Fachhochschule Wedel

University of applied sciences

Eine Einführung in die Grundbegriffe der Kryptologie:

Kryptographie, Kryptoanalyse, Steganographie,

Kerckhoffs'sches Prinzip.

Seminararbeit

Abgabedatum: 24. Mai 2017

Vorgelegt von:	Farzad Khojazada
Adresse:	Schafshagenberg 18, 21077 Hamburg
Matrikelnummer:	100540
Studiengang:	Wirtschaftsingenieur
Email:	wing100540@fh-wedel.de
Betreuer:	Prof. Dr. Michael Anders

Inhaltsverzeichnis

Abbildungsverzeichnis

Literaturverzeichnis

Atterer, R. (2014). Atterer.org. Retrieved Mai 29, 2015, from http://atterer.org/uni/crypto.html#idea

eheime Botschaften – Dier Kunst der Verschlulüsselung von der Antike bis in die Zeiten des Internets- Autor Simon Singh

Bauer, F. L. (2000). Entzifferte Geheimnisse, Methoden und Maxime der Kryptologie (3. Überarbeitete Auflage ed.). Grafrath: Springer Verlag.

Beutelspacher, A. (1996). Kryptologie (5. Auflage ed.). Vieweg Verlag. Beutelspacher, A. (2009). Kryptologie (9. Auflage ed.). Vieweg+Teubner Berlag. Buchmann, P. D. (2000). Einführung in die Kryptographie (2. ed.). Darmstadt: Springer

Verlag. Miller, M. (2003). Symmetrische Verschlüsselungsverfahren

(1. Auflage ed.). Stuttgart: B.G:

Teubner.

Kryptologie-Kompendium – Autor Uwe Schönimg

Schmeh, K. (2008). Codeknacker gegen Codemacher. Die faszinierende Geschichte der Verschlüsselung (2. Auflage ed.). Herdecke: W3l-Verlag.

Nicht zu Knacken – von ungelösten Enigma-Codes zu den Briefen des Zodiac Killers- Autos Klaus Schmeh

Schneier, B. (1996). Applied Cryptography (2. Auflage ed.). New York: John Wiley and Sons.

Stobitzer, C. (n.d.). Kryptowissen.de. Retrieved 06 05, 2015, from http://www.kryptowissen.de

Swoboda, J., Spitz, S., & Pramateftakis, M. (2008). Kryptographie und IT-Sicherheit (1. Auflage ed.). München und Athen: Vieweg+Teubner Verlag.

Wätjen, D. (2004). Kryptographie - Grundlagen, Algorithmen, Protokolle. Spektrum Akademischer Verlag.

Kryptorafie- Autor Klaus Schmeh

Yotwen. (2015, 03 23). Retrieved 06 02, 2015, from Wikipedia-Kryptographie: https://de.wikipedia.org/wiki/Kryptographie

Kryptografie Verfahren (2012), Protokolle, Infrastrukturen 5., aktualisierte Auflage Autor Klaus Schmeh

Kryptologie – von einer Geheimwissenschaft zu einer Wissenschaft von den Geheimnissen Dr. Jörg Vogel

1. Einleitung

Das Bedürfnis vieler Menschen nach ein wenig Privatsphäre im Zeitalter der weltumspannenden öffentlichen Kommunikation ist verständlich.
Ohne großen Aufwand können heutzutage Telefongespräche , Briefe und geschäftliche Transaktionen belauscht oder sogar verändert bzw. verfälscht werden. Grade in der heutigen Zeit nehmen Onlinetransaktionen, digitale Signaturen und Webkommunikation erheblich an Bedeutung zu.
Sie sind ein fester Bestandteil unseres Lebens geworden und verdienen zu recht speziellen Schutz vor Dritte. Bei der Kryptologie geht es im Grunde genommen, um den Kampf der Geheimhaltung. Auf der einen Seite sind die "Codeentwickler" und auf der anderen Seite die "Codebrecher". Dieser Kampf geht schon seit Jahrhunderten und ihr Verlauf ist dementsprechend eine sehr spannende Geschichte. Es ist ebenfalls eine Geschichte die enormen Einfluss auf die Weltgeschichte hat. Der Verlauf von Schlachten, die Ergebnisse von Kriegen und die Schicksale von Nationen hing von "Codeentwicklern" und "Codebrechern" ab. Geheimschriften sind Kinder des Krieges, meist ging es um Informationen für Angriffspläne, Truppenstärken und um List und Tücke. Von den alten Codes bis zum zweiten Weltkrieg sind die meisten veröffentlicht, ihre Geschichte ist vielfach aufgeschrieben und man kann sich die Geschichten einfach besorgen und durchlesen. Nach 1950 wurden Codes nicht nur im Regierungsauftrag, sondern mehr und mehr in den Universitäten und in der Wirtschaft entwickelt. Den mit dem Eintritt in das Informationszeitalter interessieren sich Forscher und Entwickler auch dafür, wie sich die Allgemeinheit dafür einsetzen kann, ihre Privatsphäre zu schützen.
Von dort an passierten die meisten wichtigen Durchbrüche der Kryptologie in der Öffentlichkeit. Die Leute veröffentlichen ihre Arbeiten und sprechen frei darüber. Alles worüber ich schreibe ist öffentlich zugänglich und kann von jedem genutzt werden, aber mit Sicherheit geht hinter verriegelten Türen viel vor, von dem man nichts weiß , von dem ich nichts wissen oder schreiben darf.
Die Leute, die das abstreiten arbeiten vielleicht für die Regierung oder unterliegen der Geheimhaltung.
Um eine Einführung in die Begrifflichkeiten zu verschaffen ist es vom Vorteil im ersten Schritt einmal kurz auf die Definition der Kryptologie einzugehen und später tiefer in die Materie einzusteigen. Kryptologie setzt sich zusammen aus den beiden griechischen Wörtern „kryptós", verborgen/ verbergen , und „logos" = Lehre. Sie ist also die Lehre des Verborgenen. Wenn jemand von Kryptologie redet, darf man dies nicht mit dem ähnlichen Begriff Kryptographie oder gar Kryptoanalyse verwechseln.
So teilt man die Kryptologie, die ganz oben an der hierarchischen Struktur steht, in zwei Unterthemen ein.
Diese sind wiederum in viele Themen unterteilt. Grundsätzlich unterscheidet man bei der Kryptologie zwischen der Kryptographie und der Kryptoanalyse.

In der Reihenfolge habe ich auch mein Inhaltsverzeichnis und den Verlauf meiner Seminararbeit ausgelegt. Ich fange mit dem Thema Kryptologie an und gehe dann auf die beiden Punkte Kryptographie und Kryptoanalyse näher ein.
Der folgende Strukturbaum soll die Reihenfolge meiner Arbeit näher beschreiben und meinen roten Faden durch die Ausarbeitung darstellen.

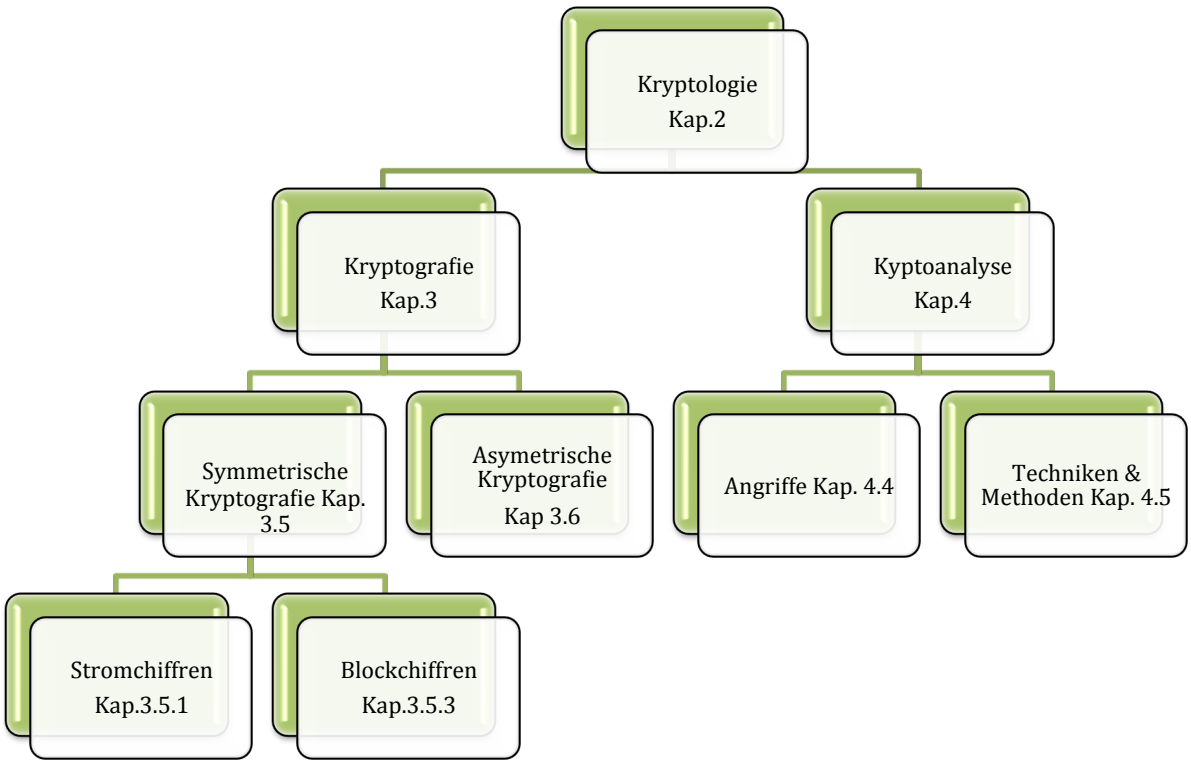

Abbildung 1: Strukturbaum der Kryptologie

2. Kryptologie

Wir alle haben Geheimnisse und wollen unsere Privatsphäre schützen. Andererseits möchten wir alle Geheimnisse unserer Konkurrenten und Feinde wissen. Während wir versuchen unsere eigenen Geheimnisse zu schützen, versuchen wir die Geheimisse anderer zu stehlen, auf der zwischenmenschlichen- , militärischen- oder politischen Ebene. Die Methode Botschaften für andere unlesbar zu machen, heißt verschlüsseln oder chiffrieren. Beim Chiffrieren geht es darum die eigentliche Botschaft bzw. den Klartext, mit Hilfe eines Schlüssels in eine verschlüsselte Botschaft oder auch Chiffretext umzuwandeln. Unter Schlüssel versteht man in der Kryptologie, einen oder mehrere Verfahren, die angewendet werden müssen, um ein Chiffretexte zu generieren. Die Länge eines Schlüssels kann dabei den Grad der Komplexität eines Chiffretext bestimmen und somit die Sicherheit eines Systems. Die Methode verschlüsselte Texte des Absenders zu entschlüsseln heißt dechiffrieren. Beim Dechiffrieren wird durch umkehren des Verschlüsselungsverfahrens versucht, die verschlüsselten Botschaft zurück in den Klartext zu transformieren.

Oft wird im Sprachgebrauch für dechiffrieren auch entziffern oder brechen verwendet, was fachbegrifflich nicht ganz stimmt.
Das Entziffern oder Aufbrechen ist die Kunst, verschlüsselte Texte ohne den dazugehörenden Schlüssel zu knacken. Derjenige, der dies tut, nennt man Kryptoanalyst oder Angreifer. Unter einem passiven Angriff versteht man das unbefugte Lesen übertragenen Nachrichten. Von einem aktiven Angriff stricht man, wenn die übertragene Nachricht nicht nur gelesen, sondern auch verändert wird.
Die Technik, in der viele ihre Hoffnung setzten ist die Kryptographie, die Technik des Verschlüsseln von Geschriebenen. Bei der Kryptographie geht es darum Verfahren und Algorithmen der Verschlüsselung zu entwerfen, während es bei der Kryptoanalyse darum geht diese entworfenen Verfahren auf ihre Stärken und Schwächen zu testen und daraus Rückschlüsse auf ihre Schwachstellen zu ziehen.

Das Prinzip des Verschlüsselns soll folgende Darstellung hervorheben.
Der Sender verfaßt einen Klartext und läßt diese Botschaft verschlüsseln.
Diese verschlüsselte Botschaft gelangt dann über einen ungesicherten Übertragungsweg zum Empfänger. Dieser muss den Chiffretext, dechiffrieren und gelangt so auf den Klartext.

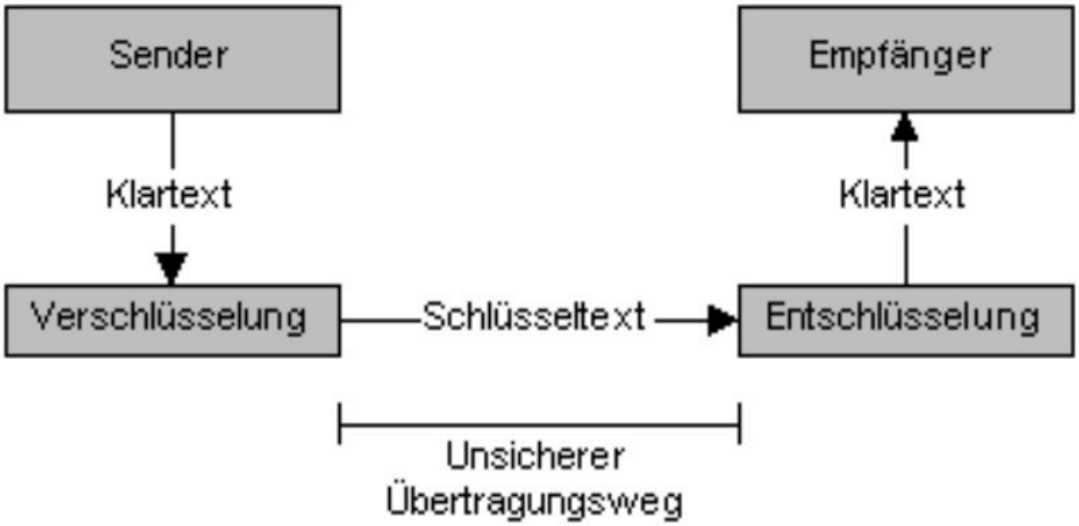

Abbildung 2: Prinzip der Verschlüsselung

Solange der Algorithmus zum Entschlüsseln geheim bleibt, ist die Nachricht sicher. Selbst wenn sie auf dem Übertragungsweg entdeckt wird, kann kein Dritter sie entschlüsseln. Wird das Entschlüsselungsverfahren dagegen entdeckt, kann die Nachricht und mit ihr, alle anderen Nachrichten, die mit demselben Verfahren verschlüsselt wurden, entziffert werden. Da man bei den vielen Verschlüsselungsverfahren, außer mit besonderes Maßnahmen, nicht sicher sein kann, dass niemand die Botschaft mitliest, spricht man bei der Entsendung einer Botschaft über den digitalen Weg, von einem unsicheren Übertragungsweg.

3. Kryptographie

Die erste Entdeckung von Geheimschriften finden wir bei Herodot, dem griechischen Philosophen und Geschichtsschreiber aus dem fünften Jahrhundert. Der Perserkönig Xerxes trachtete danach, die griechischen Städte Sparte und Athen zu erobern. Innerhalb von fünf Jahren stellte er die größte Streitmacht in der Geschichte seines Landes zusammen. Es sollte ein Überraschungsangriff werden. Einen Griechen jedoch, der von seiner Heimat verstoßen worden war und in Persien lebte, entging die gigantische Aufrüstung nicht. Er musste den Spartanern eine Nachricht zuschicken, um sie zu warnen. Aber wie sollte er diese an den Persern vorbeischmuggeln. Da half nur eine List.
Er nahm eine kleine Schreibtafel und schabte das Wachs ab und schrieb auf das Holz was Xerxes vorhatte. Dann goß er wieder Wachs auf die Schrifttafel, um die Botschaft zu verbergen. Tatsächlich gelangt die Tafel nach Sparta, doch dort wusste man nichts mit ihr anzufangen. Eine Frau schrieb Herodot ,war es schließlich gewesen, die buchstäblich hinter das Geheimnis kam und das Wachs von der Tafel kratze.
So kam die Geheimbotschaft und damit die Aufrüstungspläne ans Licht.
Als Xerxes losschlug, stellten sich die Griechen dem verblüfften Perserkönig mit einer ebenfalls großen und gut gerüsteten Streitmacht entgegen.
Diese Art der Geheimbotschaft, in der man verheimlicht das Überhaupt eine Botschaft existiert, nennt man Steganographie. Das griechische Wort „Steganos“ heißt gedeckt und „Graphen“ bedeutet schreiben.
Bedecktes unsichtbar geschriebenes gab es überall auf der Welt.
Zur Steganographie gehört selbstverständlich auch die unsichtbare Tinte, die man schon seit dem ersten Jahrhundert nach Christus kannte. Dafür wird das Milch der Tithymalus-Pflanze verwendet. Sie wird nach dem trocknen durchsichtig und färbt sich beim Erhitzen braun. Eine Verbergungstechnik mit modernen mitteln, ist zum Beispiel ein Text , der fotografisch auf einem Punkt von kaum einem Millimeter Durchmesser verkleinert und auf ein scheinbar harmlosen Brief gesetzt wird.
Das FBI entdeckte 1941 den Ersten dieser Mikro Punkte, nachdem das Sie einen anonymen Hinweis bekommen hatte. Doch die Gefahr des Verrats ist bei dieser Methode sehr hoch und wenn die Botschaft erst mal entdeckt wird, ist sie sofort lesbar, deshalb entstand mir der Steganographie, die eigentliche Kryptographie vom griechischen „Krypthos“ "verborgen".
Ziel ist es hier nicht die Botschaft selbst, sondern den Sinn zu verbergen.
Voraussetzung ist das Sender und Empfänger sich kennen und das Verschlüsselungssystem vorher abgesprochen haben.

3.1. Prinzip der Kryptographie

In der Kryptographie kann man mit einer Nachricht zweierlei machen.
Man kann entweder alle Buchstaben aus dem Klartext willkürlich mit anderen Buchstaben oder Zeichen ersetzten,
anstelle des „H“ schreibt man ein „T“ , statt „A“ schreibt man „g“, anstelle das „L“, schreibt man „q“ und so weiter , dies wird als Substitutionsmethode bezeichnet.
Die andere Verfahren heißt Transposition oder Permutation , das bedeutet man verändert nicht die Buchstaben eines Textes, sondern man setzt sie an anderer Stellen.

Also bei dieser Methode schreibt man die Buchstaben beispielsweise in umgekehrter Reihenfolge oder vertauscht den ersten Buchstaben mit dem zweite Buchstaben, den zweiten Buchstaben mit dem sechsten Buchstaben, dem dritten mit dem fünften und so weiter. Die Transposition ändert die Anordnung der Zeichen in der Reihenfolge, lässt das Auftreten der Zeichen jedoch unverändert. Aus dem Wort Kryptographie wird dann Rkpyotrgpaihe. Alle Codes basieren mehr oder weniger auf diesen 2 Prinzipien, ob sie nun tausend Jahre alt sind oder ganz modern. Es ist nur die Frage wie komplex die Substitution oder die Transposition ist. Die heute gebräuchlichen modernen Schlüssel sind deshalb so Sicher, weil es mehrere hundert Trilliarden verschiedenen Kombinationsmöglichkeiten von einer Substitution geben kann.
Es würde einfach zu viel Zeit in Anspruch nehmen alle Möglichkeiten durchzugehen.
Zusammengefaßt lässt sich sagen, in der Kryptographie unterscheidet man zwischen zwei grundsätzliche Schlüsselverfahren. Das Transpositionsverfahren und das Substitutionsverfahren, wobei die modernen Schlüssel sogenannte “pseudo Zufallsgenerator“ beinhalten, auf die wir später näher eingehen werden.

3.2. Klassische Kryptographie

Grob gesehen kann man die Kryptographie in zwei Bereiche eingliedern, in klassische und moderne kryptographischer Verfahren.
Die klassischen Verfahren gelten eher als unsicher, weil sie ohne elektronische Rechner generiert werden können und immer vollständige Buchstaben oder Buchstabenkombinationen benutzen.
Zu den klassischen Verfahren gehörten unter anderem Skytale, Krebsalgorithmus, Cäsar-Verschlüsselung und Gartenzaunverfahren, die zum Teil sehr großen Einfluß auf die Weltgeschichte genommen haben und auf die ich deshalb kurz näher eingehen möchte.

3.2.1. Skytale

Beim Skytale wurde als Schlüssel ein runder oder meist sechseckiger Stab verwendet. Um diesen Stab wurde wendelförmig eine langes Lederband herum gewickelt und die Botschaft draufgeschrieben. Nachdem das Lederstück vom Stab entnommen wird, könnte man annehmen eine Reihe sinnlos aneinandergereihte Buchstaben vorzufinden.
Der Empfänger kann mit einem identischen Stab die Nachricht Lesen.
In dem Fall war der Durchmesser des Stabes der Schlüssel zum Ver- und Entschlüsseln. Der Chiffretext sieht aus wie eine willkürlich zusammengewürfelte Kombination aus Buchstaben, der Klartext hingegen könnte das Ergebnis einer Schlacht signifikant verändert haben. So wie auf dem folgenden Bild könnte eine Botschaft ausgesehen haben:

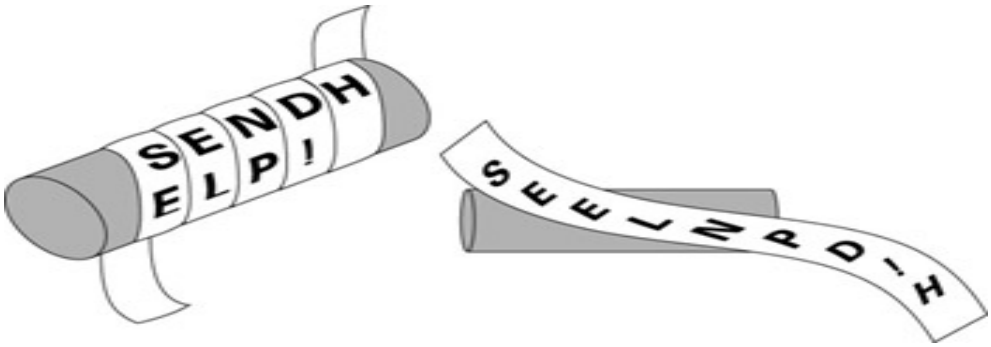

Abbildung 3: Musterdarstellung einer Skytale

Bei der Substitutionsverfahren werden die Buchstaben aus dem Klartext durch ein anderes Symbol oder Buchstaben ersetzt.
Zu den Substitutionsverfahren zählen unter anderem die Caesar-Verschlüsselung und die Vigenère-Verschlüsselung.

3.2.2. Cäsar-Verschlüsselung

Bei der Cäsar-Verschlüsselung hat man sich auf die Zahl „Drei“ geeinigt.
Jeder Buchstabe aus dem Klartext wurde drei Buchstaben verschoben. Bei “Z“ angekommen begann man wieder beim Anfang. Aus einem "A" wird durch eine Verschiebung, um drei Zeichen der Buchstabe "D", aus "X" wird durch ein "A" und aus "Y" durch "B" usw. Damit ergibt sich am Ende folgende Tabelle:

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
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

Abbildung 4: Ceser-Verschlüsselungstabelle

Aus unserer Botschaft „sendhelp“ wird mit der Cesar-Verschlüsselung, „vhqgkhos“ generiert.

3.3. Kryptographische Ziele

In dem Zusammenhang ist es aber wichtig auf die Ziele der Kryptographie einzugehen. Die modere Kryptographie verfolgt 4 Hauptziele zum Schutz von Datenbeständen, Nachrichten und Übertragungskanäle.

1. Vertraulichkeit: Nur eine bestimmte Person oder ein bestimmter Personenkreis soll Zugang zu den Informationen haben und diese lesen können.

2. Integrität: Die Daten müssen nachweisbar vollständig sein und unverändert bleiben, um sicherzustellen das keiner den Inhalt verändert hat.

3. Authentifizierung: Der Absender der Nachricht muss eindeutig identifizierbar sein und seine Urheberrechte sollten nachprüfbar sein.

4. Verbindlichkeit: Der Absender der Datei soll in der Lage sein, seine Urheberschaft gegenüber dritten nachzuweisen.

3.4. Moderne Kryptographie

In Abgrenzung zur klassischen Kryptographie meint die moderne Kryptographie alle komplexeren Verfahren, die meist unter Einsatz eines Rechners verwendet werden.
Die moderne Kryptographie kann man in drei Bereiche einteilen, in die symmetrische Verfahren, asymmetrische Verfahren und in die hybrid Verfahren.

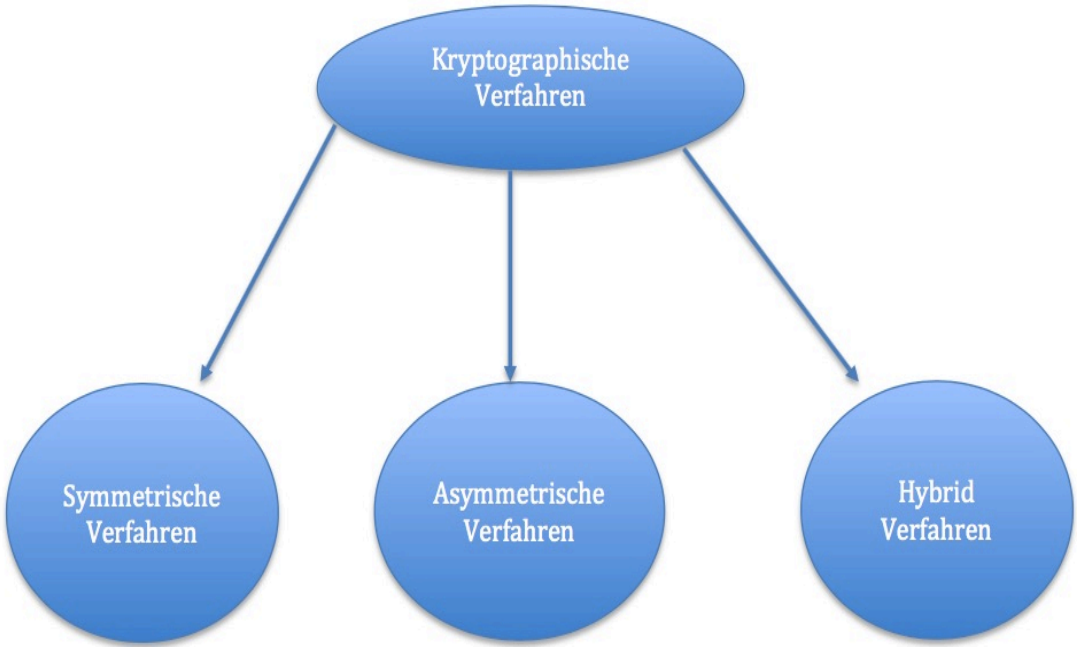

Abbildung 5: Darstellung zur Unterteilung der Kryptographie

3.5. Symmetrische Kryptographie

Das Symmetrische Verschlüsselungsverfahren auch Secret-Key-Kryptographie oder Secret-Key-Verschlüsselung genannt, arbeitet mit einem einzigen Schlüssel, welcher der ver-und entschlüsselnden Seiten bekannt sein muss.
Sender und Empfänger müssen sich auf einen Schlüssel einigen, bevor die verschlüsselte Kommunikation stattfinden sollte.
Ganz wichtig ist die sichere Übertragung des Schlüssels, denn sie sollte über einen gesicherten Kanal erfolgen. Denn gelangt erst einmal der Schlüssel in falsche Hände, ist es kein Problem mehr die verschlüsselten Nachrichten zu entschlüsseln.
Der geheime Schlüssel ist vorab von Sender (A) und Empfänger (B) vereinbart worden. Sender (A) verfaßt einen Klartext, dieser wird mit dem geheimen Schlüssel verschlüsselt, gelangt über das Internet zum Empfänger (B), dieser entschlüsselt mit dem Schlüssel den Chiffretext und empfängt die Botschaft.

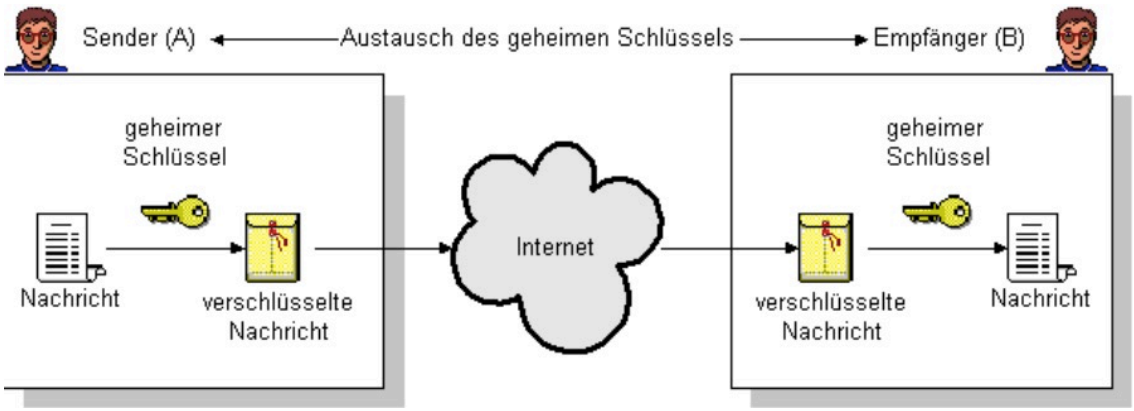

Abbildung 6: Symmetrische Verschlüsselungsverfahren

Bei den wertgeschätzten klassischen Verschlüsselungsverfahren, wie dem Skytale oder der Cäsar-Verschlüsselung, handelte es sich ebenfalls um symmetrische Verschlüsselungsverfahren. Nur die Anwendung unterscheidet sich zu den heutigen Algorithmen. Man teilt die symmetrischen Verfahren in Blockchiffren und Stromchiffren auf. Mit Stromchiffren wird der Klartext Zeichen für Zeichen verschlüsselt. Eine Blockchiffre arbeitet mit einer festen Blockgröße und ver- bzw. entschlüsselt mehrere Zeichen in einem Schritt.

3.5.1. Stromchiffren

Wie bereits kurz behandelt, unterscheidet man bei der symmetrischen Chiffrierung zwischen der Blockchiffren und den Stromchiffren.
Wobei die Stromchiffren auch als sequentielle Chiffren bezeichnet werden.
Alle gängigen symmetrischen Verschlüsselungsverfahren gehören entweder zu den Block- oder zu den Stromchiffren.
Eine Stromverschlüsselung ist ein kryptographisches Algorithmus bei dem Zeichen des Klartext mit dem Zeichen eines Schlüsselstroms einzeln verknüpft werden.
Der Schlüsselstrom ist normalerweise ein pseudo zufällige Zeichenfolge, die aus dem Schlüssel abgeleitet wird.
Die zufällige Zeichenfolge wird mit dem XOR-Operator gebildet.
Der XOR-Operator ist eine Schalfunktion, die aktiviert wird, wenn bei mehreren Eingängen nur ein Ausgang aktiviert wird. Wenn alle Eingänge aktiviert sind, ist der Ausgang gleich “0“, ebenso wenn alle Eingänge nicht aktiviert sind, ist der Ausgang “0“. Ist der Eingang eines XOR-Operators “1“, dann ist der Ausgang auch gleich “1“.

Die zufällige Zeichenfolge, die durch der Stromchiffre generiert wird, nennt man Keystream. Die wichtigste Regel bei den Stromchiffren ist, das der Keystream auf keinen Fall mehrfach verwendet werden darf.
Halten sich zwei in kontaktstehende Kommunikationspartner nicht daran, dann können von Angreifern eine Attacke gestarten werden, indem sie zwei Geheimtexte, die mit demselben Keystream generiert wurden, miteinander vergleichen. Als Ergebnis erhält er dann eine Exklusiv-oder-Verknüpfung der beiden Klartexte, was in den meisten Fällen für eine erfolgreiche Aufbrechung des Chiffretext ausreicht.

Die Stromchiffren gelten als kleine kompakte Verschlüsselungsmethoden, die seit dem neuen Jahrtauschend mehr und mehr an Bedeutung gewinnen und vor allem beim Mobilfunk eingesetzt werden.
Innerhalb der Stromchiffrierung unterscheidet man außerdem noch zwischen synchronen und selbstsynchronisierenden Stromchiffren.
Bei einer selbst selbstsynchronisierende Stromchiffre hängt der Schlüsselstrom von vorhergehenden verschlüsselten Bits ab.
Eine synchrone Stromverschlüsselung generiert unabhängig vom Schlüsselstrom den Klartext oder Schlüsseltext.

3.5.2. Stromchiffre Verfahren

Stromchiffre haben zwei grundsätzliche Vorteile. Der eine Vorteil ist, dass der Keystream vorausberechnet und zwischengespeichert werden kann, was die Geschwindigkeit erhöht. Der zweite Vorteil ist, dass bei einem Bitfehler im Geheimtext nur ein Bit im Klartext defekt ist.
Der Aufwand für die Initialisierung ist recht hoch. Deshalb stellt sich nur bei längerem Klartext eine hohe Geschwindigkeit ein. Ein Angriff auf eine Stromchiffre basiert darauf, dass der Angreifer einen Teil des Keystream kennt.

3.5.2.1. RC4

Ein in der Vergangenheit sehr wertgeschätzte Stromchiffre hat den Namen RC4, der später auch als ARCFOUR bekannt wurde. Sie gehört zu einer Familie von Verfahren, die von Ron Rivest entwickelt wurden. RC4 wird unter anderem in Standards wie SSH 1, HTTPS und WEP/WPA eingesetzt und dient der Anwendung in Implementierungssoftware. Der Schlüssel ist vom Startwert abhängig und kann frei zwischen einem Bit und 2.048 Bit gewählt werden. Ist der Schlüssel kürzer als 2.048 Bit, dann wird er mehrfach hintereinander geschrieben.

Die Verschlüsselungsgeschwindigkeit ist bei Softwareimplementierung sehr hoch. Die Schnelligkeit und Einfachheit dieses Verfahren ist der Grund für seine hohe Favorisierung unter vielen Webbrowsern. Er galt in den offiziellen Plattformen als sehr sicher und war lange Zeit Konkurrenzlos, jedoch wurde diese Sicherheit von einigen Informatikern in den letzten Jahren geprüft und als mehrfach fehlerhaft bezeichnet. Hierbei wurde die Zufallsfolge des RC4 infrage gestellt und es konnte ausreichend Beweise geliefert werden, dass die Zufallsfolge des RC4 nicht ausreichend Sicherheit bietet.

3.5.2.2. A5

Eine weitere bedeutende Stromchiffre trägt den Namen “A5“. Bei dem A5 handelt es sich um das Verschlüsselungsverfahren, das weltweit von GSM-Mobilfunknetzt (Global System for Mobile Communications) angeboten wird, um die Übertragung zur nächsten Empfangsstation zu verschlüsseln. Ähnlich wie bei RC4 stand die Funktionsweise des A5 erstmal geheim dar. Informationen, wer die Entwickler waren, gab es zunächst auch keine. Im laufe der Zeit wurden Stück für Stück die Funktionsweise unter dem Namen „BrGoWA“ veröffentlicht.
Je mehr man sich in den letzten Jahren über die Funktionsweise Gedanken gemacht hat, desto bewusster wurde man, dass der A5 den Anforderungen der

modernen kryptographischen Verfahren nicht gerecht wird. Es kam sogar der Verdacht auf, dass die Entwickler absichtlich einen einfach knackbaren Algorithmus etablieren wollten, um das Abhören von Polizei und Geheimdienst einfacher zu machen.

3.5.3. Blockchiffren

Die Blockchiffre/Blockverschlüsselung ist eine der beiden symmetrischen Verschlüsselungsmöglichkeiten, Daten zu chiffrieren. Anders als bei der Stromverschlüsselung, werden bei der Blockverschlüsselung, die Daten eines Klartextes in feste Blöcke unterteilt und gemeinsam verschlüsselt.
Wenn der Klartext 40 Zeichen Lang ist, befinden sich jeweils exakt 10 Zeichen in einem Block.

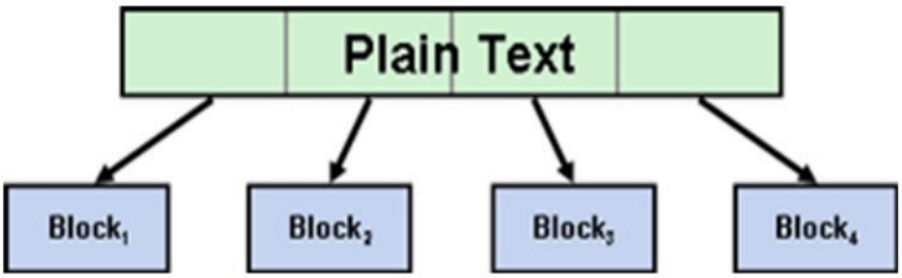

Abbildung 7: Prinzip der Blockverschlüsselung

Die Länge der chiffrierten Blöcke kann sowohl fest als auch variabel sein. Typische Werte für die Blockgrößen ist ein vielfaches von 64 Bit also 128, 192 oder 256 Bit. Ist eine Zeichenkette kürzer als z.B. 128 Bit, so wird sie mit Fülldaten (Nullen und Einsen) vervollständigt, diese Ausfüllung wird auch Padding genannt.

Wenn gleiche Blocke mit dem selben Schlüssel verschlüsselt werden, bietet das für einen Angreifer genug Angriffsfläche, um den kryptographischen Text zu entschlüsseln. Damit identische Nachrichten nicht einen identischen Verschlüsselungstext ergeben, kommt ein Initialisierungsvektor zum Einsatz, der aus einem Pseudozufallsgenerator entsteht. Der Initialisierungsvektor bezeichnet einen Block von Zufallsdaten, der in Modi einiger Blockchiffren verwendet wird. Man kombiniert das Ergebnis mit dem Text im ersten Block und dem Schlüssel. So ist garantiert, dass aus allen nachfolgenden Blöcken ein Chiffretext entsteht, der nicht identisch mit den vorangegangenen Blöcken ist.

3.5.4. Blockchiffre Verfahren

Die drei bedeutenden Verfahren bei der Blockchifferierung sind die Data Encryption Standard (DES), der International Data Encryption Algorithm (IDEA) und der Advanced Encryption Standard (AES), auf die ich im folgenden Eingehen möchte.

3.5.4.1. DES

Data Encryption Standard ist ein Blockverschlüsselung und zeichnet sich wie alle symmetrischen Verfahren dadurch aus, dass er für die Ver-und Entschlüsselung den selben Schlüssel verwendet.
Der DES unterlief mehrerer Weiterentwicklungen bis er schließlich von den amerikanischen Behörden für den Privaten Sektor zugelassen worden ist und vor der Weiterentwicklungen “Lucifer“ genannt wurde.
Der modifizierte Lucifer wurde 1975 von der NSA veröffentlicht.
Eine Wesentliche Modifizierung war die Reduzierung der Schlüssellänge auf 56 Bit.
1977 wurde dieser Algorithmus als Data Encryption Standard (DES) durch das National Bureau of Standards zum US-Verschlüsselungsstandart genormt.
Schon ab 1977 gab es vielfache Kritik an der zu kurzen Schlüssellänge.
Deutlich wurde diese Schwäche durch Angriffe, die den Schlüsselraum systematisch durchsuchen, z.B 1994 als ein DES-Schlüssel in 50 Tagen ermittelt wurde. 1998 wurde ein besonderer Computer vorgestellt, der einen DES –Schlüssel in 56 Stunden entschlüsseln konnte.
2001 gelang ein erfolgreicher Angriff innerhalb von 22 Stunden.
Der DES verschlüsselt einen 64-Bit Eingabeblock mir einem Schlüsse von 64-Bit, bei dem 56 Bit frei wählbar sind, die restlichen 8 Bit sind Paritätsbits. Damit besitzt der DES einen Schlüsselraum von 2^{56} unterschiedlichen Schlüsseln.
Der effektive Angriff besteht aus dem durchprobieren aller möglichen Schlüssel bis der richtige gefunden wird.

3.5.4.2. IDEA

IDEA ist ein ebenfalls eine symmetrisches Verschlüsselungsverfahren, das in den neunziger Jahren sehr populär war und ebenfalls mit Blockchiffren arbeitet.
Das Verschlüsselungsverfahren, das 1991 erstmals veröffentlicht wurde, erwies sich als erfolgreiche Alternative zum DEA.
Im Gegensatz zum DES bietet der IDEA mir seinen 128 Bit eine längere Schlüssellänge und die Blocklänge von IDEA beträgt, wie beim DES 64 Bit.
Eine Verschlüsselungsoperation besteht aus acht runden gefolgt von einer Ausgabetransformation . Um schnell in Software implementierbar zu sein werde die Verwendung von Permutation und Substitution verzichtet. Die eingesetzten Operation beschränkt sich auf XOR, Addition und Multiplikation.
Die 64-Bit Eingabewerte werden in vier 16-Bit Blöcke aufgeteilt die die Eingabe der ersten Runde bilden. In jeder Runde werden verschiedene Operationen durchgeführt deren Ergebnis von der nächsten Runde weiterverarbeitet werden.
Nach acht Runden gilt es noch eine einfache Ausgabetransformation.
Die Entwickler des IDEA haben aus verschiedenen mathematischen Gruppen, Operationen eingeführt und somit den Algorithmus sehr abwechslungsreich gemacht, was dazu führte, dass der IDEA erfolgreich patentiert wurde und damit der Zugang zum IDEA , nach dem patentieren durch erhöhte Kostenaufwand erschwert wurde.

3.5.4.3. AES

Der AES kann nicht mehr als sicher angesehen werden, wie mehrere erfolgreiche Angriffe gezeigt haben. Daher hat das US-amerikanische National Institut of Standards and Technology (NIST) angefangen 1997 ein einem öffentlichen Wettbewerb aufgerufen, dessen Sieger Advanced Encryption Standard festgelegt werden soll. Im Mai 2000 wurde die Analysen und öffentlichen Diskussionen abgeschlossen und schließlich am 2 Oktober 2000 der Sieger bekannt gegeben. Der belgische Algorithmus Rijndael wird neuer Standard.
Rijndael bietet ein sehr hohes Maß an Sicherheit, erst nach mehr als 10 Jahren nach seiner Standardisierung, wurde der erste theoretisch interessante, praktische aber nicht relevante Angriff gefunden.

Der AES ist eine Blockchiffre dessen Blocklänge unabhängig voneinander die Werte 128, 192, oder 256 Bit erhalten kann. Jeder Block wird zunächst in eine zweidimensionale Tabelle mit vier Zellen geschrieben dessen Zellen Byte groß sind. Die Anzahl der Spalten variiert somit je nach Blockgröße von 4 (128 Bit) bis 8 (256 Bit). Jeder Block wird nun nacheinander bestimmten Transformationen unterzogen, aber anstatt jeden Block einmal mit dem Schlüssel zu chiffrieren, wendet des AES verschiedene Teile des Schlüssels nacheinander auf den Klartextblock an. Innerhalb des AES besteht eine weitere Aufteilung in drei Varianten, welche sich jeweils auf die Schlüssellänge beziehen, AES-128, AES192 und AES-25. AES-192 und AES-256 sind in den USA aufgrund ihrer hohen Sicherheit für staatliche Dokumente mit höchster Geheimhaltungsstufe zugelassen.

3.6. Asymmetrische Verschlüsselungsverfahren

Wie wir bereits behandelt haben wird bei der symmetrischen Kryptographie ein Schlüssel für das Ver – und Entschlüsseln verwendet, anders ist es bei der asymmetrischen Kryptographie.
Das besondere an der asymmetrischen Kryptographie ist, dass man ein Schlüsselpaar verwenden muss. Ein Schlüsselpaar besteht aus einem öffentlichen Schlüssel (Public Key) und einem privaten Schlüssel (Privat Key).
Man bezeichnet dieses Verfahren auch als Publik-Key-Verfahren.
Der Sender chiffriert seine Botschaft zunächst mit seinem Privat Key und dann mit dem Public Key des Empfängers.
Nach erhalten der Botschaft dechiffriert der Empfänger die Nachricht zunächst mit seinem Privat Key und dann mit Public Key des Senders. Dieser aller letzte Schritt führt jedoch nur dann ans Ziel, wenn die Nachricht von dem bezeichnetem Sender kam, da andernfalls der verwendete öffentliche Schlüssel nicht passend ist.

Die Einwegfunktion spielt bei dem asymmetrischen Kryptographie eine wichtige Rolle. Sie wird durch einige komplexe mathematische Operatoren wie z.B. Modulo oder Logarithmen herbeigerufen, deren Hintransformation verständlich, während die Rücktransformation nicht nachvollziehbar ist.
Mit Hintransformation sei z.B gemeint.: $66 * 92 = 6072$.
Es ist leicht begreiflich wie der Rechenweg hin zum Ergebnis 6072 führt, wenn wir jedoch das gleiche Beispiel Rücktransformieren und uns die Frage was ergibt den 6072, erhalten wir sehr viele Möglichkeiten, die zu dem selben Ergebnis führen. Dieses Ziel haben die Einwegfunktionen bei dem Schlüsselauswahl.

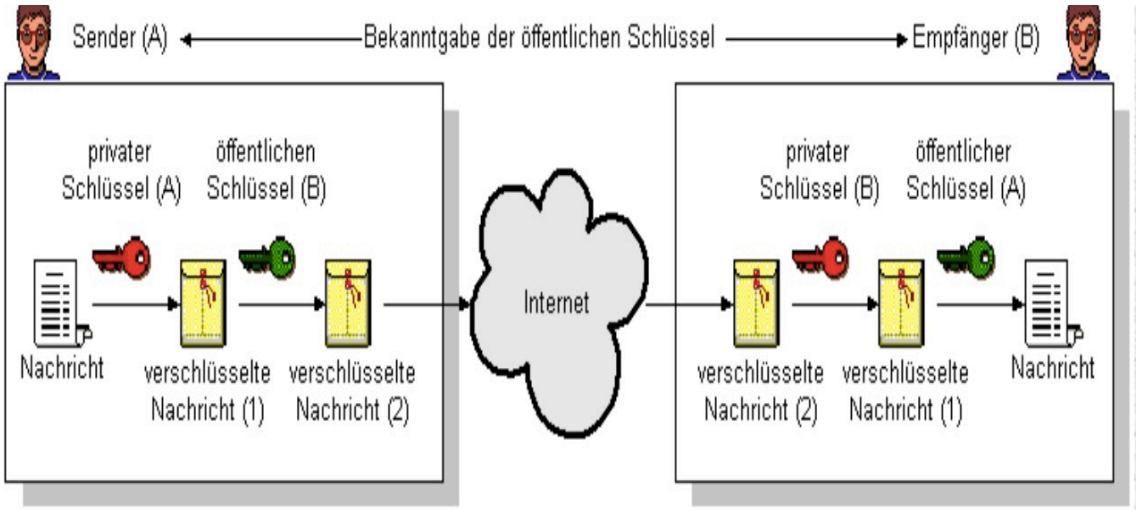

Abbildung 8: Asymmetrisches Verschlüsselungsverfahren

Der Vorteil der asymmetrischen Verfahren lieg darin, dass der Angreifer auch mit dem Erhalt unseres öffentlichen Schlüssels nicht auf den Chiffretext schließen kann. Daher kann der öffentliche Schlüssel auch über unsichere Kanäle ausgetauscht werden. Aber was der Angreifer definitiv erhält sind sogenannte Metadaten, diese geben Ausschluss darüber, wann , welche Personen miteinander kommuniziert haben. Diese Metadaten können ebenfalls eine Menge von einem ausdrücken und teilweise den Chiffretext erahnen.

3.6.1. Schlüsselaustauschproblem

Die gesamten symmetrischen Verfahren basieren auf einem vorab beidseitig vereinbarten Kommunikationsschlüssel. Im Normalgebrauch (z.B. Internet) ist dies natürlich nicht ganz einfach umzusetzen, denn man kann zwar den sichersten Algorithmus benutzen, dem aber nichts bringt, wenn man die Schlüssel über einen ungesicherten Kanal überträgt. Zudem maximiert sich die Anzahl der Schlüssel, umso mehr Teilnehmer miteinander in Kommunikation stehen.
Demnach muss ein Schlüsselaustauch so stattfinden, dass nur die Kommunizierenden einen Schlüssel erhalten.

3.6.1.1. Diffie-Hellman-Merkle-Schlüsselaustausch

Der Diffie- Helman-Schlüsselaustausch oder Diffie-Hellman-Merkle-Schlüsselaustausch ist ein Schlüsselaustauschprotokoll. Dieses Verfahren wurde im Jahre 1976 von Whitfield Diffie und Martin Hellman veröffentlicht.
Das Verfahren funktioniert wie folgt:
Die beiden Kommunikationspanter Alice und Bob wollen über einen unsicheren Kanal wie z.B. eine Kabel-oder Funkverbindung, mit Hilfe eines symmetrischen Kryptosystems miteinander kommunizieren. Dafür benötigen sie zunächst einmal einen geheimen gemeinsamen Schlüssel. Mithilfe des DHM-Kommunikationsprotokolls kann dieser geheime Schlüssel berechnet werden, ohne dass Dritte davon erfahren. Wenn N die Anzahl der Schlüssel ist brauchte man für 20 Kommunizierende 190 Schlüssel ($(\frac{N}{2}) = \frac{N(N-1)}{2} = \frac{20(20-1)}{2} = 190$).

1. Alice und Bob einigen sich öffentlich auf eine große Primzahl "P" und eine natürliche Zahl „G".
2. Sowohl Alice als auch Bob wählen nun eine große zufällige Zahl a,b (meist 100 Stellen nach dem Komma), welche jeweils geheim zu haltend sind (privater Schlüssel). Zu beachten: a und b werden nicht übertragen bleiben also bei dem jeweiligen Kommunikationspanter.
3. Alice sendet an Bob $\mathbf{B = G_b \bmod N}$
4. Bob sendet an Alice $\mathbf{A = G_a \bmod N}$
5. Alice berechnet nun den Schlüssel $\mathbf{K = A_b \bmod N}$
6. Bob berechnet $\mathbf{K_0 = b_a \bmod N} * \mathbf{K = K_0 = G_{ab} \bmod N}$

Ein Angreifer, kann aus der abgehörten Kommunikation nicht ohne Weiteres an den Schlüssel kommen. Um den Schlüssel zu berechnen, benötigt man beide zufällig ausgewählte Zahlen. Dieser Algorithmus war der erste Public-Key Algorithmus, der patentiert wurde.

3.6.1.2. RSA

Das RSA-Verfahren ist nach seinen Urhebern Rivest, Shamir und Adleman benannt. Es handelt sich bei dem RSA nicht nur um eines der ältesten, sondern auch wichtigste asymmetrische Verschlüsselungsverfahren.
Im Vergleich Diffie-Hellman-Schlüsselaustausch ist der RSA vielseitiger.
Es kann nicht nur zum Schlüsselaustausch, sondern auch zur asymmetrischen Verschlüsselung verwendet werden. Er beschreibt somit einen Kryptosystem anstatt nur ein Schlüsselaustauschverfahren.
Theoretisch kann ein Angreifer das RSA-Verfahren durch eine vollständige Schlüsselkombinationssuche brechen.
Praktisch ist das jedoch schon bei einer bescheidenen Schlüssellänge von 256 Bit ein mehr als aussichtsloses Unterfangen.
Nichtsdestotrotz kann das RSA-Verfahren anfällig sein, gegenüber falschen Implementierungen.
Eine zu kurze Schlüssellänge, falsch gewählte Parameter und andere Fehler können schnell zu erheblichen Sicherheitslücken führen. Andererseits ist RSA nach wie vor ein sehr gutes Verfahren, wenn die genannten Fehler vermieden werden.

3.6.1.3. Digitale Signaturen

Bei einer digitalen Signatur handelt es sich um eine elektronische Signatur, mit deren Hilfe der Absender einer Datei oder der Unterzeichner eines Dokuments seine Identität nachweisen kann. Unter Umständen lässt sich damit auch sicherstellen, dass der ursprüngliche Inhalt eines versendeten Dokuments oder einer Nachricht nicht verändert wurde. Digitale Signaturen sind einfach zu übertragen, lassen sich nicht durch Dritte imitieren und werden mit einem automatischen Zeitstempel versehen. Da der Empfang der originalen signierten Nachricht nachgewiesen werden kann, ist es dem Absender später zudem nicht möglich, den Versand der Nachricht abzustreiten.

3.7. Hybrid Verfahren

Da die bisherige Implementierung von asymmetrischen Systemen immer noch sehr langsam gegenüber symmetrischen Systemen ist und dazu kommt, dass sie ungeeignet für große Datenmengen ist, ist man auf die Idee gekommen, die Vorteile der beiden Systeme zu kombinieren. Hybride Verschlüsselung ist ein Verfahren, das symmetrische und asymmetrische Verschlüsselung kombiniert. Der Öffentliche symmetrische Schlüssel wird zunächst frei gewählt, dieser wird auch Sitzungsschlüssel genannt, damit die großen Datenmengen verschlüsselt werden. Nach dem Erhalt des chiffrierten symmetrischen Schlüssels, entschlüsselt der Empfänger, mit Hilfe seines privaten Schlüssels. Mit dem entschlüsselten symmetrischen Schlüssel kann er auch die Nachricht entschlüsseln.
Durch das Kombinieren dieser beiden Verfahren, löst man die Nachteile, die beide mit sich bringen. Bei den symmetrischen Verfahren hat man das Problem mit dem sicheren Austausch der Sitzungsschlüssel, wohingegen asymmetrische Verfahren das Problem mit dem Schlüsselaustausch lösen. Die Vorteile der beiden Verfahren werden ebenfalls miteinander vereinigt wie z.B. die geringe Schlüsselmenge und erhöhte Sicherheit bei asymmetrischen Verfahren. Dies wird z.B. bei der Verschlüsselung von E-Mails und der Sicherheitsprotokolle im Internet eingesetzt.

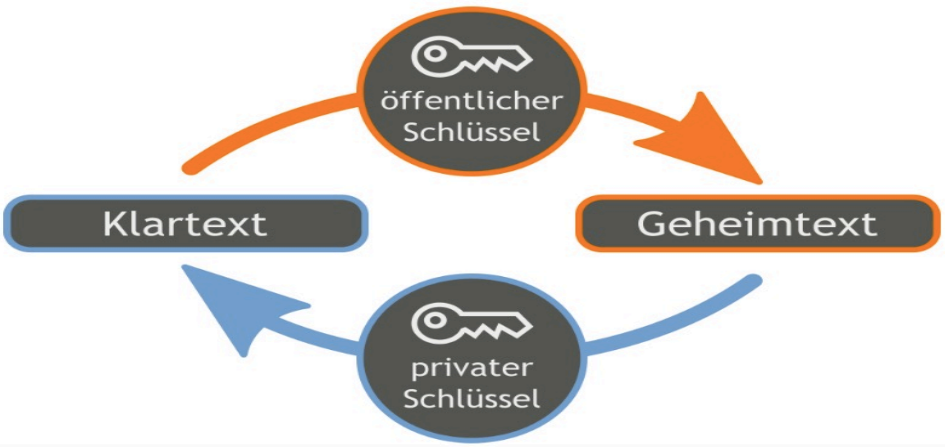

Abbildung 9: Hybrid Verfahren

4. Kryptoanalyse

Wie wir bereits in der Einleitung behandelt haben, wird Kryptologie in zwei Bereiche eingeteilt, nämlich in Kryptographie und Kryptoanalyse.
Die Kryptographie ist die Wissenschaft, Algorithmen zur Verschlüsselung zu entwickeln und diese in gegebenen Systemen zu implementieren. Die Kryptoanalyse ist die Wissenschaft Schlüssel ohne deren Befugnis aufzubrechen und beschäftigt sich damit kryptographische Verfahren auf Schwachstellen zu untersuchen.
Die Erkenntnisse aus den Untersuchengen können klare Handlungsbedarf in den jeweiligen Verfahren aufdecken und Informationen übe deren Schutzgrad bekannt geben. Ein interessanter Unterpunkt der Kyptoanalyse ist die die Steganalyse. Diese ist der Gegenpol der Steganographie.
Hierbei handelt es sich darum, zunächst nur mit der Annahmen zu rechnen, dass sich in einem Trägermedium eine versteckte Information befindet. Erst wenn diese Annahme erhärtet wird versucht man die eigentlichen Informationen zu extrahieren.

4.1. Kerckhoffs Prinzip

Im Jahr 1883 wurde Kryptoanalyse durch die Aussage eines Mannes revolutioniert. Auguste Kerckhoffs formulierter den Grundsatz, der die modernen Kryptoanalyse bis heute beeinflusst. Bei der Kryptoanalyse wird üblicherweise das Kerkhoffs Prinzip angenommen. Dieser besagt:

„Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen. Die Sicherheit gründet sich nur auf die Geheimhaltung des Schlüssels.“.

Mit anderen Worten, unterschätze niemals den Kryptoanalytiker.
Gehe insbesondere immer von der Annahme aus, dass dem Gegner das angewandte System bekannt ist. Dies ist eine grundsätzliche Warnung an den Entwickler eines Kryptosystems. Er darf auf keinen Fall so blauäugig sein anzunehmen, der Angreifer hätte keine Möglichkeit, Kenntnis des Algorithmus zu erlangen.

4.2. Kryptosystem

Um das Kerkhoffs Prinzip gut zu verstehen, ist es sinnvoll kurz auf Kryptosysteme einzugehen.
Bei einem Kryptosystem handelt es sich um eine Zusammenfassung ähnlicher Verschlüsselungsmethoden (z.B A – und Symmetrische-Verfahren)
Gute Kryptosysteme haben insbesondere einen viel größeren Schlüsselraum, allerdings macht dessen Größe allein noch nicht die Qualität aus.
Ein Schwachpunkt aller Kryptosysteme ist die Möglichkeit, von Regelmäßigkeiten des Chiffretextes auf Regelmäßigkeiten des Klartextes Rückschlüsse ziehen zu können. Wenn ein Angreifer weiß, welches Kryptosystem verwendet wurde, ist es natürlich einfacher für ihn, als wenn er dies nicht weiß.

4.3. Ziele der Kryptoanalyse

So wie die Kryptographie verfolgt auch die Kryptoanalyse bestimmte Ziele, deren erreichen, mit der Aushebelung der kryptographischen Ziele gleichzusetzen wäre. Primär verfolgen die kryptoanalytischen Verfahren das Ziel, die geheimen Schlüssel zu ermitteln und damit Kenntnis über den Klartext zu erhalten.
Für das Aufbrechen der Verschlüsselungsmethoden sind weiterhin folgende Angriffsziele relevant:

- Entschlüsselung, d. h. die Ermittlung des Klartextes.

- Der Angreifer möchte, einen Chiffretext so zu verändern, dass der zugehörige neue Klartext, mit dem ursprünglichen Klartext in einer bestimmten Relation steht, die dem Angreifer nicht nur bekannt ist, sondern auch zu gute kommt.

- Wenn der Angreifer den Schlüssel nicht brechen kann, verfolgt er das Ziel einen Chiffretext zu erzeugen, ohne den dazugehörigen Klartext zu kennen.

4.4. Angriffe

Zur Einstufung des Erfolgs eines Angriffes unterscheidet der Kryptoanalytiker zwischen folgenden Punkten, die mit sinkendem Schweregrad wie folgt definiert sind

- vollständiges Aufbrechen: Ein Kryptoanalytiker findet den Schlüssel, d.h, dass jede Nachricht, die mit verschlüsselt wird, entschlüsselt werden kann.

- Globale Deduktion: Ein Kryptoanalytiker findet ohne Kenntnis auf dem Schlüssels einen alternativen Algorithmus, der identisch zum knackenden Algorithmus ist.

- Lokale Deduktion: Ein Kryptoanalytiker findet den Klartext zum abgefangenen Chiffretext.

- Informationsdeduktion **:** Der Kryptoanalytiker stößt auf oder findet Informationen über den Schlüssel aus dem Informationen vom Klartext gewonnen werden können.

Auch wenn viele Möglichkeiten eines Angriffs nicht vorhersehbar sind, so soll folgende Aufstellung eine Vorstellung schaffen, welchen unterschiedlichen Angriffsszenarien ein Kryptosystem im praktischen Einsatz ausgesetzt sein kann.

4.4.1 **Ciphertext-only-Attacke** (Angriff bei bekanntem Chiffretext):

Der Angreifer fängt den Chiffretext ab und versucht, allein aus ihrer Kenntnis Rückschlüsse auf die zugehörigen Klartexte oder auf die benutzten Schlüssel zu ziehen. Dies ist eine außerordentlich realistische Annahme, da es in der Regel einfach ist, sich Stücke des Geheimtext zu verschaffen.

4.4.2 **Known-plaintext-Attacke** (Angriff bei bekanntem Klartext):

Der Angreifer ist im Besitz von einigen zusammengehörigen Klartext-Chiffretext-Paaren. Hierdurch wird erfahrungsgemäß die Entschlüsselung weiterer Chiffretexte wesentlich erleichtert. Diese Angriffsszenario ist realistischer als sie auf den ersten Blick erscheint. Denn oft weiß der Angreifer, worum es geht, und kann also zumindest einige Worte erahnen, wie z.B. die Begrüßungsfloskel.

4.4.3 **Chosen-plaintext-Attacke** (Angriff bei frei wählbarem Klartext):

Der Angreifer hat Zugriff zur Verschlüsselungsmaschinerie und kann einen Klartext wählen und den zugehörigen Chiffretext generieren.
Wenn der Kryptoanalytiker Zugang zum Verschlüsselungsalgorithmus hat, so kann er, um den Schlüssel zu erschließen, auch selbstgewählte Stücke Klartext verschlüsseln und versuchen, aus dem erhaltenen Geheimtext Rückschlüsse auf die Struktur des Schlüssels zu ziehen.

4.4.4 **Chosen-ciphertext-Attacke** (Angriff bei frei wählbarem Chiffretext):

Der Angreifer hat temporär Zugriff zur Entschlüsselungsmaschinerie und kann einen Chiffretext wählen und den zugehörigen Klartext generieren. Bei dieser Art von Angriff ist dies die gefährlichste, weil der Kryptoanalist nicht nur zusammengehörende Klartext- und Chiffretextsegmente kennt, sondern kann diese auch frei nach Lust und Laune selbständig generieren.

4.5 Techniken und Methoden

4.5.1 Häufigkeitsanalyse

Diese Methode ist mit Abstand die älteste Technik zur Aufklärung von verschlüsselten Texten und hat seine Anfänge ca. 600 Jahre nach Christus, als die ersten muslimischen Theologen der Schulen Basra und Kufa den Koran auf seine Linguistik analysierten und zusammenhänge zwischen Häufigkeit der Wörter aus dem Koran mit der Reihenfolge der Offenbarung feststellten.
Jeder Buchstabe hat eine bestimmte Wahrscheinlichkeit in einem Text aufzutauchen. Im deutschen sind das die Buchstaben „e“ mit über 17 % und „n“ mit ca. 10 % Wahrscheinlichkeit. Jedes Klartextzeichen bekommt ein oder mehrere Geheimtextzeichen zugewiesen. Die vorkommenden Geheimtextzeichen werden zum Knacken der Chiffre nun einfach gezählt und mit der durchschnittlichen Häufigkeit von Klartextbuchstaben in der entsprechenden Landessprache verglichen.

4.5.2 Wörterbuchattacke

Mit einer Wörterbuchattacke meint man die Technik in der Kryptoanalyse, ein unbekannten Schlüssels mit Hilfe einer Passwörterliste oder Wörterbuch zu ermitteln. Man verwendet diese Methode, wenn man davon ausgehen kann, dass das Passwort aus einer sinnvollen Zeichenkombination besteht.
Erfolgversprechend ist dieses Verfahren nur, wenn möglichst viele Passwörter schnell hintereinander ausprobiert werden können.

4.5.3 Lineare Kryptoanalyse

1993 wurde diese Methode von einem Mann namens „Mitsuru Matsui“ veröffentlicht. Das Verfahren basiert auf ein lineares Annäherungsverfahren, an den die Ermittlung des richtigen Schlüssels mit Wahrscheinlichkeitsberechnung und Statistiken Erfolgt. Das Verfahren basiert auf dem Versuch, die Nichtlinearität der S-Boxen durch lineare Ausdrücke anzunähern. In der Kryptographie bezeichnet eine S-Box (auch Substitution-Box genannt), eine Grundkomponente symmetrischer Kyptosysteme. S-Boxen werden in Blockverschlüsselungen wie beispielsweise DES eingesetzt, um die Beziehung zwischen Klar- und Geheimtext zu verwischen.
Weiterhin wird bei der linearen Kyptoanalyse mit Wahrscheinlichkeiten gearbeitet, dass die im Verfahren bestimmte Bedingungen gelten, die in Form von mathematischen Gleichung erfolgen. Diese Methode ist heutzutage so erfolgreich, das sie am häufigsten für Angriffe gegen Blockchiffren verwendet werden.
Andere Varianten der linearen Kryptoanalyse wurden sowohl für Block- als auch für Stromchiffren entwickelt. Daher wird bei neu entworfenen Algorithmen normalerweise ihre Sicherheit gegen die lineare Kryptoanalyse geprüft.
Die lineare Kryptoanalyse zielt auf den Klartext und versucht einfache, lineare Zusammenhänge zwischen Bits des Klartextes und des Geheimtextes zu ermitteln, um daraus Informationen über den Schlüssel zu erhalten.

4.5.5 Differentiellen Kryptoanalyse

Die differentielle Kryptoanalyse wurde 1991 von Eli Biham und Adi Shamir entwickelt. Das primäre Ziel war es den DES zu brechen.
Dieser Angriffsversuch schlug fehl, da die differentielle Kyptoanalyse, der NSA bei der Entwicklung von DES bereits bekannt war.
Die differentiellen Kryptoanalyse arbeitet mit Chosen-Plaintext-Paaren.
Also der Angreifer hat Zugriff zur Verschlüsselungsalgorithmus und kann einen Klartext wählen und den zugehörigen Chiffretext generieren.
Bei der differentiellen Kryptoanalyse werden die Klartextpaare unterschiedlich verschlüsselt, um aus den unterschiedlichen Chiffrate den geheimen Schlüssel des symmetrischen Kryptosystems abzuleiten.
Dabei wird darauf hingearbeitet, dass mehrere ausgewählte Paare, einer gewünschten Charakteristika besitzen und dadurch ein hohe Wahrscheinlichkeit haben , als Schlüssel zu dienen. Die differentielle Kryptoanalyse beruht darauf, zu beobachten wie sich bestimmte Änderungen in den Klartexten auf die Unterschiede in den Chiffretexten auswirken. Anhand dieser Unterschiede kann Rückschlüsse Verschlüsselungsalgorithmus gezogen.

4.5.6 Man-in-the-middle-Angriff

Der Angreifer befindet sich zwischen zwei Kommunikationspartnern und kann alle Nachrichten mithören, verändern oder neue Nachrichten einfügen.
Bei diesem Angriff täuscht ein böswilliger Dritter "in der Leitung" zwei Kommunikationspartner, indem er ihnen jeweils die Identität des anderen vorspiegelt. Typischerweise geschieht das, um eine an sich sichere Verschlüsselung auszuhebeln. Voraussetzung dafür ist, dass er eine Verbindungsanfrage auf sich umleiten kann und die Kommunikationspartner die Identität des Gegenübers nicht überprüfen. Über Man-in-the-middle-Angriffe lassen sich beispielsweise gesicherte SSL-Verbindungen zum Online-Banking belauschen.

4.5.7 Angriffe durch Gitterbasenreduktion

Viele kryptographische Verfahren lassen sich angreifen, indem man einen kurzen Vektor in einem bestimmten Gitter ermittelt. Diese Angriffsmethode wird bei Kryptoverfahren, wird z. B. bei dem Diffie-Hellman-Merkle Verfahren eingesetzt, kann aber auch in Kombination mit anderen asymmetrischen Kryptoverfahren, wie z. B. RSA angewendet werden.

4.5.8 Brute-Force-Angriff

Ein Brute-Force-Angriff stellt einen gewaltsamen Angriff auf einen kryptographischen Algorithmus dar. Das Verfahren probiert systematisch alle möglichen Kombinationen durch, um einen Schlüssel zu knacken. Dazu werden alle Ziffern, Buchstaben und Leerzeichen bis zu einer maximal Wortlänge ausprobiert. Brute-Force-Angriffe können auf verschlüsselte Passwörter, Dateien, Nachrichten und Informationen angesetzt werden.
Daher ist es ratsam stets lange Passwörter zu verwenden, die so viele Kombinationsmöglichkeiten bieten, dass die Brute-Force-Angriff zu lange

brauchen würde, um alle auszutesten. Trotzdem wird der Brute-Force angriff, als sehr effektiv angesehen.

4.5.9 Seitenkanalattacke

Der Angreifer versucht, außer dem Klartext, Chiffretext oder dem Schlüssel zunächst auch andere Daten zu erfassen und daraus Informationen über den verwendeten Algorithmus und Schlüssel zu gewinnen. Hierfür kommen zum Beispiel in Frage: die Dauer der Verschlüsselung, der zeitliche Verlauf des Stromverbrauchs eines Chips, Berechnungsfehler aufgrund extremer Umgebungsbedingungen oder die Abstrahlung elektromagnetischer Wellen.

4.6 Fazit

Durch die zunehmende Digitalisierung und den stetig steigenden Fortschritt steigt auch das starke Verlangen nach mehr Sicherheit von Computersystemen.
Infolge der steigenden Rechnerleistung steigt auch die maximale Schlüsselanzahl, um so Angriffen wie z.B. einen Brute Force Angriff, wo alle Schüssel durchprobiert werden, vorzubeugen.
Dennoch ist es zu erwähnen, das durch den fortschreitenden Know-How, es nur eine Frage der Zeit ist bis die aktuell sichere Verschlüsselungsverfahren in immer kürzer Zeit geknackt werden können.
Bestes Beispiel hierfür war die Entschlüsselung eines DES Algorithmus mit 256 Schlüsseln, im Jahre 1998. Dieser wurde in 56 Stunden geknackt und ein Jahr später brauchte man für den selben Angriff nur noch 22 Stunden, was zur Bekanntgabe eines neuen Standards im Oktober 2000 führte.
Anstelle den Fokus darauf zu legen immer mehr und sichere Algorithmen der Verschlüsselung zu entwickeln, um sich vor Angriffen zu schützen, finde ich es ratsamer das gesamte System in dem wir Leben aufzuklären und zu verändern.
Wenn unsere Mitmenschen und wir nicht langsam begreifen was um ums herum geschieht, wird das System unseren Kindern und Kindeskindern es fast unmöglich machen sich ohne Ängste vor böswillige Abhörer auszutauschen.
Wie sollen wir uns über spezielle Thematiken eine eigene Meinung bilden, wenn wir uns untereinander nicht frei austauschen können ?
Ein wichtiger Aspekt der Freiheit ist, das man selbst entscheiden kann, wem man erlaubt in die eigene Privatsphäre einzudringen.
Die Meinungen über solch eine Art von Überwachung gehen stark auseinander, jedoch ist eines klar, im Zuge der technischen Möglichkeiten wird es nicht einfacher sich vor solch einer Überwachung zu schützen.