche Beschreibung, z. B. zur Funktionsweise der verschiedenen Algorithmen, sollte man allerdings in der entsprechenden Fachliteratur nachschlagen.

<b>Hinweis</b>	<b>1</b>
<b>A</b>	<b>5</b>
AES	5
Alice	5
Asymmetrische Verschlüsselung	5
<b>B</b>	<b>5</b>
Blockchiffre	5
Blowfish	5
Bob	5
Brute-Force Angriff	5
<b>C</b>	<b>6</b>
Caesar-Chiffre	6
CBC	6
Certificate Authority	6
Charly	6
Chiphertext	6
Chosen-Chiphertext-Attack	6
Code	7
CRT	7
<b>D</b>	<b>7</b>
DES	7
Diffie-Hellman-Schlüsseltausch	7
Digest	7
Digitale Signatur	8
<b>E</b>	<b>8</b>
ECB	8
ECC	8
Elgamal	8
Enigma	8
<b>F</b>	<b>9</b>
Faktorisierungsproblem	9
<b>G</b>	<b>9</b>
Geheimtext	9
<b>H</b>	<b>9</b>
Hash	9
<b>I</b>	<b>9</b>
Initialisierungsvektor (IV)	10
<b>J</b>	<b>10</b>

JSSE	10
<b>K</b>	<b>10</b>
Klartext	10
Known-Chiphertext-Attack	10
Known-Plaintext-Attack	10
<b>L</b>	<b>11</b>
<b>M</b>	<b>12</b>
MD2	12
MD4	12
MD5	12
<b>N</b>	<b>12</b>
National Institute of Standards and Technology	12
<b>O</b>	<b>12</b>
One-Time-Pad	12
OpenSSL	13
<b>P</b>	<b>13</b>
PGP	13
Plaintext	13
<b>Q</b>	<b>13</b>
Quantenkryptografie	13
<b>R</b>	<b>13</b>
RC4	14
RC5	14
Rijndael	14
RIPEMD-160	14
RSA	14
<b>S</b>	<b>15</b>
Serpent	15
SHA	15
Skytale	15
Smartcard	15
SSL	16
Stromchiffre	16
Substitutionschiffre	16
Symmetrisches Verschlüsselungsverfahren	16
<b>T</b>	<b>16</b>
TLS	17
Transpositionschiffre	17

<b>Twofish</b>	<b>17</b>
<b>U</b>	<b>17</b>
<b>V</b>	<b>17</b>
<b>Vernam-Verschlüsselung</b>	<b>17</b>
<b>Vigenère-Chiffre</b>	<b>17</b>
<b>W</b>	<b>17</b>
<b>X</b>	<b>17</b>
<b>Y</b>	<b>18</b>
<b>Z</b>	<b>18</b>
<b>Zertifikat</b>	<b>18</b>
<b>Quellen</b>	<b>19</b>
<b>Wikipedia</b>	<b>19</b>
<b>Kryptografie in Theorie und Praxis</b>	<b>19</b>
<b>Handbook of Applied Cryptography</b>	<b>19</b>

## A

### AES

Der Algorithmus Rijndael wurde im Jahr 2000 zum Advanced Encryption Standard erhoben, der die Nachfolge des bisher genutzten *DES* antreten soll, da dieser Algorithmus mit Schlüsselgrößen von 56 (Single-DES), 112 und 168 Bits (Triple-DES) leider nicht mehr als sicher eingestuft werden kann. AES bietet daher Schlüsselgrößen von 128, 192 und 256 Bit und damit einen erheblich größeren Schlüsselraum als *DES*.

### Alice

Alice ist ein in vielen Büchern oder Veröffentlichungen über Kryptologie verwendeter Name für die Person, die eine vertrauliche Informationen austauschen möchte.

## Asymmetrische Verschlüsselung

Bei asymmetrischen Verschlüsselungsverfahren werden im Gegensatz zu *symmetrischen Verschlüsselungsverfahren*, bei denen ein und derselbe Schlüssel sowohl zum Ver- als auch zum Entschlüsseln verwendet wird, zwei verschiedene Schlüssel benutzt. Da einer der beiden Schlüssel öffentlich sein kann, werden solche Verfahren auch bei *digitalen Signaturen* verwendet. Der sogenannte öffentliche Schlüssel (Public Key) wird zum Verschlüsseln oder Verifizieren einer *digitalen Signatur*, der private Schlüssel (Private Key) zum Entschlüsseln oder *digitalen Signieren* eingesetzt. Beispiele für asymmetrische Verschlüsselungsalgorithmen sind *RSA*, *ECC* und *Elgamal*.

## B

### Blockchiffre

*Symmetrisches Verschlüsselungsverfahren*, bei denen der zu verschlüsselnde Text in Blöcke bestimmter Länge (z. B. 64 Bit) eingeteilt und jeder Block einzeln verschlüsselt wird, werden als Blockchiffre bezeichnet. Bekannte Beispiele für solche Blockchiffren sind *DES* und *AES*.

### Blowfish

Bei Blowfish handelt es sich um einen von Bruce Schneier im Jahr 1993 entwickeltes, nicht patentiertes *Symmetrisches Verschlüsselungsverfahren* mit einer Blocklänge von 64 Bit und variablen Schlüssellängen von 32 bis 448 Bit, der insbesondere auf 32 Bit-Prozessoren besonders performant arbeitet.

### Bob

Bob ist ein in vielen Büchern oder Veröffentlichungen über Kryptologie verwendeter Name für die Person, die die vertraulichen Informationen von *Alice* erhalten soll.

## Brute-Force Angriff

Das Durchprobieren aller möglichen Schlüssen für einen Verschlüsselungsalgorithmus wird als Brute-Force Angriff bezeichnet. Ein Verschlüsselungsalgorithmus kann dann als sicher bezeichnet werden, wenn der Brute-Force Angriff der einzige mögliche Angriff ist, um den Schlüssel zu finden.

## C

### Caesar-Chiffre

Beim Caesar-Chiffre handelt es sich um ein Verschlüsselungsverfahren, das wahrscheinlich auch von dem römischen Staatsmann und Feldherr Gaius Julius Caesar eingesetzt wurde. Hierbei werden alle Buchstaben durch denjenigen ersetzt, der eine bestimmte Anzahl von Stellen später (z. B. 3) im Alphabet steht. Da also jeder Buchstabe durch seinen Geheimbuchstaben ersetzt wird, ist der Caesar-Chiffre ein Beispiel für einen *Substitutionschiffre*.

## CBC

Der Cipher Block Chaining (CBC) Mode ist ein Verfahren für symmetrische *Blockchiffren*, bei denen jeder *Klartextblock* vor der Verschlüsselung mit dem zuvor verschlüsselten Block durch eine Exklusiv-Oder-Funktion (XOR) verknüpft wird. Beim ersten Block wird hierfür ein sogenannter *Initialisierungsvektor (IV)* verwendet. Der CBC ist deshalb sicherer als der einfache *ECB*, weil hierbei regelmäßige Muster im Klartext, die z. B. durch immer wiederkehrende Textphrasen entstehen, verschleiert werden.

### Certificate Authority

Eine Certificate Authority (CA) ist eine anerkannte Organisation, die *Zertifikat* ausstellt. Ein *Zertifikat* ist eine Art elektronischer Ausweis und dient dazu sich beispielsweise im Internet als vertrauenswürdiger Kommunikationspartner auszuweisen. Wenn eine Person oder eine Organisation ein *Zertifikat* bei einer CA beantragt, muss sie deshalb ihre Identität gegenüber der CA nachweisen. Die CA unterschreibt das ausgestellte *Zertifikat* mit ihrer *Digitale Signatur*. Auch eine Certificate Authority besitzt ein *Zertifikat*, das sie allerdings selbst unterschrieben hat. Ein solches *Zertifikat* wird als "self-signed Certificate" bezeichnet. Die selbst-signierten *Zertifikate* bekannter CAs, z. B. [\*Versign\*](#) oder [\*Thawte\*](#), sind als Wurzel-Zertifikate (Root-Certificates) bereits bei vielen Browsern vorinstalliert, so dass verschlüsselten Seiten (siehe *SSL*), deren *Zertifikate* von einer bekannten CA signiert wurden, ohne Nachfrage vertraut wird.

## Charly

Charly ist ein in vielen Büchern oder Veröffentlichungen über Kryptologie verwendeter Name für die Person, die versucht, durch diverse Angriffe Informationen über die Kommunikation zwischen *Alice* und *Bob* zu bekommen.

### Chiphertext

Englischer Fachbegriff für den verschlüsselten Text (deutsch: *Geheimtext*).

### Chosen-Chiphertext-Attack

Bei einem solchen Angriff ist der Angreifer in der Lage, aus einer Reihe frei wählbarer *Geheimtexte* die zugehörigen *Klartexte* zu generieren. Diese Datenpaare sowie die Kenntnis des verwendeten Verschlüsselungsalgorithmus lassen dann auch Rückschlüsse auf den verwendeten Schlüssel zu.

## Code

In der Kryptographie werden unter Codes meist Verschlüsselungsverfahren verstanden, bei denen ganze Wörter durch bestimmte andere Wörter ersetzt werden.

## CRT

Das Chinese Remainder Theorem (CRT) ist ein Verfahren für die Anwendung des *RSA*-Verschlüsselungsalgorithmus, bei dem statt des privaten Exponenten und des Modulus die beiden Primzahlen  $p$  und  $q$ , zwei Primexponenten  $dp$  und  $dq$  und ein sogenannter CRT-Koeffizient zur Berechnung einer Private-Key-Operation verwendet werden. Der Vorteil dieser Methode ist zum einen die höhere Geschwindigkeit, mit der solche Operationen ausgeführt werden können, zum anderen die Länge der verwendeten Komponenten, die nur die Hälfte der eigentlichen Schlüssellänge beträgt.

## D

## DES

Der Data Encryption Standard wurde im Jahre 1973 von der Firma IBM (International Business Machines) in Zusammenarbeit mit der NSA (National Security Agency) mit dem Ziel entwickelt, einen einheitlichen Standard für einen kryptografischen Algorithmus zu schaffen. DES ist ein *symmetrischer Verschlüsselungsalgorithmus*, der trotz seiner geringen Schlüssellänge von nur 56 Bit eine höhere Sicherheit bietet als der Algorithmus Lucifer (128 Bit Schlüssellänge), auf dem er basiert. Beim heute immer noch zur Anwendung kommenden Triple-DES wird der Klartext mit einem ersten Schlüssel verschlüsselt, mit einem zweiten (vom ersten natürlich verschiedenen) Schlüssel wieder entschlüsselt und mit einem dritten Schlüssel wieder verschlüsselt. So kann die Schlüssellänge auf bis zu 168 Bit vergrößert werden. Sind der erste und der dritte Schlüssel nicht identisch, so spricht man auch vom 3-Key Triple-DES mit einer Schlüssellänge von 168 Bit, während beim normalen Triple-DES der erste und der dritte Schlüssel identisch sind, so dass die Schlüssellänge nur 112 Bit beträgt. Trotz dieser Verbesserungen gilt DES wegen seiner geringen Schlüssellänge nicht mehr als sicher und soll in naher Zukunft vom *AES* abgelöst werden.

## Diffie-Hellman-Schlüsseltausch

Der Diffie-Hellman-Algorithmus kann für einen sicheren Austausch von Schlüsseln für *Symmetrisches Verschlüsselungsverfahren* über ein unsicheres Medium eingesetzt werden, da die hierbei von den Kommunikationspartnern ausgetauschten Daten nicht ausreichen, um damit den eigentlichen Schlüssel zu berechnen. Dieses Verfahren wurde 1976 veröffentlicht, nachdem es von Martin Hellman gemeinsam mit Whitfield Diffie und Ralph Merkle an der Universität von Stanford (Kalifornien) entwickelt worden war. Es ist kein Verschlüsselungsalgorithmus im eigentlichen Sinne, beruht aber auf dem mathematischen Problem der Berechnung diskreter Logarithmen, auf dem beispielsweise auch die *Asymmetrische Verschlüsselung ECC* und *Elgamal* basieren.

## Digest

Als Digest wird das Zwischenergebnis eines *Hash* bezeichnet, das auf den nächsten Datenblock wartet. Die Abkürzung MD (z. B. in den Namen der *Hashalgorithmen MD2, MD4* und *MD5*) steht deshalb auch für Message Digest.

## Digitale Signatur

Die Digitale Signatur oder digitale Unterschrift wird eingesetzt, um sicherzustellen, dass ein Dokument wirklich vom angegebenen Sender stammt. Meistens wird hierfür der *Hash* des zu signierenden Textes berechnet, der dann wiederum mit dem privaten Schlüssel des Senders verschlüsselt wird. Der Empfänger kann dann ebenfalls den *Hash* des Textes berechnen, die empfangene Signatur mit dem öffentlichen Schlüssel des Senders entschlüsseln und mit dem berechneten *Hash* vergleichen. Sind diese identisch, so kann der Empfänger sowohl sicher sein, dass der Text vom angegebenen Sender stammt, denn nur dieser kennt den privaten Schlüssel, als auch, dass der Text nicht verändert wurde, denn sonst hätte er einen anderen *Hash* errechnet.

## E

### ECB

Der Electronic Code Block (ECB) Mode ist ein Verfahren für symmetrische *Blockchiffre*, bei welchen jeder Block einzeln und unabhängig von den anderen Blöcken verschlüsselt wird. Dies birgt die Gefahr in sich, dass bestimmte Muster aus dem Klartext auch im Geheintext erkennbar werden (z. B. bestimmte Textphrasen), weil diese immer gleich verschlüsselt werden. Diese Modus ist zwar in der Anwendung sehr einfach, allerdings auch relativ unsicher, weshalb bei den meisten *Blockchiffren* der sogenannte *CBC-Mode* zur Anwendung kommt.

### ECC

Die Elliptic Curve Cryptography (ECC) ist ein *Asymmetrische Verschlüsselung*, das auf der Mathematik elliptischer Kurven und dem damit verbundenen Problem des diskreten Logarithmus beruht. Vorteil von ECC gegenüber anderen *Asymmetrische Verschlüsselung* ist eine hohe Sicherheit bei vergleichsweise geringer Schlüssellänge. So bietet ein ECC-Schlüssel mit einer Länge von nur 160 Bit in etwa die gleiche Sicherheit wie ein *RSA-Schlüssel* mit einer Länge von 1024 Bit, weshalb dieses Verfahren gerne zur Anwendung kommt, wenn nur geringe Ressourcen zur Verfügung stehen, z. B. auf *Smartcards*.

## Elgamal

Das Elgamal-Kryptosystem (auch al-Dschamal-Kryptosystem) ist die Bezeichnung für ein *Asymmetrische Verschlüsselung*, welches im Jahr 1985 von Taher Elgamal (Tahir al-Dschamal) entwickelt wurde. Es basiert ähnlich wie der *Diffie-Hellman-Schlüsseltausch* oder der *ECC* auf dem mathematischen Problem zur Berechnung diskreter Logarithmen, unterliegt aber keinem Patent. Es kann sowohl zum Erzeugen *Digitale Signatur* als auch zum Ver- bzw. Entschlüsseln eingesetzt werden.

## Enigma

Die Enigma war eine im Jahr 1923 von dem Deutschen Arthur Scherbius konstruierte elektromechanische Chiffriermaschine, die durch ihren Einsatz zur Verschlüsselung des deutschen Funkverkehrs während des zweiten Weltkrieges bekannt wurde. Das Wort „Enigma“ kommt aus dem

Griechischen und bedeutet Rätsel. Da diese Maschine aber einige kryptographische Schwächen hatte und die Alliierten mit Hilfe ihrer Geheimdienste auch Kenntnisse über den Aufbau der verschiedenen Enigma-Maschinen hatten, konnten sie die meisten Teile des deutschen Funkverkehrs trotz einiger Verbesserungen durch deutsche Kryptologen gegen Ende des zweiten Weltkrieges entschlüsseln.

## F

### Faktorisierungsproblem

Als Faktorisierungsproblem wird in der Mathematik die Tatsache bezeichnet, dass es zwar relativ leicht ist, zwei Primzahlen miteinander zu multiplizieren, die Zerlegung des Produktes in seine Primfaktoren ist jedoch mit erheblichem Aufwand verbunden. Diese Tatsache machen sich beispielsweise der *Asymmetrische Verschlüsselung RSA* und das Rabin-Kryptosystem zu nutze. Haben beide Primzahlen etwa die gleiche Größenordnung (also etwa  $\sqrt{n}$ ), so müssen bei der sogenannten Probiervision alle Zahlen (eigentlich nur alle Primzahlen) bis  $\sqrt{n}$  durchprobiert werden. Auch wenn es inzwischen effektivere Faktorisierungsverfahren gibt, würden diese Jahrhunderte benötigen, um die in der Kryptologie verwendeten großen Zahlen in ihre Primfaktoren zu zerlegen.

## G

### Geheimtext

Geheimtext (engl.: *Chiphertext*) ist der deutsche Fachausdruck für die zu übertragene Information, nachdem sie verschlüsselt wurde.

## H

### Hash

Als Hash wird eine kryptografische Prüfsumme bezeichnet, die über eine lange Nachricht, die verschlüsselt oder auch unverschlüsselt übermittelt wird, berechnet wird, um sicherzustellen, dass die Nachricht während der Übertragung nicht verändert wurde. Solche Hashalgorithmen müssen sicherstellen, dass jede Veränderung am Text auch eine Veränderung der Prüfsumme bewirkt und es sehr schwierig ist, Kollisionen zu finden, also (sinnvolle) Texte, die die gleiche Prüfsumme erzeugen. Bekannte Hashalgorithmen sind *MD2*, *MD5* oder *SHA-1*, von denen aber insbesondere die beiden zuerst genannten nicht mehr als sicher gelten und auch der *SHA-1*, der wahrscheinlich immer noch meist genutzte Algorithmus, soll bald durch die sichereren Algorithmen *SHA-256*, *SHA-384* und *SHA-512* abgelöst werden. Ein weiterer, nicht patentgeschützter Hashalgorithmus ist *RIPEMD-160*.

## I

### Initialisierungsvektor (IV)

Der Initialisierungsvektor (IV, englisch: Initial Vector) ist der Wert, mit dem bei *Symmetrisches Verschlüsselungsverfahren* im *CBC-Modus* der erste Datenblock ver-X-odert wird, bevor er verschlüsselt werden kann.

## J

### JSSE

Die Java Secure Socket Extension (JSSE) ist ein API für die Verwendung des *SSL* Protokolls aus Java Programmen heraus. Während es in den ersten Java Versionen (bis V1.3) nur als zusätzliche Erweiterung des Java-APIs zur Verfügung stand, ist JSSE seit Version 1.4 fester Bestandteil des Standard Java-APIs. Sun stellt zwar eine Referenzimplementierung der Protokolle (*SSL V3* und *TLS*) und verschiedener Verschlüsselungsalgorithmen zur Verfügung, die aber auch durch Implementierungen anderer Anbieter ausgetauscht werden können.

## K

### Klartext

Klartext ist der deutsche Fachbegriff für die Information, die über ein unsicheres Medium übertragen werden soll, bevor sie verschlüsselt wird (engl.: *PGP*

*Pretty Good Privacy* (PGP) ist ein Programm zum sicheren Versand von eMails. Eine vom Sender gewählte Zufallszahl wird bei diesem Verfahren als Schlüssel für ein *Symmetrisches Verschlüsselungsverfahren*, z. B. *DES* oder *Triple-DES*, verwendet. Zur Übermittlung dieses Schlüssels an den Empfänger der Nachricht kommt dann ein *Asymmetrische Verschlüsselung* wie *Elgamal* oder *RSA* zum Einsatz. Der öffentliche Schlüssel des Empfängers wird verwendet, um den zufällig gewählten Schlüssel der *Symmetrisches Verschlüsselungsverfahren* zu verschlüsseln. Zur Authentisierung des Senders berechnet dieser vor der Verschlüsselung mit Hilfe des *SHA-1-Algorithmus* einen *Hash* über seine Nachricht und signiert diesen Hash mit seinem privaten Schlüssel. Zusätzlich kann auch noch nach der Berechnung des *Hash-Wertes* und vor der Verschlüsselung ein Komprimierungsverfahren angewendet werden.

Plaintext).

### Known-Chiphertext-Attack

Wenn nur der *Geheimtext* bzw. große Teile davon sowie der verwendete Verschlüsselungsalgorithmus bekannt sind, kann man versuchen, Regelmäßigkeiten zu finden, die z. B. durch immer wiederkehrende Wörter oder Phrasen im *Klartext* entstanden sind, und mit diesen Kenntnissen den verwendeten Schlüssel zu finden.

### Known-Plaintext-Attack

Wenn der Angreifer sowohl den *Geheimtext* als auch ein passendes Stück *Klartext* kennt, kann er diese Kenntnisse nutzen, um bei bekanntem Verschlüsselungsalgorithmus auf den verwendeten Schlüssel zu schließen. Eine solche Situation ist gar nicht einmal so unwahrscheinlich, da ein An-

greifer meistens zumindest grob weiß, worum es in dem Text geht, also Schlüsselworte kennt, und auch die Eröffnungs- oder Schlussfloskeln erraten kann.

## L

## M

### MD2

Der Message Digest 2 (MD2) ist ein für 8-Bit Rechner optimierter *Hash*-Algorithmus, der im Jahr 1988/89 von Ronald L. Rivest entwickelt wurde. Der Text muss vorher auf ein Vielfaches der Blocklänge von 16 Byte (128 Bit) ergänzt werden, was normalerweise durch das Anfügen so genannter Paddingbytes geschieht. Der *Hash* hat ebenfalls eine Länge von 16 Bytes (128 Bits). MD2 gilt inzwischen als veraltet und unsicher, da Methoden entdeckt wurden, um effektiv Kollisionen zu finden.

### MD4

Der Message Digest 4 (MD4) ist ein *Hash*-Algorithmus, der im Jahr 1990 von Ron Rivest mit dem Ziel entwickelt wurde, auf 32-Bit-Rechnern besonders schnell und gleichzeitig auch einfach implementierbar zu sein. Doch schon früh wurden in diesem Algorithmus Schwächen entdeckt, z. B. von Professor Hans Dobbertin, und selbst das "Cryptobytes Journal" der Firma *RSA* veröffentlichte eine Methode, mit der sich innerhalb von nur einer Stunde zwei bis auf ein Zeichen identische Nachrichten finden lassen, die den gleichen Hashwert erzeugen. Auch *RSA* rät von der Benutzung des MD4 ab und Rivest selbst bestätigt die Unsicherheit in "The *MD5* Message Digest Algorithm". Daher wurde MD4 schließlich als Public Domain lizenziert und bildete die Grundlage für viele weitere Hashfunktionen.

### MD5

Der Message Digest 5 (MD5) ist ein *Hash*, der im Jahr 1991 als sicherer Ersatz für die zuvor veröffentlichten *Hash MD2* und *MD4* von Ronald L. Rivest entwickelt wurde. Er erzeugt ebenfalls einen *Hash* mit einer Länge von 16 Bytes (128 Bits). Doch schon im Jahr 1996 fand Professor Hans Dobbertin eine Kollision in der Kompressionsfunktion des *MD5*, was zwar noch kein Angriff auf die vollständige MD5-Funktion war, doch im Jahr 2004 fanden chinesische Forscher Kollisionen für den vollständigen Algorithmus. MD5 gilt daher als nicht mehr sicher und es wird empfohlen, statt dessen eher die als sicher geltenden Algorithmen *SHA* oder *RIPEMD-160* zu verwenden.

## N

### National Institute of Standards and Technology

Das National Institute of Standards and Technology (NIST) ist eine Behörde des Wirtschaftsministeriums der USA mit Sitz in Gaithersburg und Boulder. Sie bestimmt auch Standards auf dem Gebiet der Verschlüsselungsalgorithmen. Sowohl der *DES* als auch der *AES* wurden vom NIST festgelegt.

## O

### One-Time-Pad

Das One-Time-Pad ist ein *Stromchiffre*, bei dem für jede neue Verschlüsselung ein neuer Schlüssel gewählt wird, der völlig zufällig ist, keine statistisch auswertbare Daten enthält und genauso lang wie der zu verschlüsselnde Text ist. Er bietet keine Angriffsmöglichkeiten für Formen der Kryptoa-

nalyse. Das One-Time-Pad ist somit mathematisch nachweisbar sicher, da jeder Schlüssel immer nur ein einziges Mal verwendet wird. Ein *Brute-Force Angriff* mit allen möglichen Schlüsseln würde zwar auch den richtigen Klartext liefern, aber auch alle anderen Nachrichten gleicher Länge. Größte Nachteile des One-Time-Pads sind jedoch die große Schlüssellänge und das damit verbundene Problem der sicheren Übertragung dieses Schlüssels, sowie die einmalige Verwendung des gleichen Schlüssels. Es wird daher meist nur bei der Übertragung besonders vertraulicher Informationen und straff organisierter Schlüsselverteilungsmechanismen (z. B. "Heißer Draht") eingesetzt.

## OpenSSL

OpenSSL ist eine Open-Source-Implementierung des *SSL*-Protokolls. Neben dem eigentlichen Protokoll steht unter [www.openssl.org](http://www.openssl.org) auch eine Funktionsbibliothek zur Verfügung, die die für das *SSL*-Protokoll notwendigen Verschlüsselungsalgorithmen (z. B. *DES*, *RC4*) implementiert. OpenSSL steht sowohl als Source-Code als auch als Funktionsbibliothek für unterschiedliche Plattformen (z. B. Linux, Win32 usw.) zur Verfügung. Außerdem enthält OpenSSL auch ein Tool zum Generieren von *Zertifikat*, womit sich auch eine private *Certificate Authority* implementieren lässt.

## P

### PGP

Pretty Good Privacy (PGP) ist ein Programm zum sicheren Versand von eMails. Eine vom Sender gewählte Zufallszahl wird bei diesem Verfahren als Schlüssel für ein *Symmetrisches Verschlüsselungsverfahren*, z. B. *DES* oder *Triple-DES*, verwendet. Zur Übermittlung dieses Schlüssels an den Empfänger der Nachricht kommt dann ein *Asymmetrische Verschlüsselung* wie *Elgamal* oder *RSA* zum Einsatz. Der öffentliche Schlüssel des Empfängers wird verwendet, um den zufällig gewählten Schlüssel der *Symmetrisches Verschlüsselungsverfahren* zu verschlüsseln. Zur Authentisierung des Senders berechnet dieser vor der Verschlüsselung mit Hilfe des *SHA-1*-Algorithmus einen *Hash* über seine Nachricht und signiert diesen Hash mit seinem privaten Schlüssel. Zusätzlich kann auch noch nach der Berechnung des *Hash*-Wertes und vor der Verschlüsselung ein Komprimierungsverfahren angewendet werden.

## Plaintext

Plaintext ist der englische Fachbegriff für den unverschlüsselten Text (deutsch: *Klartext*).

## Q

### Quantenkryptografie

Eine der neuesten Forschungsgebiete der Kryptografie ist die sogenannte Quantenkryptografie, mit der auch sogenannte passive Angriffe erkannt werden können, d. h. also wenn die Nachricht abgehört wird. Sie beruht auf der Heisenbergschen Unschärferelation, die besagt, dass jede Messung eine quantenmechanische Störung des Systems hervorruft. Zur Übertragung der Daten wird hierbei polarisiertes Licht verwendet. Versucht nun jemand, die Nachricht abzuhören, so ist dies eine Messung, die eine Störung des Systems hervorruft, welche erkannt werden kann.

## R

## RC4

Ron's Code oder Rivest Cipher 4 (RC4) ist eine *Stromchiffre*, der im Jahr 1987 von Ronald L. Rivest für RSA Data Security Inc. (heute: [RSA Security](#)) entwickelt wurde. Er hat eine variable Schlüssellänge von bis zu 2048 Bit und wurde für die Implementierung in Software optimiert. Da der Algorithmus sehr schnell und kompakt ist, wird er gerne in zeitkritischen Anwendungen eingesetzt, z. B. für Mobilfunk oder gesicherte Netzwerk- oder Internetverbindungen (z. B. Wireless LAN, Secure Shell oder *SSL*).

## RC5

Ron's Code oder Rivest Cipher 5 (RC5) ist im Gegensatz zum *RC4* Blockchiffre keine *Stromchiffre*, sondern eine *Blockchiffre* mit sowohl variabler Blocklänge von 32, 64 oder 128 Bit, als auch variabler Schlüssellänge von bis zu 2040 Bit. Er wurde ebenfalls von Ronald L. Rivest entwickelt, zum ersten Mal im Dezember 1994 veröffentlicht und war auch als möglicher Nachfolger des *DES* gedacht.

## Rijndael

Der Rijndael-Algorithmus, so benannt nach seinen Erfindern Joan Daemen und Vincent Rijmen, wurde im Oktober 2000 vom National Institute of Standards and Technology zum *AES* erwählt. Es ist somit Nachfolger des *DES*.

## RIPEMD-160

RIPEMD-160 ist ein von Hans Dobbertin, Anton Bosselaers und Bart Preneel in Europa entwickelter und 1996 veröffentlichter *Hash*-Algorithmus. Er erzeugt Hashwerte mit einer Länge von 160 Bits und ist eine verbesserte Version des RIPEMD, der auf den Prinzipien des *MD4* basiert. Die Abkürzung RIPEMD steht für RACE Integrity Primitives Evaluation Message Digest. Es existieren auch 256- und 320 Bit-Versionen dieses Algorithmus (RIPEMD-256 und RIPEMD-320), die aber keine höhere Sicherheit bieten, sondern lediglich die Wahrscheinlichkeit für Kollisionen verringern. RIPEMD-160 unterliegt keinerlei Patentrechte.

## RSA

RSA ist ein nach seinen Erfindern Ronald L. Rivest, Adi Shamir und Leonard Adleman benanntes *Asymmetrische Verschlüsselung*, auf das die Erfinder im Jahr 1977 bei der Suche zur Widerlegung des *Diffie-Hellman-Schlüsseltausch* stießen. Es macht sich die Tatsache zu Nutze, dass die Multiplikation zweier großer Primzahlen zwar relativ einfach, die *Faktorisierungsproblem* des Produktes aber relativ schwierig ist (Einwegfunktion, engl. One-Way-Function). Die Schlüssellänge wird hierbei durch das Produkt der beiden verwendeten Primzahlen bestimmt, typische RSA-Schlüssel haben eine Länge, die ein Vielfaches von 32 oder 64 Bit (für das *CRT*-Verfahren) ist. Inzwischen gelten Schlüssel mit einer Länge von weniger als 1024 Bit als unsicher und werden daher kaum noch verwendet.

## S

### Serpent

Serpent ist ein von Ross Anderson, Eli Biham und Lars Knudsen entwickelter *Symmetrisches Verschlüsselungsverfahren*, der ebenfalls ein Kandidat für den *AES* war und bei dem Auswahlverfahren zusammen mit dem *Rijndael* und dem *Twofish* in der Runde der letzten drei landete. Serpent ist eine *Blockchiffre* mit einer Blockgröße von 128 Bit und Schlüssellängen von bis zu 256 Bit. Da er ähnlich wie der *Twofish* mit 32 Runden operiert, ist er im Vergleich zu anderen Algorithmen etwas langsam.

### SHA

Beim Secure Hash Algorithm (SHA) handelt es sich um einen von der *National Institute of Standards and Technology* zusammen mit der NSA (National Security Agency) entwickelten *Hash-Algorithmus*, der Hashwerte mit einer Länge von 160 Bit erzeugt. Ein nicht weiter beschriebener Design-Fehler im 1993 veröffentlichten SHA-0 wurde im 1995 veröffentlichten SHA-1 korrigiert. Sie unterscheiden sich vorallem in der Anzahl der zu durchlaufenden Runden zur Erzeugung des Hashwertes. Der Secure Hash Algorithm kann Daten mit einer Länge von bis zu  $2^{64}$  Bit verarbeiten. Im August 2002 veröffentlichte die NIST die Algorithmen SHA-256, SHA-384 und SHA-512. Die Zahl gibt jeweils die Länge des erzeugten Hashwertes an. SHA-384 und SHA-512 bieten zusätzlich den Vorteil, dass sie Daten mit einer Länge von bis zu  $2^{128}$  Bit verarbeiten können. Im Februar 2004 wurde mit SHA-224 eine weitere Version veröffentlicht. Im Februar 2005 wurde von chinesischen Kryptologen eine Methode gefunden, um den Aufwand zur Kollisionsberechnung bei den Algorithmen SHA-0 und SHA-1 von  $2^{80}$  auf  $2^{69}$  zu reduzieren. Es bleibt allerdings abzuwarten, ob man damit den heute sehr verbreiteten SHA-1 als gebrochen ansehen kann.

### Skytale

Die Skytale ist ein schon seit der Antike bekanntes Verschlüsselungsverfahren, bei dem ein Pergament- oder Lederstreifen um einen Holzstab mit einem bestimmten Durchmesser (Skytale) gewickelt wird. Anschließend wird die zu verschlüsselnde Nachricht längs auf den Stab geschrieben und das Pergament bzw. Leder wieder abgewickelt. Nun kann niemand mehr die Nachricht lesen, da die Buchstaben nun in einer scheinbar zufälligen Anordnung darauf stehen. Die Skytale gehört damit zu den so genannten *Transpositionschiffre*. Der Empfänger benötigt ebenfalls einen Holzstab mit exakt dem gleichen Durchmesser, um die Nachricht wieder lesbar zu machen, indem er das empfangene Band darum wickelt.

### Smartcard

Eine Smartcard ist ein Mikrocontroller, der neben einer CPU, RAM, persistentem Speicher (EEPROM, Flash o. Ä) und IO-Bausteinen meistens auch kryptografische Coprozessoren enthält, die zur schnellen Berechnung kryptografischer Algorithmen (*DES*, *ECC*, *RSA*) dienen. Diese Mikrocontroller werden z.B. in Kreditkarten eingebaut, um damit elektronische Bezahlvorgänge sicher zu implementieren. Auch eine elektronische Geldbörse kann mit Hilfe eines solches Mikrocontrollers realisiert werden (z. B. EC-Karte). Für Transportsysteme oder zum Sammeln von Treuepunkte (Loyalty-Points) können Smartcards ebenfalls eingesetzt werden. In Zukunft werden wahrscheinlich auch elektronische Ausweise mit Hilfe von Smartcards realisiert werden. Moderne Smartcards setzen daher meist Betriebssysteme ein, die es ermöglichen, mehrere verschiedene An-

wendungen auf der gleichen Karte ablaufen zu lassen (z. B. Multi-Function-Cards (MFC) oder Javacards).

## SSL

Das Secure Socket Layer Protokoll ist ein Protokoll zur sicheren Datenübertragung, bei welcher die Daten verschlüsselt übertragen werden. Es wurde in der ersten Version im Jahr 1994 von Netscape Communications veröffentlicht. Mit der nächsten Version des Netscape Navigators wurde die Version SSL 2.0 eingeführt, die auch heute noch von vielen Browsern unterstützt wird. Als Microsoft mit ihrem Internet Explorer das Private Communication Technology (PCT) Protokoll vorstellte, welches einige Vorteile gegenüber SSL V2 hatte, wurde bald darauf SSL V3 vorgestellt, welches viele der Vorteile von PCT enthielt. Im Januar 1999 wurde das SSL Protokoll von der Internet Engineering Task Force (IETF) zum Standard für gesicherte Übertragungen ernannt und in *TLS* Protokoll umbenannt. Die Unterschiede von *TLS* V1.0 zu SSL V3.0 sind jedoch minimal, *TLS* meldet sich beim so genannten Handshake zwischen Server und Client, der jeder Datenübertragung vorangeht und bei welchem auch *Zertifikat* zur Authentisierung ausgetauscht werden, als SSL V3.1. Dieser Handshake ist notwendig, damit der Client weiß, ob er dem Server vertrauen kann, und ggf. auch, ob der Server dem Client den Zugriff erlauben darf oder nicht, wenn auch der Client durch ein *Zertifikat* seine Identität nachweisen muss (Client Authentication). Außerdem wird während dieses Handshakes mit Hilfe eines *Asymmetrische Verschlüsselung* der Schlüssel für die anschließende *Symmetrisches Verschlüsselungsverfahren* der Daten ausgehandelt.

## Stromchiffre

Eine Stromchiffre ist ein *Symmetrisches Verschlüsselungsverfahren*, bei dem die Daten Bit für Bit bzw. Zeichen für Zeichen verarbeitet werden, im Gegensatz zu den sogenannten *Blockchiffre*, bei welchem immer gleich ganze Datenblöcke verarbeitet werden müssen. Zum Ver- bzw. Entschlüsseln muss hierzu zunächst aus dem geheimen Schlüssel ein so genannter Schlüsselstrom erzeugt werden, der in der Regel eine Folge von Pseudozufallszahlen ist. Dieser Schlüsselstrom wird dann mit dem zu ver- oder entschlüsselnden Text durch eine einfache Operation verknüpft, in der Regel eine einfache XOR-Funktion. Stromchiffren arbeiten daher sehr schnell. Bekannte Beispiele für Stromchiffren sind der *RC4* oder das *One-Time-Pad*.

## Substitutionschiffre

Bei Substitutions- oder Ersetzungschiffren wird zur Verschlüsselung jedes Zeichen durch ein anderes Zeichen ersetzt. Hierbei werden monoalphabetische Substitutionschiffren, bei welchen ein bestimmtes Zeichen im Klartext immer durch das gleiche Zeichen im Geheimtext ersetzt wird, und polyalphabetischen Substitutionschiffren, bei denen das gleiche Zeichen im Klartext durch verschiedene Zeichen im Geheimtext ersetzt werden kann. Ein Beispiel für eine monoalphabetische Substitutionschiffre ist der *Caesar-Chiffre*, ein Beispiel für eine polyalphabetische Substitutionschiffre ist der *Vigenère-Chiffre*.

## Symmetrisches Verschlüsselungsverfahren

Bei symmetrischen Verschlüsselungsverfahren wird ein und derselbe Schlüssel sowohl zum Verschlüsseln des Klartext, als auch zum Entschlüsseln des Geheimtext verwendet. Zum Entschlüsseln muss daher meist die sogenannte Umkehrfunktion zur Verschlüsselungsfunktion verwendet werden. Die bekanntesten Beispiele für symmetrische Verschlüsselungsverfahren sind *DES* und *AES*.

## T

## TLS

Die vom IETF zum Standard ernannte Version 3.1 des *SSL* wird als Transport Layer Security (TLS) Protokoll bezeichnet. Es enthält nur sehr geringe Änderungen gegenüber der Vorgängerversion 3.0, unter anderem werden von TLS neue Crypto-Algorithmen (z. B. *AES*) unterstützt. Beim Handshake wird TLS V1.0 als *SSL V3.1* gemeldet.

## Transpositionschiffre

Bei einer Transpositionschiffre behalten im Gegensatz zu den *Substitutionschiffren* alle Buchstaben und Zeichen ihre ursprüngliche Bedeutung, allerdings wird ihre Reihenfolge innerhalb der Nachricht so verändert, dass sie nicht mehr lesbar ist. Eine schon seit der Antike bekannte Transpositionschiffre ist die *Skytale*.

## Twofish

Twofish wurde als Nachfolger des *Blowfish*-Algorithmus vorgestellt und ebenfalls von Bruce Schneier mitentwickelt. Es handelt sich hierbei um einen *Symmetrisches Verschlüsselungsverfahren* mit Schlüssellängen von 128, 192 und 256 Bit. Als *Blockchiffre* hat er eine Blockgröße von 128 Bit und arbeitet mit 32 Runden. Twofish nahm auch an der Bewerbung zum *AES* teil und erreichte zusammen mit *Serpent* und *Rijndael* die Runde der letzten drei.

## U

## V

## Vernam-Verschlüsselung

Vernam-Verschlüsselung oder Vernam-Code ist eine andere Bezeichnung für das *One-Time-Pad*, bei welchem der Schlüssel genauso lang ist wie der zu verschlüsselnde Klartext.

## Vigenère-Chiffre

Die Vigenère-Chiffre ist eine sogenannte polyalphabetische *Substitutionschiffre*, bei dem der gleiche Buchstabe im Klartext immer wieder durch einen anderen Buchstaben im Geheimtext ersetzt werden kann. Mit welchem Buchstabe ein bestimmter Buchstabe ersetzt wird, wird durch den Schlüssel festgelegt. Der Schlüssel bei der Vigenère-Chiffre ist ein Schlüsselwort, das solange wiederholt über Klartext geschrieben wird, bis dessen Ende erreicht ist. Derjenige Buchstabe, der nun über einem bestimmten Klartextbuchstaben steht, bestimmt durch seine Position im Alphabet, um wie viele Stellen dieser Buchstabe im Alphabet verschoben werden muss, um zum Geheimtextbuchstaben zu kommen. Hierzu kann auch das sogenannte Vigenère-Quadrat verwendet werden, in dem der gesuchte Geheimtextbuchstabe in der Zeile unter dem Klartextbuchstaben steht, die mit dem Schlüsselbuchstaben beginnt.

## W

## X

**Y****Z****Zertifikat**

Ein Zertifikat ist eine Art elektronischer Ausweis, mit der der Inhaber des Zertifikates seine Identität nachweist. Solche Zertifikate können bei so genannten Zertifizierungsstellen (*Certificate Authority*) beantragt werden. Die Zertifizierungsstelle überprüft zunächst die Identität des Antragsstellers, bevor sie das Zertifikat ausstellt und mit ihrer eigenen *Digitale Signatur* unterschreibt. Wenn ein Zertifikatsinhaber ein Zertifikat mit der Unterschrift einer Zertifizierungsstelle vorlegen kann, die als vertrauenswürdig eingestuft wurde, so kann auch dem Zertifikatsinhaber vertraut werden. Zertifikate werden beispielsweise beim *SSL*-Protokoll eingesetzt, um die Identität des Servers, mit dem der Benutzer sich verbindet, nachzuweisen. Außerdem enthält ein Zertifikat auch den öffentlichen Schlüssel des Zertifikatinhabers, der dann genutzt werden kann, um sowohl die *Digitale Signatur* des Zertifikatinhabers zu verifizieren, als auch um einen symmetrischen Schlüssel für die *SSL*-Verbindung auszuhandeln. Elektronische Zertifikate werden meistens nur für einen bestimmten Zeitraum ausgestellt, d. h. sie sind nur in einem bestimmten Zeitraum gültig. Liegt das aktuelle Datum des Rechners, mit dem ein Zertifikat empfangen wird, nicht in diesem Gültigkeitszeitraum, so erhält der Benutzer eine Warnmeldung.

## Quellen

### Wikipedia

Meinen besonderen Dank möchte ich hier den Autoren des [Wikipedia](#)-Lexikons und den Verantwortlichen für das DVD-Image aussprechen, da dieses Glossar mit Hilfe der Wikipedia-DVD (Download-Version 1/2005) erstellt wurde.

### Kryptografie in Theorie und Praxis

Für die Erklärung einiger Begriffe wurde auch das Buch "Kryptologie in Theorie und Praxis" von Albrecht Beutelspacher, Heike B. Neumann und Thomas Schwarzpaul (1. Auflage Januar 2005, Vieweg Verlag, Wiesbaden) zu Rate gezogen.

### Handbook of Applied Cryptography

In manchen Fällen wurde ebenfalls das "Handbook of Applied Cryptography" von Alfred J. Menezes, Paul C. von Oorschot und Scott A. Vanstone (frei downloadable Version unter <http://www.cacr.math.uwaterloo.ca/hac/>) verwendet.