Inhaltsverzeichnis

1. Einführung in die Kryptologie

Die Kryptologie ist die Wissenschaft der Verschlüsselung und der Entschlüsselung von Informationen. Man teilt diese in 3 Kategorien ein:

1. **Kryptographie**
   Verschlüsselung von Informationen – man spricht hier auch von „Geheimschriften“
2. **Steganographie**
   Verstecken von Informationen – man spricht hier vom Geheimhalten, dass überhaupt eine Information gesendet wird
3. **Kryptoanalyse**
   Entschlüsseln von Informationen ohne Kenntnis des passenden Schlüssels zum decodieren oder auffinden einer Nachricht

Während früher Texte mühsam von Hand sowohl ver- als auch entschlüsselt wurden, so hilft uns hierbei heute die moderne Technik – der Computer. Es gab jedoch auch schon vor dem Computer andere Arten von Maschinen wie z.B. die Enigma, auf welche ich im späteren Verlauf noch eingehen werde.

2. Kryptographie – Einleitung

Die Kryptographie (aus dem griechischen: „kryptos“ = „verborgen“ und „graphein“ = „schreiben“) ist die Wissenschaft der Verschlüsselung von Informationen, um diese vor anderen Personen zu verbergen und somit auch zu schützen. Hierbei geht es nur darum, den reinen Inhalt einer Botschaft für Dritte unzugänglich zu machen. Man codiert eine Nachricht und gibt den so genannten Schlüssel nur an Personen weiter, welche auf die Information zugreifen dürfen. Sie benötigen diesen zum decodieren der Informationen.
Im Laufe der Jahre wurden unzählige Verfahren entwickelt um eine sichere Verschlüsselung zu gewährleisten. Jedoch hat sich keines bis dato als sicher bewiesen. Ob nun der passende Schlüssel zum decodieren einer Botschaft durch systematisches Vorgehen oder nur durch Glück gefunden wurde, so war das Verschlüsselungsverfahren von diesem Zeitpunkt an nicht mehr sicher und damit auch nicht mehr zu gebrauchen.

2.1. Klassische Kryptographie

Die Vorraussetzung für eine verschlüsselte Übermittlung von Informationen ist,

- dass der Empfänger den Schlüssel kennt, den der Sender auch verwendet
- niemand außer Sender und Empfänger diesen Schlüssel kennt
- es ohne Kenntnis des Schlüssels für Dritte nicht möglich oder so schwer wie möglich ist, die Information (auch Klartext genannt) zu decodieren

Schwierigkeiten ergeben sich dadurch, dass Sender und Empfänger

- bevor Sie die Information austausche sich auf einen gemeinsamen Schlüssel einigen müssen
- diesen Schlüssel an keine Dritten weitergeben dürfen, da somit die Botschaft von anderen entschlüsselt werden kann und nicht mehr sicher ist

Früheste Einsätze der Kryptologie findet man bei den alten Ägyptern um 1900 v. Chr. in der Atbash- Verschlüsselung. Im Mittelalter wurde z.B. durch das Alphabetum Kaldeorum diplomatischer Briefverkehr geführt. Im Folgenden werden einige der klassischen Verfahren aufgeführt.

2.1.1 Monoalphabetische Verschlüsselung

Bei der Monoalphabetischen Verschlüsselung wird ein Zeichen genau einem Buchstaben exakt zugeordnet.

2.1.1.1 Atbash Verschlüsselung

Wie eben bereits erwähnt nutzen die alten Ägypter schon die Atbash Verschlüsselung, nur mit dem Unterschied, dass diese nicht nur wie wir das Alphabet mit 26 Zeichen sondern gleich ca. 500 – 600 Zeichen nutzten.

Atbash ist eine eigentlich hebräische Geheimschrift, welche lediglich das Alphabet umdreht. Schreibt man nun diese beide untereinander auf, muss man lediglich den Vergleich machen. Hierbei wird auf Groß- und Kleinschreibung nicht geachtet.

Beispiel:

Wie wollen das Wort „IuT“ Verschlüsseln, 3 Buchstaben ergeben somit 3 Schritte:

Schritt 1:

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

„I zu „R“

Schritt 2:

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

„u“ zu „f“

Schritt 3:

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

„T“ zu „G“

Das Wort ist nun verschlüsselt und heißt „RfG“.

1. Caesar-Chiffre Verschlüsselung

Auch im alten Rom wusste man sich bereits zu helfen um wichtige Botschaften sicher zu übermitteln. Gegeben ist wieder das Alphabet mit 26 Buchstaben mit welchen wir einen Klartext chiffrieren möchten.

Man kann nun entscheiden zwischen 1 bis 26. Die Zahl gibt an wie vom Ausgangsbuchstaben aus codiert werden soll.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Chiffriert man nun mit dem Buchstaben „A“ so muss man den nächsten Buchstaben nach „A“ als Chiffre nehmen. Nimmt man „B“ so den zweiten usw. Es gilt nach „Z“ folgt wieder „A“.

Beispiel 1:

Der Klartext „Zeit“ soll mit „B“ codiert werden.

Original	**„+ 1“**
Z	A
E	F
I	J
T	U

Das Ergebnis ist „AFJU“.

Beispiel 2:

Der Klartext „Zeit“ soll mit „D“ codiert werden.

Original	*+1*	*+2*	**„+3“**
Z	*A*	*B*	C
E	*F*	*G*	H
I	*J*	*K*	L
T	*U*	*V*	W

Das Ergebnis ist „CHLW“.

2.1.2. Polyalphabetische Verschlüsselung

Das Prinzip dieses Verfahrens beruht darauf, dass bei der Übertragung eines Klartexts in eine Geheimschrift mehrere Geheimtextalphabete genutzt werden. Man springt dabei z.B. von jedem Buchstaben in das nächste Alphabet über. Entwickelt wurde dies von Leone Battista Alberti im 15. Jahrhundert.

Beispiel:

Orginal	**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
Geheim1	**Z**	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	**G**	F	E	D	C	B	A
Geheim2	A	F	B	G	C	H	D	I	E	X	V	T	V	U	**J**	Z	Y	L	P	O	**K**	Q	R	M	N	S

Klartext = Auto

Geheimtext = Zkgj

2.1.2.1. One-Time-Pad - Verfahren

Das One-Time-Pad ist aufgrund seiner Aufwendigkeit und Regelung einer der sichersten Verschlüsselungsverfahren. Die Übersetzung liefert auch die Begründung – „Einmal Block“. Hierzu bekamen Sender und Empfänger einen identischen Block aus einzelnen Seiten, welcher immer aus einer andere Reihenfolge von neuen Alphabeten bestand. Nach einmaligem Gebrauch wurde diese Seite anschließend vernichtet. Diese Seiten durften jedoch nicht auf mathematischen Statistiken beruhen sondern mussten immer neu frei erfunden werden, um nicht von Kryptoanalytikern decodiert zu werden.

Eine große Gefahr ist es einen solchen Block von „Codes“ an dem Empfänger zu übermitteln, somit wäre bei einem Abfang eine Menge Arbeit umsonst gewesen.

2.1.2.2. Vigenère- Verschlüsselung

Ein Schlüsselwort bestimmt, wie viele Alphabete genutzt werden. Die Alphabete leiten sich aus dem Caesar-Chiffre Verfahren ab. Durch Aneinanderreihung des Schlüsselwortes kann man den Klartext verschlüsseln.

Beispiel:

Klartext: Referat

Schlüssel: Iut → also I = 8, U = 20, T = 19

Caesar: s. 2.1.1.2. Seite 4 (Prinzip)

R	E	F	E	R	A	T
I	U	T	I	U	T	I
Z	**Y**	**Y**	**M**	**L**	**T**	**B**

2.2. Die moderne Kryptographie

Die moderne Kryptographie beginnt um 1972. 1975 gab es dann 2 Fortschritte gegenüber der klassischen Kryptographie.

Zu einem wurde der „DES“ (Data Encryption Standard 2.2.1) Algorithmus von IBM und der NSA veröffentlicht um sichere Bankdienstleistungen zu ermöglichen, zum anderen die Veröffentlichung des Artikels von Whitfield Diffie und Martin Hellmann, in dem die Schlüsselverteilung eine neue Methode bekam. Bekannt wurde dies durch den „Public Key“ (2.2.2).

2.2.1. Hauptziele der Kryptographie

1. **Vertraulichkeit der Nachricht:**
   Nur der vom Sender bestimmte Empfänger soll die verschlüsselte Nachricht lesen können. Dabei soll keine statistische Verteilung der Zeichen erfolgen.
2. **Verbindlichkeit:**
   Der Absender sollte nicht bestreiten können, die Nachricht an dem Empfänger gesendet zu haben.

3. **Datenintegrität der Nachricht:**
   Der Empfänger sollte eindeutig feststellen können, ob die Nachricht seit der Absendung / Übertragung verändert worden ist.
4. **Authentifizierung:**
   Der Empfänger sollte feststellen können, ob die Ihm übermittelte Nachricht wirklich von dem angegebenen Absender stammt.

2.2.2. Symmetrische Verschlüsselung

Vor der Entwicklung der „Public Key“ Kryptographie waren die Schlüssel symmetrisch. Das heißt, dass man mit dem Besitz eines Schlüssels sowohl verschlüsseln als auch entschlüsseln konnte. Daher musste man den Schlüssel zwischen Sende und Empfänger auf sicherem Wege austauschen lassen. Dieses System wird als „Private Key“ Kryptographie bezeichnet.

2.2.3. Asymmetrische Verschlüsselung

Beim „Public Key“ wir ein paar zusammen gesetzter Schlüssel eingesetzt. Man unterscheidet hierbei zwischen dem,

- Public Key
  Dieser Schlüssel ist öffentlich, mit diesem kann man Informationen verschlüsseln
- Private Key
  Dieser Schlüssel ist geheim, mit diesem kann man Informationen entschlüsseln

Mit dieser Methode wird nur ein einziges Schlüsselpaar für jeden Empfänger benötigt, da der Besitz des Public Key nicht die Sicherheit des Private Key gefährdet.
Nachteile jedoch an diesem Verfahren sind:

- Das Verfahren ist sehr rechenaufwendig und benötigt viel Zeit. Daher gibt es eine Art Trick. Es wird ein symmetrisches Verfahren asymmetrisch verschlüsselt und ausgetauscht. Eine solche Kombination nennt man auch hybride (kombinierte) Verschlüsselung.
- Es ist schwer zu ersehen ob der verwendete Public Key auch wirklich demjenigen gehört, welchen man die verschlüsselte Nachricht senden will. Jemand könnte sich für die eigentliche Person ausgeben und seinen Public Key übergeben. Dieses Problem wird jedoch mit Hilfe der Public Key Infrastructure auch PKI genannt verhindern.

2.2.3.1. Public Key Infrastructure

PKI funktioniert durch die sogenannte Zertifizierungsstelle. Diese ist allgemein anerkannt, und sorgt dafür, dass mittels „Zertifikat“ das einmalige Schlüsselpaar einer natürlichen Person fest zugeordnet wird.
Die Erkennung läuft nun wie folgt ab:

- Jeder Benutzer kennt den Public Key der Zertifizierungsstelle, natürlich haben nur diese den dazu gehörigen Private Key.
- Die Zertifizierungsstelle erstellt einen Dokument (meist Textdatei), in welchem ein Public Key einer natürlichen Person zugeordnet wird und verschlüsselt diesen. Da Jeder den Public Key kennt, kann jeder dieses Dokument auch lesen.
- Somit ist die Datei digital „signiert“, und bei Vertrauen gegenüber der Zertifizierungsstelle kann man mit einem echten Public Key von der richtigen Person rechnen.

2.2.4. DES – Data Encryption Standard

DES ist ein Verfahren zur Datenkompression und -verschlüsselung zur sicheren Übertragung über öffentliche Netze wie dem Internet. Dies fand vor allem Anwendung im Bereich von Banken und Versicherungen. Mit der Hilfe des DES- Algorithmus z.B. wird die PIN einer ec-Karte errechnet durch die Faktoren wie z.B. Kontonummer, Bankleitzahl, Geb. Datum, Gültigkeit etc.).
DES ist ein symmetrisches Verfahren. Gemessen an der Rechenleistung heutiger Computer jedoch und dem damit verbunden Dechiffrierpotenzial ist DES nicht mehr zeitgemäß.

2.2.4.1. Geschichte des DES

Die Geschichte des DES ist im folgendem tabellarisch aufgeführt und chronologisch erläutert.

1972 Das National Bureau of Standards (NBS) startet ein Programm zur sicheren Datenübermittlung. Ziel ist es einen einheitlichen Algorithmus zu finden, welcher sicher ist.

1973 Ausschreibung im Federal Register. Entwicklungsziele sind: hohe Sicherheit und leichte Implementation. Kein eingereichter Vorschlag ist annähernd ausreichend.

1974 Zweite Ausschreibung – IBM reicht einen Vorschlag ein und verzichtet auf das beantragte Patent.

1975 Veröffentlichung des von der National Security Agency (NSA) modifizierten Algorithmus. Nur Aufgrund eines Missverständnisses von der NBS bekannt gegeben.

1976 Trotz des Missgeschicks wurde DES als US-Bundesstandard anerkannt.

1983 Alle 5 Jahre gilt eine Neuzertifizierung des Standards

1987 Anzeichen von Mängel in DES

1993 Da keine Alternative vorhanden ist, erneute Zertifizierung. Eine Maschine zum knacken würde zu diesem Zeitpunkt ca. 1 Mio. Doller kosten und ca. 4 Std. zum knacken brauchen.

1994 Durch lineare Kryptonanalyse wird ein DES- Schlüssel von 12 HP9735 Workstations in 50 Tagen ermittelt.

1998 Ein Computer schafft es durch eine Brute-Force Attacke den Schlüssel in 56 Stunden zu knacken. Diese Maschine kostete 250.000 Dollar.

2.2.4.2. Funktionsweise

Wie bereits erwähnt handelt es sich um eine symmetrische Verschlüsselung, also wird der Schlüssel sowohl zum ver- als auch entschlüsseln genutzt.

DES funktioniert als Blockchiffre, das bedeutet, dass jeder Block einzeln verschlüsselt wird.

Man kann das Verfahren in Grob Drei Schritte einordnen *(s. S10.1)*

Schritt 1:

Der Eingabeblock durchläuft eine Permutation *(Substitution und Transposition nach dem Schema von Feistel*), wodurch die Reihenfolge der einzelnen Bits geändert wird. Das Ergebnis wird in die zwei 32-Bit-Register „L-Block“ und „R-Block“ geschrieben.

Dasselbe gilt auch für den Schlüssel,

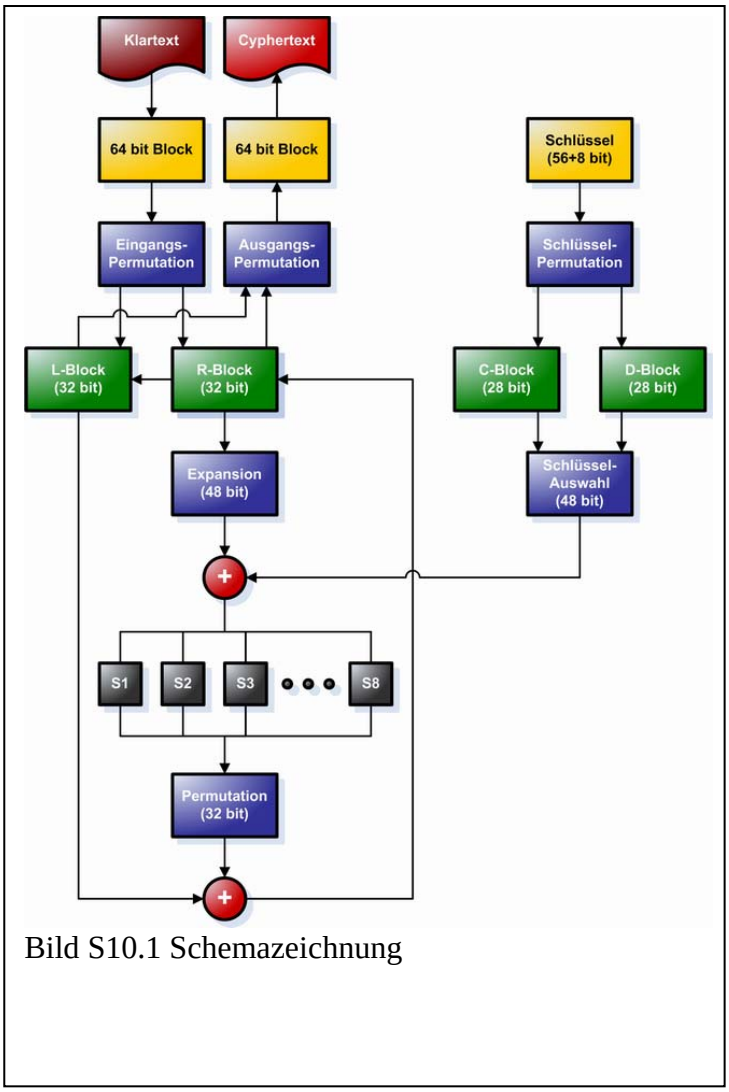


Bild S10.1 Schemazeichnung

jedoch werden hier nur 56 Bits verwendet, da jeweils ein Bit aus einem Byte für den Paritäts-Check benötigt wird. Diese zwei 28-Bit-Register werden in „C-Block“ und „D-Block“ geschrieben.

Schritt 2:

In 16 Iterationen werden 16-mal dieselben Rechenschritte durchgeführt, die Operationen werden durch einer der 16 Teilschlüssel beeinflusst. Nach einer Runde werden die neuen Werte zurück in das Register geschrieben und anschließend neu verarbeitet.

Schritt 3:

Anschließend werden der „L-Block“ und der „R-Block“ nach der 16. Runde wieder zu einem 64-Bit-Wert zusammengefügt. Nun erfolgt noch eine Ausgangspermutation welche invers zur 1. Permutation ist.

2.2.4.3. Schwächen und Ersatz

Weil der „reine“ Schlüssel nur 56 Bit hatte, konnte DES schnell durch eine Brute-Force Attacke (durch systematischen Tests aller Schlüssel) geknackt werden. Bereits in den 70ern hatte die NSA theoretisch genug Rechenkapazität.

„Deep Crack“, so der Name des Super-Computer konnte am 15. Juli 1998 in nur 56 Stunden den DES Code knacken. Diese Maschine enthielt 1536 Chips und konnte somit 88 Milliarde Schlüssel pro Sekunde testen. 1999 wurde durch ein weltweites Netzwerk von 100.000 PCs der Code mit der „Deep Crack“ zusammen in 22 Stunden und 15 Minuten geknackt. In einer Sekunde wurden ca. 245 Milliarden Schlüssel getestet.

Ein Ersatzalgorithmus „3DES“ (Triple DES) findet heute noch Anwendung. Dabei wird der Datenblock mit dem ersten Schlüssel chiffriert mit dem zweiten dechiffriert und dem dritten erneut chiffriert. Der „reine“ Schlüssel beträgt somit 168 Bit. Der Nachteil hierbei ist jedoch das jede Menge Rechenkapazität gefordert ist.

Der offizielle Nachfolger wurde im Oktober 2000 bestimmt und heißt AES (Advanced Encryption Standard) bzw. nach den belgischen Entwickeln Vincent Rijmen und Joan Deamon auch *Rijndael*-Algorithmus genannt.

AES musste folgende Kriterien erfüllen:

- ein symmetrischer Algorithmus sein, und zwar eine Blockchiffre.
- mindestens 128 Bit lange Blöcke verwenden
- Schlüssel von 128, 192 und 256 Bit Länge einsetzen können.
- leicht in Hard- und Software zu implementieren sein.

- eine überdurchschnittliche Performance haben.
- allen bekannten Methoden der Kryptoanalyse widerstehen können
- Der Algorithmus muss frei von patentrechtlichen Ansprüchen sein und darf von jedermann unentgeltlich genutzt werden.

2.2.5. RSA- Kryptosystem

Das RSA Verfahren verdankt seinen Namen aus den Buchstaben der Namen seiner drei Erfinder Ronald Rivest, Adi Shamir und Leonard Adleman und wurde 1977 erfunden. Es handelt sich dabei um einen klassischen Public-Key *(s. 2.2.3.)*.

Die Grundlage für das Verfahren ist, das die Faktorisierung (Zerlegung) einer großen Zahl in min. 2 Faktoren sehr zeitaufwendig ist. Dagegen ist das Erzeugen einer Zahl durch Multiplikation von zwei Primzahlen trivial.

Man nennt dies die so genante Einwegfunktion. Das heißt, dass eine Richtung (Multiplikation) einfach ist, die andere (Faktorisierung) schwer zu berechnen ist. Damit man jedoch entschlüsseln kann, bedarf es einer Zusatzinformation. Man greift hierbei auf die Falltürfunktion zurück.

Beispiel:

Man sieht einen Fuhrpark voll von Autos. Alle sind gleich. Da jedoch das Kennzeichen (Zusatzinformation) bekannt ist, ist die Suche nach dem Richtigen Auto wesentlich einfacher als überall den Schlüssel auszuprobieren.

2.3. Quantenkryptographie

Die Quantenkryptographie ist kein Kryptongraphisches Verfahren im Sinne der eigentlichen Kryptographie. Sie dient dazu den Schlüssel zwischen zwei Partnern sicher auszutauschen. Aufgrund dieser Eigenschaft spricht man eher von einer quantenmechanischen Schlüsselverteilung.

Diese Verschlüsselungstechnik beruht auf den physikalischen Gesetzten der Quantenmechanik und wird daher nicht weiter erläutert sondern nur der Vollständigkeit wegen aufgeführt.

3. Steganographie

Während sich die Kryptographie mit der Verschlüsselung von Informationen beschäftigt, so ist es die Aufgabe der Steganographie die Information zu verbergen, sie es bei der Speicherung oder der Übermittlung.
Die Übersetzung aus dem Griechischen von Steganographie ist „verborgenes Schreiben“. Man soll also Informationen verbergen. Ziel ist es hierbei dem Angreifer nicht die Existenz der eigentlichen Nachricht zu vermitteln. In der Geschichte taucht die Steganographie bereits beim Wasserzeichen, Papier oder Banknoten auf.
Ein weiteres Anwendungsgebiet ist außer dem verstecken der Botschaft, auch eine Prüfung des Ursprungs um zu zeigen ob eine Datei verändert worden ist.
Die sicherste Lösung ist die Kombination der Kryptographie und der Steganographie.
Mögliche Methoden der Steganographie sind z.B.:

- Unsichtbare Tinte
  Wird das Dokument neu geschrieben also gefälscht, so merkt es der Empfänger da er die verborgene Tinte nicht auffindet.
- Mikropunkte
  Wird das Dokument neu geschrieben also gefälscht, so merkt es der Empfänger da er die Mikropunkte nicht auffinden kann.
- Einbetten einer Nachricht in einer anderen
  Hierzu eignen sich digitale Medien

3.1. Symmetrische Steganographie

Die Symmetrische Steganographie bedeutet, das wie bei der symmetrischen Kryptographie Sender um Empfänger den geheimen Schlüssel – sowohl zum ver- als auch entschlüsseln – ausgetauscht haben und besitzen.
Beiden ist bewusst auf welche Art und Weise an welcher Stelle die eigentliche Botschaft versteckt ist. Nur durch Kenntnis des Schlüssels ist die Erkennbarkeit gewährleistet.

3.2. Asymmetrische Steganographie

Auch hier greift das Prinzip der asymmetrischen Kryptographie. Also der Sender kann durch die Bereitstellung des Public Key nur verschlüsseln. Das Problem hierbei ist jedoch das Sender nicht herausfinden kann, ob sich seine Nachricht im Medium versteckt, außer er kann

das Trägermedium mit dem Steganogramm (Trägermedium inkl. der Botschaft) vergleichen. Daher ist die asymmetrische Steganographie nur schwer zu schaffen.

3.3. Arten der Steganographie

Man unterscheidet zwischen der technischen Steganographie (s. 3.3.1.) und der linguistischen Steganographie (s 3.3.2.).

3.3.1. Technische Steganographie

Technische Steganographie entspricht einer unsichtbaren Geheimschrift. Jüngstes Beispiel in der Geschichte ist hierbei der griechische Geschichtsschreiber Herodot. Um 400 v. Chr. ließ er seinen Sklaven eine Glatze schreiben und darauf die Nachricht tätowieren. Nach dem genug Haare nachgewachsen waren konnte die Nachricht übermittelt werden. Durch erneutes schneiden einer Glatze konnte der Empfänger diese lesen.
Ein weiteres Beispiel ist die Geheimtinte. Zwiebelsaft wird durch eine erneute Erwärmung z.B. auch UV-Strahlung wieder Sichtbar.

3.3.1.1. Computer gestützte Steganographie

Die Computer gestützte Steganographie lässt sich vor allem besonders gut an Bild und Sounddateien anwenden. So werden z.B. einzelne Bits überschrieben und die verborgene Information darin eingebettet.
Bei einer Grafik z.B. haben die niederwertigsten Bits einen so kleinen Einfluss auf das Bald, so das die dadurch entstehenden Bildstörungen mit dem Auge nicht erkennbar sind. Während der Empfänger nun weiß wie er vorzugehen hat, weiß ein unbefugter Dritter nicht das statt eines Bildes (das Trägermedium) vor Ihm unzählige Informationen vorliegen.
Man muss jedoch darauf Achten, dass man nicht nach einer Einbettung von Informationen das Dateiformat ändert. So würde z.B. durch eine Kompression vom BMP Format in das JPG Format die Information zerstört werden.

3.3.2. Linguistische Steganographie

Linguistische Steganographie entspricht einer getarnten Geheimschrift. Die linguistische Steganographie lässt sich in zwei große Teilbereiche gliedern: „Open Code“ (s. 3.3.2.1.) und „Semagramme“ (s. 3.3.2.2.).

3.3.2.1. Open Code

Open Code bedeutet sich eine eigene Geheimsprache einfallen zu lassen, oder ein Art Muster von Geheimzeichen in einem Text einzubetten. Dieses Muster oder die erfundene Sprache kann nicht so einfach von Dritten identifiziert werden. Man unterscheidet hierbei zwischen „maskierter“ (s. 3.3.2.1.1.) und „getarnter“ (s. 3.3.2.1.2.) Geheimschrift.

3.3.2.1.1. Maskierte Geheimschrift

Die maskierte Geheimschrift ist eine Geheimsprache. Ausdrücke oder Worte erhalten eine neue Bedeutung. Natürlich muss der Empfänger diese Sprache verstehen.

Beispiel 1:

Mit dem Wort Kohle ist nicht das Material zum heizen gemeint, sondern Geld.

Beispiel 2:

Während eines Kartenspiels bedeutet der erste Buchstabe des ersten Wortes bei einem Satz, welcher Kartentyp gespielt wird, bzw. die Anzahl der Wörter im Satz welcher Wert.

Satz / Aussage: Hammer

Karte: Herz 7

Begründung: Das erste Wort beginnt mit „H“ und 7 ist der niedrigste Wert in diesem Spiel.

3.3.2.1.2. Getarnte Geheimschrift

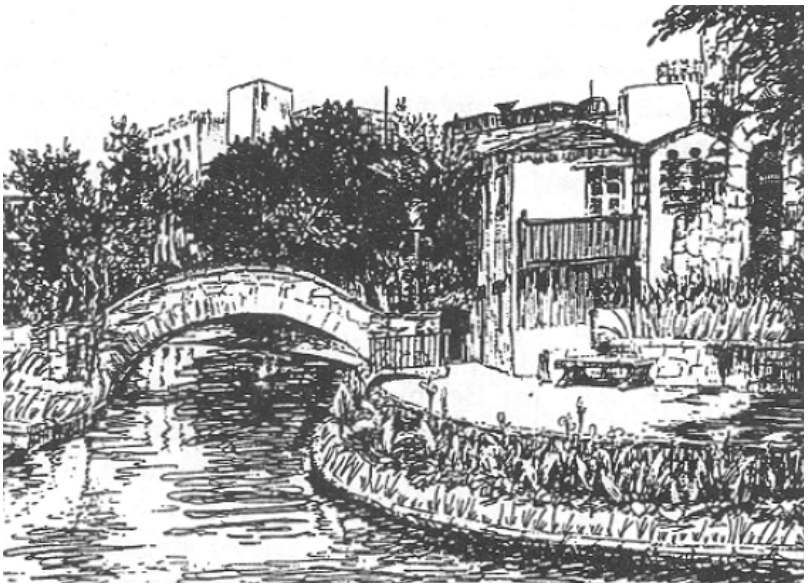
Die geheimen Zeichen stehen bei der getarnten Geheimschrift in einem bestimmten Muster zusammen. Auch hier ist es wichtig, dass der Empfänger weiß wie er vorgehen muss. Schwierig ist es hierbei Sinnvolle Texte zu verfassen.

3.3.2.2. Semagramme

Bei einem Semagramm werden kleine Details in ein Bild oder eine Zeichnung eingetragen. Der Empfänger wiederum weiß was er mit dem Trägermedium anfangen muss um an die Information zu gelangen.

Beispiel:

Die Nachricht steht im Morsecode, der aus kurzen und langen Grashalmen links von der Brücke entlang des Flusses und auf der kleinen Mauer gebildet wird *(s. S16.1).*



S16.1 Beispiel eines Semagramm

Natürlich gibt es auch andere Möglichkeiten, wie z.B. die Wahl verschiedener Schriftarten (Block und Schreibschrift). Jedoch kann hier ein auch ein ungeübtes Auge, das nach geheimen Informationen sucht schnell zum Ziel – die wahre Nachricht – kommen.

4. Kryptoanalyse

Während die Kryptographie und Steganographie sich damit beschäftigen wie man etwas verschlüsselt und anschließend den Rückweg zum entschlüsseln geht, beschäftigt sich die Kryptoanalyse damit wie es gelingt den Schlüssel oder den Klartext zu erlangen.
Hierbei zählt ein wiederkehrendes Muster zu erkennen und das so genannte Social Engineering – dies bedeutet, dass man an die Information durch gesellschaftliche Kontakte kommt. Vor dem Zeitalter der Computer war die Statistik jedoch das beste Mittel geheime Informationen oder den Schlüssel zu erlangen, da sich ein Mensch nicht zu komplizierte Algorithmen wie ein Computer in einem Programm merken konnte.

4.1. Kerckhoffs Prinzip

August Kerckhoffs Prinzip ist heute ein Designkriterium für die moderne Kryptographie. Hiernach geht hervor, dass nicht der Algorithmus geheim gehalten werden soll, sondern nur der Schlüssel – also die Zusatzinformation zum ver- oder entschlüsseln.

4.2. Angriffsmethoden

Ziel einer Angriffsmethode ist es in Besitz des geheimen Schlüssels zu kommen, der dann in der Zukunft beliebige Entschlüsselungen erlaubt. Einige Verfahren sind im folgendem aufgelistet, diese haben jedoch bei einem modernen Verfahren wie z.B. RSA mit sehr komplexen Schlüsseln bisher nicht den geheimen Schlüssel finden können. Einige der genannten Methoden lassen sich auch im übrigen kombinieren.

4.2.1. Brute-Force

Bei einer Brute-Force Attacke werden alle möglichen Schlüssel nacheinander ausprobiert. Diese Methode ist besonders bei sehr kleinen Passwörtern anwendbar.

4.2.2. Wörterbuch Attacke

Auch hier werden alle möglichen Schlüssel nacheinander ausprobiert. Man geht hierbei von einem Standard Wort aus. Ausgehend davon, dass eine Sprache etwas mehr als 50.000 Worte besitzt, kann man solche Attacken auch sehr gut bei kleinen „ein Wort“ Passwörtern wie z.B. Namen anwenden.

4.2.3. Known Plaintext

Angreifer hat sowohl Klartexte als auch Geheimtexte und versucht diese zu Untersuchen um auf den Schlüssel zu kommen.

4.2.4. Probable Plaintext

Angreifer kennt die Geheimtexte und geht systematisch vor nach Wortgruppen etc. nach dem Schlüssel zu suchen.

5. Fazit

Die Kryptologie ist heute unverzichtbar geworden, sowohl die Kryptographie als auch Steganographie um Informationen vor Dritten zu schützen, als auch die Kryptoanalyse, welche von Geheimdiensten genutzt wird um z.B. die Innere Sicherheit zu gewährleisten. Natürlich wird die Kryptologie nicht nur von den „Guten“ genutzt, welches Sie wiederum zu einer Gefährlichen Waffe macht.

Bedenkt man, dass min. eine Person immer weiß wie der Schlüssel lautet, so muss man auch bedenken das es immer einen Weg gibt an diese Information zu gelangen – außer man versteckt die Person vor der Außenwelt oder hatte eine KI welche unantastbar für andere ist.

6. Glossar

Begriff	Erklärung
3DES	Triple DES
AES	Advanced Encryption Standard
Asymmetrisch	bedeutet nicht eben
Authentifizierung	Prüfung durch ein zugewiesenes Merkmal
Blochchiffre	Blockverschlüsselungsalgorithmen
Datenkompression	Verfahren zur Reduktion des Speicherbedarfs
DES	Data Encryption Standard
Faktorisierung	Zerlegung
IBM	International Business Machines
Iteartion	von lateinisch iterare, "wiederholen"
Kryptographie	verborgenes Schreiben
Kryptologie	Techniken zur Ver - und Entschlüsselung von Daten
linguistisch Steganographie	getarnte Geheimschrift
Monoalphabetisch	mono = eins ; hier ein Alphabet
NBS	National Bureau of Standards
NSA	National Security Agency
One-Time-Pad	entspricht Einmalblock
Permutation	Veränderung der Reihenfolge der Elemente einer Menge X
PIN	Persönliche Identifikationsnummer
PKI	Public Key Infrastructure
Polyalphabetisch	poly = viele ; hier mehrere Alphabete
Private Key	geheimer Schlüssel
Public Key	öffentlicher Schlüssel
Schlüssel	Zusatzinformation
Social Engineering	Information durch gesellschaftliche Kontakte
Steganographie	verborgenes Schreiben
Symmetrisch	von Symmetrie (gr. symmetria) bedeutet Ebenmaß
technische Steganographie	unsichtbare Geheimschrift

Quellen

Offline Quellen:

Altes Schulmaterial	Referat Kryptologie HHI001

Online Quellen:

http://www.wikipedia.de	Suchwort Kryptologie
http://www.wissen.de	für die Erstellung des Glossar