Symmetrische und Asymmetrische Kryptographie

Maurice

21.05.2012

Dozent:
Prof. Dr. Michael Anders

Inhalt

1. Einleitung

Die Kryptographie gilt als die Wissenschaft der Verschlüsselung. Sie befasst sich vor allem mit dem Thema der Informationssicherheit, was die Konzeption, Definition und Konstruktion von Informationssystemen beinhaltet.

Das Thema meiner Seminararbeit lautet „Symmetrische und Asymmetrische Kryptographie“, womit die 2 grundlegenden Methoden der Kryptographie gemeint sind.

Symmetrische Verfahren wurden bereits von den alten Ägyptern benutzt und seitdem fortlaufend weiterentwickelt, wohingegen die erste Idee zu asymmetrischen Verfahren im Jahr 1974 von Ralph Merkle mit seinem Merkles Puzzle gemacht wurde. Dieses lieferte den Grundsatz der asymmetrischen Kryptographie und führte z.B. zum Diffie-Hellman-Schlüsselaustausch der 1976 entwickelt wurde.

Im folgenden Text werde ich auf die Grundzüge der beiden Verschlüsselungsverfahren eingehen, Beispiele zur Anwendung erläutern und die Möglichkeiten zeigen, die sich aus ihnen ergeben.

2. Symmetrische Kryptografie:

Bei der symmetrischen Kryptografie handelt es sich um die klassische, schon lang verwendete Art von Kryptografie. So wurde das sogenannte Caesar-Chiffre, erstmals von Julius Caesar entwickelt, schon von dem alten Römern verwendet, um geheime meist militärische Nachrichten zu verschicken. Heutzutage findet dies allerdings keine Verwendung mehr, da es bereits mit geringem Rechenaufwand zu entschlüsseln ist.

Das Hauptmerkmal der symmetrischen Verschlüsselung ist es, dass Chiffrier- und Dechiffrierschlüssel meist identisch sind, und falls nicht, auf mathematischem Wege leicht aus dem jeweils anderen berechnet werden können. Es müssen also beide Seiten, Sender und Empfänger, über den Schlüssel verfügen. Daraus resultiert der wohl größte Nachteil der symmetrischen Kryptografie, da der Schlüssel über einen sicheren Kanal übertragen werden muss, um Sicherheit der Verschlüsselung zu gewähren.

Es ist zu sagen, dass es in der symmetrischen Kryptographie grundsätzlich 2 unterschiedliche Arten der Verschlüsselung gibt. Die Stromchiffrierung und die Blockchiffrierung. Bei einem Stromchiffre wird jedes Zeichen bzw. jeder Bit einzeln und nacheinander mit dem eines Schlüsselstroms verbunden (z.B. über XOR), wohingegen beim Blockchiffre der Klartext in eine Folge von gleichlangen Blöcken zerlegt wird, um dann Blockweise anhand des Schlüssels chiffriert zu werden. Sollte der Klartext nicht ganzzahlig durch die Blocklänge teilbar sein, muss dieser mittels Füll-Bits (Padding) aufgefüllt werden.

Außerdem werden die Verfahren der symmetrischen Kryptographie in Transpositions- und Substitutionschiffren unterteilt, auf die ich im Folgenden eingehen werde.

2.1 Transpositionschiffren:

Transpositionschiffren verschlüsseln den Klartext durch Veränderung der Buchstaben- bzw. Bitfolge. Dies geschieht nach einem frei wählbaren Schema, wie z.B. durch das Verschieben jedes zweiten Buchstabens an das Ende des Textes oder über geometrische Formen.

Um die Funktionsweise zu verdeutlichen bringe ich hier ein kleines Beispiel:

Das Wort „Kryptografie“ soll mittels eines Transpositionschiffre verschlüsselt werden. Hierzu tragen wir den Klartext in eine 3 x 4 Matrix ein.

$$\begin{pmatrix} K & R & Y & P \\ T & O & G & R \\ A & F & I & E \end{pmatrix}$$

Nun könnte man entweder die Spalten oder die Zeilen neu ordnen, wobei die Neuordnung der Spalten durchaus sinnvoller ist, da so mit Sicherheit die einzelnen Silben des Wortes getrennt werden. Ich ordne die Spalten neu in der Reihenfolge 4,1,2,3, woraus sich der Chiffretext: „PREKTAROFYGI“ ergibt.

Um einen solchen Transpositionschiffre zu entschlüsseln, wird als erstes Gewissheit benötigt, dass es sich auch wirklich um einen solchen Chiffre handelt. Dies kann mittels der Häufigkeitsanalyse der Buchstaben bestätigt werden. Ist man sich sicher einen Transpositionschiffre vor sich zu haben, kann dieser mittels Anagramming entschlüsselt werden.

2.2 Substitutionschiffren:

Es gibt verschiedene Typen von einfachen Substitutionschiffren, die sich in ihrer Komplexität und Sicherheit unterscheiden. Die monoalphabetische Substitution, bei der nur ein einziges Geheimalphabet zur Verschlüsselung genutzt wird. Bei der homophonen Substitution hingegen können einzelne Klartextzeichen auch durch mehrere Zeichen im Chiffretext dargestellt werden, wohingegen bei der polyalphabetischen Substitution direkt mehrere Alphabete zum Verschlüsseln genutzt werden.

2.2.1 Monoalphabetische Substitution:

Wie bereits oben beschrieben, wird hier genau ein Geheimalphabet für die Verschlüsselung benutzt. Das führt dazu, dass jeder Buchstabe durch einen anderen ersetzt wird. Es gibt einmal die Möglichkeit das normale Alphabet, wie bei der Caesar-Verschlüsselung, um eine gewisse Anzahl von Buchstaben zu verschieben oder ein komplett neu geordnetes Geheimalphabet zu entwerfen, wie ich es in folgendem Beispiel getan habe.

Der Klartext: „SUBSTITUTION“ soll mit dem Geheimalphabet „QWERTZUIOPASDFGHJKLYXCVBNM“ verschlüsselt werden.

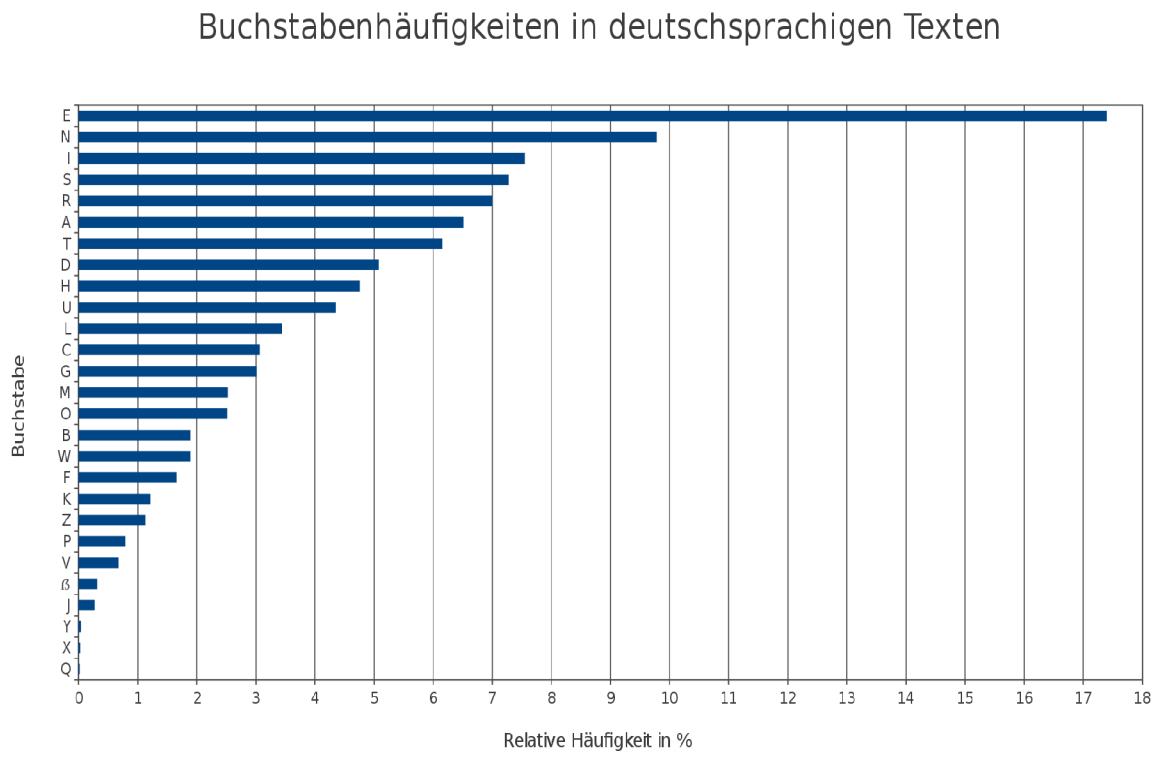
Normales Alphabet :	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Geheim-alphabet :	Q W E R T Z U I O P A S D F G H J K L Y X C V B N M

Klartext :	S U B S T I T U T I O N
Chiffretext :	L X W L Y O Y X Y O G F

Der entscheidende Nachteil der monoalphabetischen Substitution ist die geringe Sicherheit des Verfahrens. Zwar gibt es 26! ≈ $4*10^{26}$ Möglichkeiten zur Anordnung des Alphabets, jedoch können monoalphabetisch verschlüsselte Texte leicht durch statistische Untersuchung (Häufigkeitsanalyse der einzelnen Buchstaben) entschlüsselt werden.

2.2.2 Homophone Substitution:

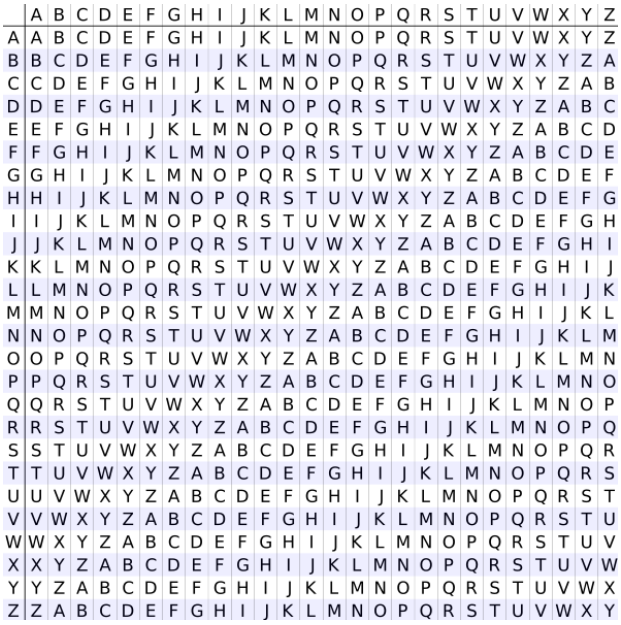
Ziel der homophonen Substitution ist, gegenüber der normalen monoalphabetischen Substitution, die Sicherheit bei einer Häufigkeitsanalyse zu verbessern. Hierzu werden den einzelnen Buchstaben des Alphabets die zahlen 0 bis 99, entsprechend ihrer Häufigkeit, zugeordnet. Dementsprechend werden im deutschen dem „E“ 17 und somit die meisten Zahlen zugordnet. Eine Häufigkeitsanalyse der einzelnen Buchstaben führt nun zu keinem statistisch brauchbaren Ergebnis. Anstatt dessen können allerdings Bigramme, Trigramme und Tetragramme analysiert werden, was bei längeren Texten zur Entschlüsselung der Nachricht führen würde.



2.2.3 Polyalphabetische Substitution:

Im Gegensatz zur monoalphabetischen Substitution werden bei der polyalphabetischen Substitution mehrere Geheimalphabete verwendet. Ein Verfahren dieser Technik ist die Vigenère-Verschlüsselung, bei der mittels des Vigenère-Quadrats und einem sich meist periodisch wiederholenden Schlüsselwort, ein Klartext in einen Chiffretext umgewandelt wird.

Das Vigenère-Quadrat:



	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Möchte man nun mittels der Vigenère-Verschlüsselung den Klartext „KRYPTOGRAPHIE“ mit dem Schlüsselwort „HEUTE“ verschlüsseln bildet man einen Schlüsselstring mit gleicher Länge des Klartextes. In meinem Beispiel wäre das „HEUTEHEUTEHEU“. Nun liest man im Vigenère-Quadrat den Chiffretext-buchstaben ab, indem man die Spalte über den Klartextbuchstaben und die Zeile über den Schlüsselbuchstaben bestimmt.

Entschlüsselt werden kann dieses Verfahren mit dem Kasiski-Test, der es erlaubt, die Länge des Schlüsselwortes zu bestimmen.

2.2.4 Vernam-Verschlüsselung/One-Time Pad:

Ist der Schlüssel einer Vigenère-Verschlüsselung genauso lang wie der Klartext und durch einen wahren Zufallsgenerator erzeugt, handelt es sich um einen Vernam-Chiffre. Dieser bietet eine noch deutlich höhere Sicherheit als die normale Vigenère-Verschlüsselung. Sollte der Vernam-Chiffre nur einmal verwendet werden handelt es sich um ein One-Time Pad, welches auch mit unbegrenzten Rechenressourcen nicht zu brechen ist. Der große Nachteil des One-Time Pad ist die komplizierte Schlüsselübertragung. Um sicher zu gehen, dass der Schlüssel nicht abgehört wird, muss dieser von einem Boten z.B. per CD übermittelt werden, woraufhin die eigentlichen Daten an einem beliebigen Zeitpunkt über das Internet verschickt werden können. Dieser hohe Aufwand macht das One-Time Pad ineffektiv für große Netzwerke, aber ist z.B. bei Geheimagenten eine gute Methode zur Datenübermittlung.

2.3 Aktuelle symmetrische Verfahren

2.3.1 DES und 3DES WIKI

Der Data Encryption Standard (DES) wurde ab 1976 als offizieller Standard für die US-Regierung eingesetzt. Er wurde unter anderem von der National Security Agency (NSA) entwickelt und war dadurch immer wieder Spekulationen über seine Sicherheit ausgesetzt. Aktuell wird DES für viele Anwendungen nicht als ausreichend sicher betrachtet, da seine Schlüssellänge auf 56 Bits begrenzt ist.

Aufgrund dessen wurde der Algorithmus zum 3DES weiterentwickelt. Da der Algorithmus allerdings einfach 3 mal ausgeführt wird, kommt es zu hohem Rechenaufwand, der das gesamte Verschlüsseln verlangsamt. Dem Gegenüber ist allerdings zu sagen, dass der 3DES als relativ sicher, mit dem Security Level 6, gilt. (Im Kapitel 3.5 ist eine Übersicht über die einzelnen Security Level zu sehen)

3DES zeichnet sich dadurch aus, dass der Klartext erst mit dem ersten Schlüssel K1 verschlüsselt wird, dann mit dem zweiten Schlüssel K2 entschlüsselt und daraufhin wieder mit dem dritten Schlüssel K3 verschlüsselt wird.

2.3.2 AES

Der Advanced Encryption Standard (AES) wurde im Jahr 2000 vom National Institute of Standards and Technology (NIST) als Standard für symmetrische Verschlüsselung bekanntgegeben. Er besitzt eine variable Schlüssellänge von wahlweise 128-, 196- oder 256-bit und gilt mit dem Security Level 8 als in absehbarer Zukunft nicht brechbar. Anwendung findet der Advanced Encryption Standard zum Beispiel bei der Sicherung von Wireless LAN mittels WPA2 oder von RAR-Archiven.

2.3.3 Hash-Funktionen:

Eine Hash-Funktion liefert einen „Fingerabdruck“ einer Datei, welcher aus dessen Inhalt mittels eines Algorithmus berechnet wird. Wichtig ist, dass eine beliebig lange Zeichenfolge auf eine Zeichenfolge fester Länge abgebildet wird (Kompressionseigenschaft). Kryptografische Hash-Funktionen müssen bestimmte Bedingungen erfüllen. So müssen sie Einwegfunktionen sein, was bedeutet, dass man von dem Hash-Wert eines Dokuments auf keinen Fall auf den Inhalt desgleichen schließen kann. Außerdem dürfen 2 verschiedene Dokumente nicht zum selben Hash-Wert führen (Kollisionsresistenz). Es gibt einige bekannte Hash-Funktionen, die in der Kryptographie eingesetzt werden. Die bekanntesten davon sind der MD5-Algorithmus, sowie der Secure Hash Algorithm (SHA).

2.3.4 Message Authentication Code

Um die Authentizität einer Nachricht zu überprüfen, kann man statt mit digitalen Signaturen auch mit speziellen Hash-Funktionen arbeiten, die durch Schlüssel parametrisiert sind. Hierbei wird allerdings von beiden Parteien der gleiche Schlüssel verwendet. Es handelt sich also um ein symmetrisches Verfahren.

Eine solche Hash-Funktion muss folgende Eigenschaften erfüllen:

1. Aus einem beliebigen Schlüssel und einer beliebigen Eingabe lässt sich der MAC-Wert leicht berechnen
2. Eine Eingabe beliebiger Bitlänge führt zu einem MAC einer festen Bitlänge (Kompressionseigenschaft)
3. Für den Angreifer ist es praktisch unmöglich, ohne Kenntnis über den geheimen Schlüssel einen neuen MAC zu dem veränderten Text zu berechnen. (Fälschungsresistenz)

Um später die Authentizität einer Nachricht prüfen zu können, muss der Sender der Nachricht den berechneten MAC-Wert an diese Nachricht anheften. Der Empfänger kann nun mittels des gemeinsamen Schlüssels einen neuen MAC-Wert berechnen und ihn mit dem angehängten vergleichen. Sollte es sich um den gleichen Wert handeln, ist die Nachricht im Original.

3. Asymmetrische Kryptografie:

Im Jahr 1975 wurde von Whitfield Diffie und Martin Hellman die Idee zur asymmetrischen Verschlüsselung ohne Kenntnis eines genauen Verfahrens veröffentlicht. Woraufhin 1977 von Ronald L. Rivest, Adi Shamir und Leonard M. Adleman das weit verbreitete RSA-Verfahren entwickelt wurde.

Der große Unterschied zur symmetrischen Kryptografie ist, dass es keinen geheimen Schlüssel gibt, über den beide Kommunikationspartner verfügen müssen, sondern dass ein öffentlicher und ein privater Schlüssel verwendet werden. Welcher der beiden Schlüssel zum Verschlüsseln und welcher zum Entschlüsseln benutzt wird, kommt darauf an, ob man Daten sicher versenden oder Daten mittels einer digitalen Signatur verifizieren will.

3.1 Schlüsselgenerierung:

Der erste Schritt der asymmetrischen Verschlüsselung ist das Generieren eines Schlüsselpaares bestehend aus öffentlichem und privatem Schlüssel. Dieses muss entweder vom Empfänger der Daten (Bob) bei normaler Datenübertragung oder bei Signaturverfahren vom Urheber der Daten oder von einer glaubwürdigen Instanz (Hochschule, Notar, …) generiert werden. Das Schlüsselpaar wird mittels einer langen Zufallszahl ermittelt, wobei eine Einwegfunktion (engl. One-way-function z.B. Multiplikation zweier großer Primzahlen bei RSA) benutzt wird, was dazu führt, dass das Verschlüsseln mit dem öffentlichen Schlüssel schnell und das Entschlüsseln mit dem gleichen Schlüssel unverhältnismäßig lange dauert.

3.2 Datenübertragung mittels asymmetrischer Kryptographie:

Bei der verschlüsselten Übertragung von Daten mittels asymmetrischer Kryptografie wird als erstes vom Empfänger der Daten (Bob) ein Schlüsselpaar aus einer großen Zufallszahl generiert. Der öffentliche Schlüssel kann nun über einen unsicheren Kanal zum Sender der Daten (Alice) geschickt oder für alle zugänglich, im Internet veröffentlicht werden. Nun kann der Sender der Daten (Alice) mittels des öffentlichen Schlüssels die Daten verschlüsseln und diese wiederum über einen unsicheren Kanal an Bob schicken, welcher dann mit dem passenden privaten Schlüssel die Nachricht entschlüsseln kann.

3.3 Digitale Signatur:

Eine digitale Signatur dient zur Bestimmung/Bestätigung des Urhebers eines Dokuments, sowie zur Bestätigung, dass eine Nachricht nicht verändert wurde. Dies wird mit der zunehmenden Vernetzung der Welt immer wichtiger, da z.B. mehr und mehr Verträge über das Internet und nicht mehr per Hand mit Unterschrift abgeschlossen werden. Ein weiterer wichtiger Aspekt der digitalen Signatur sind Zeitstempel, auf die ich später noch eingehen werde.

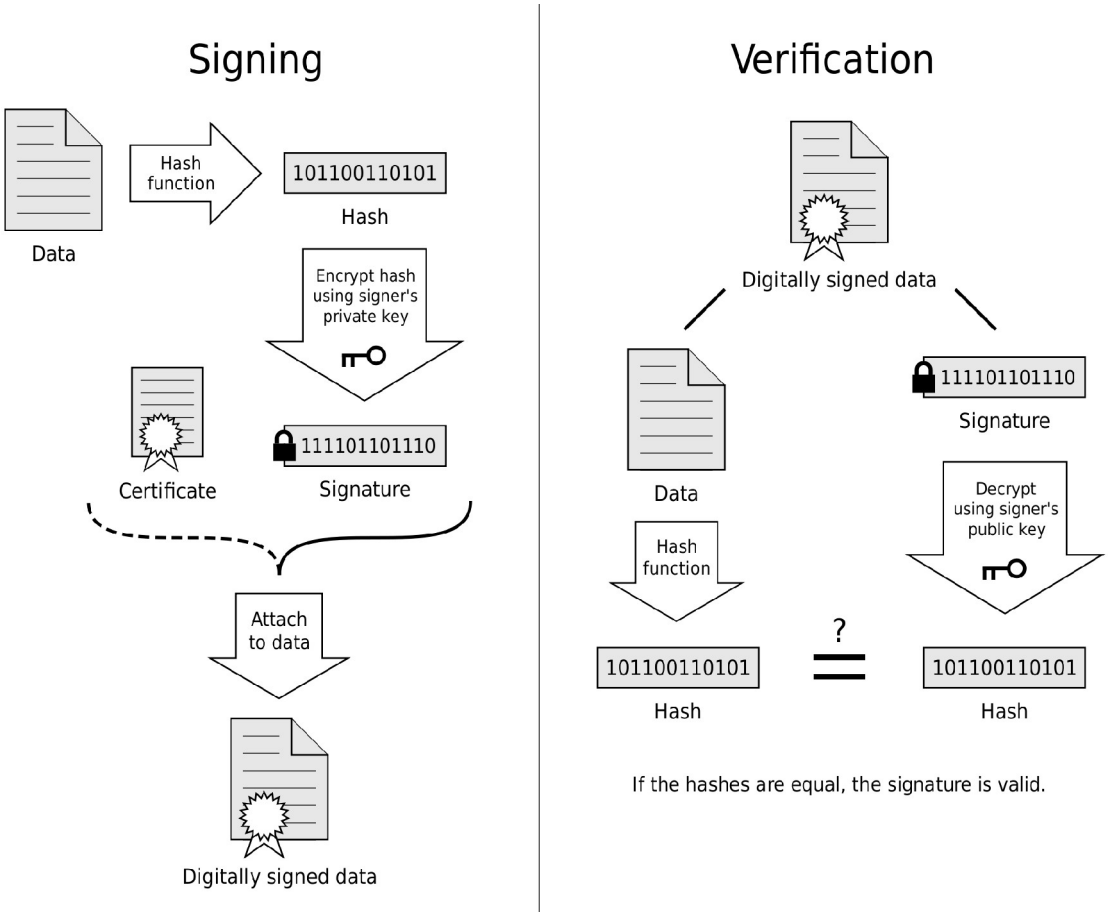
Digitale Signaturen basieren auf asymmetrischer Kryptographie und werden in weitreichenden Anwendungsbereichen (Geschäftsbereich, staatlicher Bereich und privater Bereich) eingesetzt. Sie erfüllen 5 Funktionen, die ich im folgendem aufgelistet habe:

- Identitätsfunktion:
    - Eine Person oder Instanz kann der Signatur eindeutig zugeordnet werden
- Echtheitsfunktion:
    - Durch Vergleich der Hash-Werte wird garantiert, dass das signierte Dokument nicht verändert wurde
- Abschlussfunktion
    - Hohe Verbindlichkeit, da wenn das Dokument geändert wird, eine neue Signatur erzeugt werden muss
- Warnfunktion
    - Eine Signatur ist mit einer Unterschrift gleichzusetzen und sofern nicht leichtfertig zu behandeln, was allerdings heutzutage häufig noch unterschätzt wird
- Rechtsverbindlichkeit
    - Die digitale Signatur ist der gesetzlich geforderten Schriftform in vielen Fällen gleichzusetzen

3.3.1 Ablauf des Signierens

Um ein Dokument digital zu signieren, muss als erstes der Hash-Wert dieses Dokuments berechnet werden, damit der spätere Verschlüsselungsaufwand, sowie die Größe der Signatur, nicht zu groß werden. Dies geschieht üblicherweise mit dem SHA-1 Algorithmus, welcher jedoch Schwachstellen aufzeigt und nach und nach von Hash-Algorithmen neuerer Generation, wie z.B. dem SHA-2 und SHA-3 abgelöst wird. Dieser berechnete Hash-Wert stellt einen Fingerabdruck des Dokuments dar, der sich bei der kleinsten Veränderung, wie z.B. dem Hinzufügen eines Leerzeichens, verändern würde. Um nun das Dokument digital zu signieren, wird der Hash-Wert mittels des privaten Schlüssels des Signierers verschlüsselt und die sich ergebene Signatur, dann an das Dokument angeheftet.

Hier der schematische Ablauf vom Signieren bzw. Verifizieren:



Quelle: Wikipedia

3.3.2 Zeitstempel:

Zeitstempel sollen ein mögliches Umdatieren von Dokumenten verhindern, um Betrug zu verhindern. Ein Beispiel hierfür wäre ein selbst komponiertes Musikstück, was man gerne ins Internet stellen möchte. Allerdings möchte man verhindern, dass jemand dieses Stück einfach klaut und behauptet, er hätte es vor dem eigentlichen Besitzer gehabt. Dies kann man nun mittels eines Zeitstempels machen. Man

generiert den Hash-Wert des Musikstücks, welcher dann an eine vertrauenswürdige Instanz, wie ein Trust-Center (wie Notar) geschickt wird. Dieses hängt an den Hash-Wert eine amtliche Zeitangabe an und signiert diesen nun mit ihrem eigenen Zertifikat. Dieser signierte Hash-Wert wird nun zurück zum Urheber geschickt und von diesem mit seinem privaten Schlüssel signiert.

3.4 Zertifikate:

Eine mögliche Schwachstelle bei asymmetrischer Kryptographie liegt beim Schlüsselaustausch vor. So muss der Empfänger einer asymmetrisch verschlüsselten Nachricht seinen öffentlichen Schlüssel an den Sender schicken. Hier kann sich nun aber ein Angreifer einbringen und dem Sender der Daten einen falschen öffentlichen Schlüssel zukommen lassen. Nun könnte der Angreifer die Nachricht mittels seines passenden privaten Schlüssels lesen, jedoch nicht der ursprüngliche Empfänger.

Um diese Schwachstelle zu umgehen gibt es digitale Zertifikate. Ein solches Zertifikat kann man sich als Personalausweis in digitaler Form vorstellen. Es wird durch eine vertrauenswürdige Instanz (Trust-Center) ausgegeben. Ob man nun dem Trust-Center vertraut ist Sache des Benutzers. Wobei es hier unterschiedliche „Qualitätsstufen“ was die Vertrauenswürdigkeit angeht.

Ein solches Zertifikat enthält den Namen des Inhabers, seinen öffentlichen Schlüssel, eine Seriennummer, sowie Gültigkeitsdauer und den Namen der Zertifizierungsstelle und wird mit dem privaten Schlüssel der Zertifizierungsstelle signiert. Da nun auch der öffentliche Schlüssel einer Zertifizierungsstelle überprüfbar sein muss, gibt es eine oberste Zertifizierungsinstanz, welche in Deutschland die Bundesnetzagentur ist.

3.5 Sicherheit:

Die theoretische Sicherheit von asymmetrischen Verschlüsselungsverfahren ist bestimmt durch die Länge der Operanden bzw. Schlüssel. Es werden, zum Bewerten der verschiedenen Verfahren asymmetrischer Verschlüsselung, Security Levels benutzt. Ein Algorithmus hat ein Security Level von n-Bits wenn die beste bekannte Attacke 2^n Schritte benötigt um ihn zu brechen.

Hier eine Tabelle aus dem „ECRYPT II Yearly Report on Algorithms and Keysizes“ vom Jahr 2010 über die jeweiligen Security Levels und ihre Sicherheit:

Table 7.4: Security levels (symmetric equivalent).

Security Level	Security (bits)	Protection	Comment
1.	32	Attacks in "real-time" by individuals	Only acceptable for auth. tag size
2.	64	Very short-term protection against small organizations	Should not be used for confidentiality in new systems
3.	72	Short-term protection against medium organizations, medium-term protection against small organizations	
4.	80	Very short-term protection against agencies, long-term prot. against small organizations	Smallest general-purpose level, ≤ 4 years protection (E.g. use of 2-key 3DES, $< 2^{40}$ plaintext/ciphertexts)
5.	96	Legacy standard level	2-key 3DES restricted to $\sim 10^6$ plaintext/ciphertexts, $\approx$ 10 years protection
6.	112	Medium-term protection	$\approx$ 20 years protection (E.g. 3-key 3DES)
7.	128	Long-term protection	Good, generic application-indep. recommendation, $\approx$ 30 years
8.	256	"Foreseeable future"	Good protection against quantum computers unless Shor's algorithm applies.

Passend zur oberen Grafik hier eine Tabelle die zu den Security Levels (80-, 128-, 192- und 256bit) die jeweiligen Schlüssellängen der verschiedenen Verfahren aufzeigt:

Algorithm Family	Cryptosystems	Security Level (bit)			
		80	128	192	256
Integer factorization	RSA	1024 bit	3072 bit	7680 bit	15360 bit
Discrete logarithm	DH, DSA, Elgamal	1024 bit	3072 bit	7680 bit	15360 bit
Elliptic curves	ECDH, ECDSA	160 bit	256 bit	384 bit	512 bit
Symmetric-key	AES, 3DES	80 bit	128 bit	192 bit	256 bit

Quelle: Understanding Cryptography (Christof Paar/Jan Pelzl)

Aus der Tabelle ist deutlich erkennbar, dass sich der Algorithmus mit elliptischen Kurven für hohe Security Level anbietet.

Die große Länge von Operanden und Schlüsseln führt zu einem sehr hohen Rechenaufwand, was das Verschlüsseln bzw. Entschlüssen betrifft. Je höher dabei die Bitlänge des Schlüssels ist, desto länger dauert das Ver- und Entschlüsseln. So erhöht sich die benötigte Zeit um den Faktor 27 bei einer Änderung der Bitlänge von 1024 auf 3076 Bit. Üblich ist, dass solche Operationen bei handelsüblichen PCs zwischen 10 und mehreren 100 ms dauern.

4. Hybride Verschlüsselung

Die hybride Verschlüsselung bezeichnet eine Kombination aus symmetrischer und asymmetrischer Verschlüsselung. Dabei werden die Vorteile beider Verfahren genutzt, um den jeweiligen Nachteilen entgegenzuwirken.

Die symmetrische Kryptographie ist allgemein als ein Verfahren mit sehr hoher Geschwindigkeit anzusehen, wohingegen die asymmetrische Kryptographie eher ineffizient arbeitet. Dem ist entgegenzusetzen, dass asymmetrische Kryptographie, dank des sicheren Schlüsselaustausches, um einiges sicherer ist, als symmetrische Kryptographie.

Um nun die beiden Verfahren zu kombinieren, wählt man für die eigentliche Verschlüsselung des Dokuments symmetrische Kryptographie und überträgt den gemeinsamen Schlüssel mittels asymmetrischer Kryptographie. Daraus folgt eine hohe Effizienz, sowie Sicherheit bei der Übertragung von Daten.

Abschließend ist zu sagen, dass die Kombination von symmetrischer und asymmetrischer Kryptographie der wohl effizienteste und sicherste Weg zur Datenübertragung ist. So kann zum Beispiel ein Text mittels AES sicher verschlüsselt werden, um dann deren Schlüssel mittels Elliptic Curve Cryptography (ECC) sicher zu übertragen.

5. Quellen:

- Understanding Cryptography (Christof Paar/Jan Pelzl)
- Kryptographie (Dietmar Wätjen)
- Public-Key Cryptography (Arto Salomaa)
- Elektronische Signatur (Stephan Hochmann)
- Moderne Kryptographie (Ralf Küsters/Thomas Wilke)
- Wikipedia.org
- ECRYPT II Yearly Report on Algorithms and Keysizes (2009-2012)