

Krypto- logie

GFS im Fach Mathematik

Nicolas Bellm

12. November - 16. November 2005

Der Inhalt dieses Dokuments steht unter der GNU-Lizenz für freie Dokumentation
<http://www.gnu.org/copyleft/fdl.html>

Inhaltsverzeichnis

- 1 Einleitung** **3**

- 2 Die klassische Kryptologie** **4**
 - 2.1 Skytale 4
 - 2.2 Monoalphabetische Verfahren 4
 - 2.2.1 Cäsar-Chiffre 4
 - 2.2.2 zufällige Alphabete 5
 - 2.2.3 langes Schlüsselwort 5
 - 2.2.4 Atbash 6
 - 2.3 Polyalphabetische Verfahren 6
 - 2.3.1 Vigenère 6
 - 2.3.2 One-Time-Pad 6
 - 2.4 Playfair 7

- 3 Moderne Kryptologie** **9**
 - 3.1 Symmetrische Kryptologie 9
 - 3.2 Assymetrische Kryptologie 10
 - 3.2.1 Rivest-Shamir-Adleman 10

- 4 Ausblick** **12**

1 Einleitung

Die Kryptologie (griech. *kryptós* = verborgen + *lógos* = Wissenschaft) ist die Wissenschaft der Verschlüsselung und der Entschlüsselung von Informationen.

Die Kryptologie läßt sich unterteilen in:

- Verschlüsselung von Informationen (Kryptographie)
- Verstecken von Informationen (Steganographie)
- Entschlüsselung von Informationen (Kryptoanalyse)

In meiner GFS werde ich vor allem auf den ersten Teilbereich der Kryptologie eingehen, der Kryptographie. Auf die Kryptoanalyse werde ich nur teilweise und auf die Steganographie werde ich in meiner GFS nicht zu sprechen kommen, da es sich dabei nur um ein Randgebiet der Kryptologie handelt.

2 Die klassische Kryptologie

2.1 Skytale

Dabei handelt es sich um die älteste bekannte Verschlüsselungsverfahren. Sie wurde von den Spartanern ca. 500 v. Chr. verwendet. Zur Verschlüsselung dient ein Holzstab mit einem bestimmten Durchmesser.

Der Absender wickelt um die Skytale einen Papyrusstreifen o.ä. Die Nachricht wird dann längs des Stabes auf den Papyrusstreifen geschrieben. Der Papyrusstreifen wird dann wieder von der Skytale abgewickelt und ohne die Skytale dann verschickt. Die Nachricht kann der Empfänger nur mit einem Holzstab mit dem gleichen Durchmesser entschlüsseln. Somit ist der Durchmesser der Skytale ist der geheime Schlüssel dieses Verfahrens.

Bei der Skytale muß der Papyrusstreifen rundherum beschrieben werden, sonst ist es ein Leichtes, den Durchmesser des Stabes herauszufinden. Die Skytale gehört zu den sog. *Transpositionsverfahren*, d.h. die Zeichen des Klartextes werden einfach umsortiert und nicht verändert.

2.2 Monoalphabetische Verfahren

2.2.1 Cäsar-Chiffre

Die Cäsar-Chiffre ist das einfachste Verfahren zum Verschlüsseln von Nachrichten. Dieses Verfahren ist benannt nach dem römischen Feldherrn Julius Cäsar (100-44 v.Chr.).

Bei diesem Verschlüsselungsverfahren handelt es sich um eine *monoalphabetische Substitution*, d.h. jeder Klartextbuchstabe wird einem eindeutigen Geheimtextbuchstaben zugeordnet. Die Zuordnung ist aber nicht willkürlich, sondern sie basiert auf der zyklischen Rotation des Alphabets um eine gewisse Anzahl von Zeichen. Der Schlüssel dabei ist die Anzahl, um wieviel das Alphabet verschoben wurde (z.B. um vier Zeichen).

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

Zur Verschlüsselung wird für jeden Buchstaben der darunterstehende Geheimtextbuchstaben eingesetzt (aus GEHEIM wird KILIMQ). Bei der Verschlüsselung geht man umgekehrt vor: Für jeden Geheimtextbuchstabe wird der darüberstehende Klartextbuchstabe verwendet (aus

KILIMQ wird wieder GEHEIM).

Mathematisch betrachtet handelt es sich hierbei um eine Addition im Zahlenraum von 0 bis 25, wenn man den Buchstaben von A bis Z die Zahlen von 0 bis 25 zuordnet Für Geheimtextbuchstabe c , Klartextbuchstabe m und für Schlüssel k gilt: $c \equiv m + k \pmod{26}$.

Diese Verfahren ist aber ziemlich einfach zu knacken: Da jeder Buchstabe mit dem gleichen Chiffrebuchstaben ersetzt wird, ist die Häufigkeitsverteilung der Buchstaben im Chiffre genauso wie die Häufigkeitsverteilung im Klartext. Es bereitet also keine Schwierigkeiten, jedem Geheimbuchstaben seinem Klartextbuchstaben zuzuordnen. Und wer das nicht schafft, der kann auch alle 26 Möglichkeiten durchprobieren. Diese Verfahren nennt man *Brute Force* (engl. rohe Gewalt).

Ein Sonderfall der Cäsar-Chiffre ist *ROT13* (Abkürzung von *rotiere um 13 Buchstaben*). Als Schlüssel wird 13 bzw. N verwendet. Da das Alphabet 26 Buchstaben hat, kann mit dem gleichen Algorithmus ver- und entschlüsselt werden. Diese Verfahren wird z.T. heute noch verwendet, für Texte, die nicht jeder sofort lesen soll, z.B. für Rätsellösungen.

2.2.2 zufällige Alphabete

Es gibt auch die Möglichkeit als Geheimtextalphabet ein völlig zufällig erstelltes Alphabet zu verwenden.

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

Aus GEHEIM wird RWAWSO. Aber auch dieses Verfahren läßt sich mithilfe einer Häufigkeitsanalyse recht einfach knacken.

2.2.3 langes Schlüsselwort

Eine weitere Möglichkeit ist es, ein langes Schlüsselwort (z.B. Schmetterling) zu nehmen und den Rest Alphabetisch zu ergänzen.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U ...
S	C	H	M	E	T	R	L	I	N	G	A	B	D	F	H	J	K	O	P	Q ...

Sinnvoll ist es, ein Wort zu benutzen, das mit Z beginnt, sonst werden die letzten Buchstaben des Alphabets auf sich selbst abgebildet (z.B. Zugbegleiter).

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

2.2.4 Atbash

Diese Verfahren wurde um 600 v.Chr. in Palästina angewandt und beruht auf der Umdrehung des Alphabets.

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

2.3 Polyalphabetische Verfahren

2.3.1 Vigenère

Die Vigenère-Chiffre, die nach dem französischen Diplomaten Blaise de Vigenère (1523-1596) benannt ist, funktioniert ähnlich wie die Cäsar-Chiffre, nur mit dem Unterschied, daß nicht jeder Klartextbuchstabe mit dem gleichen Alphabet verschlüsselt wird.

Um einen Text zu verschlüsseln, benutzt man ein Schlüsselwort z.B. MATHE und hängt ihn immer wieder hintereinander. Dann addiert man die Buchstaben des Klartextes und die Buchstaben des Schlüsselwortes und erhält somit den Geheimtext. Bei der Entschlüsselung subtrahiert man das Schlüsselwort vom Geheimtext.

Klartext:	P	O	L	Y	N	O	M	D	I	V	I	S	I	O	N
Schlüssel:	M	A	T	H	E	M	A	T	H	E	M	A	T	H	E
Geheimtext:	B	O	E	F	R	A	M	W	P	Z	U	S	B	V	R

Ähnlich wie bei Cäsar gilt auch hier für Geheimtextbuchstabe c_i , Klartextbuchstabe m_i , Schlüssel k_i : $c_i \equiv m_i + k_i \pmod{26}$.

Auch dieses Verfahren läßt sich recht einfach knacken. Sobald der Angreifer die Schlüssellänge herausgefunden hat, kann er für jeden ersten, zweiten, dritten, ... Buchstaben eine Häufigkeitsanalyse erstellen.

Um die Schlüssellänge zu bestimmen hilft der vom preußischen Infanteriemajor Friedrich W. Kasiski (1805-1881) entwickelte Kasiski-Test weiter. Dieser Test basiert auf der Beobachtung, daß gleiche Buchstabenfolgen um ein Vielfaches der Schlüssellänge auseinanderliegen. Beim Kasiski-Test sucht man gezielt nach solchen immer wiederkehrenden Buchstabenfolgen. Der größte gemeinsame Teiler der gefundenen Abstände ist dann die vermutete Schlüssellänge.

2.3.2 One-Time-Pad

Dieses Verfahren funktioniert genauso wie die Vigenère-Chiffre, aber der Schlüssel ist genauso lange wie die Nachricht selbst.

Der Name One-Time-Pad kommt aus dem Englischen und bedeutet Einmal-Block. Bei die-

sem Verfahren hat der Sender und Empfänger den gleichen Block mit völlig zufällig erzeugten Schlüsseln und bei jeder neuen zu verschlüsselnden Nachricht wird eine neue Seite des Blockes verwendet. Nachdem der Empfänger die Nachricht erhalten haben, wurden die Seiten des Blockes vernichtet. Der One-Time-Pad darf nur einmal verwendet werden, weil sonst die Verschlüsselung recht einfach wäre.

Der Vorteil dieses Verfahren ist, daß es perfekt sicher ist, es gibt also keine Möglichkeit, die Verschlüsselung zu knacken. Aber der Nachteil dieses Verfahren ist, daß der Schlüssel erst auf einem sicheren Kanal ausgetauscht werden muß.

2.4 Playfair

Dieses Verfahren wurde 1854 vom Physiker Charles Wheatstone (1802-1875). Das Verfahren wurde nach seinem Freund Lyon Playfair benannt, der es dem britischen Militär zur Benutzung empfahl.

Der Algorithmus basiert nicht auf der Verschlüsselung von Einzelbuchstaben, sondern auf der Verschlüsselung von Buchstabengruppen zu je zwei Buchstaben. Um damit einen Text zu verschlüsseln, erzeugt man eine 5x5-Matrix in die der Schlüssel (z.B. PHYSIK) eingetragen wird. Danach wird die Matrix mit den restlichen Buchstaben des Alphabets (ohne J) eingetragen.

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

Nun muß der Klartext entsprechend vorbereitet werden. Alle Leerzeichen und Satzzeichen werden entfernt und die Umlaute ersetzt. Danach werden alle Doppelbuchstaben, wenn sie sich in der gleichen Buchstabengruppe befinden, durch einen Füllbuchstaben z.B. X getrennt. Wenn am Ende ein einzelner Buchstabe stehen bleibt, wird auch ein X ergänzt. Nun werden die Buchstaben in Zweiergruppen eingeteilt. Aus „Ich komme am Mittwoch“ wird „ic hk om me am mi tx tw oc hx“. Bei der Verschlüsselung gibt es nun drei verschiedene Fälle:

1. Beide Buchstaben liegen in derselben Reihe: Jeder Buchstabe wird verschlüsselt, indem er durch den nächstfolgenden derselben Zeile ersetzt wird. Handelt es sich beim Klartextbuchstaben um den letzten der Zeile, wird mit dem Ersten der Zeile verschlüsselt.
2. Beide Buchstaben liegen in derselben Spalte: Jeder Buchstabe wird verschlüsselt, indem er durch den unter ihm stehenden derselben Spalte ersetzt wird. Handelt es sich beim Klartextbuchstaben um den untersten der Spalte, wird er mit dem Obersten der Spalte verschlüsselt.
3. Beide Buchstaben liegen weder in derselben Reihe noch in der selben Spalte: Man geht in der Zeile des ersten Klartextbuchstaben nach rechts oder links zur Spalte des zweiten

Buchstaben. Der dort stehende Buchstabe ist die Chiffre für diesen. Mit dem zweiten Buchstaben wird ebenso verfahren.

Aus „ic hk om me am mi tx tw oc hx“ wird dann „rdkmtgegfhedszqzsrkw“. Bei der Entschlüsselung wird dann entsprechend wieder umgekehrt vorgegangen.

Auch hier kann zum Knacken eine Häufigkeitsanalyse weiterhelfen, da es auch in der deutsche Sprache viele Zweier-Paare gibt, die oft auftreten, wie z.B. „ch“, „er“, „en“. Außerdem sind die zusammengehörigen Zweier-Gruppen kreuzweise verlinkt, wenn sie nicht in einer Zeile oder Spalte liegen. Aus „PG“ wird „YE“ und aus „YE“ wird „PG“.

3 Moderne Kryptologie

Auch in der Kryptologie hat das 20. Jahrhundert zu bedeutenden Veränderungen und Fortschritten geführt. In der Zeit vor dem 20. Jahrhundert veränderten sich nur die Verfahren zur Kryptographie und zur Kryptoanalyse, im letzten Jahrhundert zog auch die Technik in die Kryptologie ein. Hier sind vor allem drei wichtige Wendepunkte zu nennen.

- Zu Beginn des letzten Jahrhunderts wurde erste mechanische und elektromechanische Verschlüsselungsmaschinen gebaut. Die bekannteste Verschlüsselungsmaschine dieser Zeit ist wohl die Enigma, die zur Sicherung des Funkverkehrs der deutschen Wehrmacht und der Marine im Zweiten Weltkrieg eingesetzt wurde.
- Ein weiterer Wendepunkt ist die aufkommende Computerisierung. Jetzt steht die Verschlüsselung nicht nur für das Militär zur Verfügung, sondern auch für die Wirtschaft und die breite Masse, die die eingesetzten Verfahren nicht kennen muß. Außerdem kann das Verschlüsselungsverfahren von Hand recht unbequem, aber dennoch sehr sicher sein. Es wird auch nicht mehr im Geheimen geforscht, sondern vor allem in der Öffentlichkeit. Nicht das Verfahren bleibt geheim, sondern der Schlüssel.
- Der letzte wichtige Wendepunkt ist die Veröffentlichung eines neuen Verfahrens. In den siebziger Jahren veröffentlichten Diffie und Hellmann das Konzept des „Public-Key-Cryptosystems“ bzw. der asymmetrischen Kryptologie.

3.1 Symmetrische Kryptologie

Bei einem symmetrischen Kryptosystem besteht zwischen dem Schlüssel zum Verschlüsseln und zum Entschlüsseln ein einfacher mathematischer Zusammenhang. Da zum Ver- und Entschlüsseln praktisch der gleiche Schlüssel verwendet wird, muß dieser absolut geheim bleiben. Nur Sender und Empfänger dürfen den Schlüssel besitzen, der zuerst über einen sicheren Kanal ausgetauscht werden muß. Der Nachteil dieses Verfahren ist es, daß zwischen jeder Sender-Empfänger-Beziehung ein neuer Schlüssel notwendig ist. Bekannte Vertreter der modernen symmetrischen Verfahren sind der Data Encryption Standard (DES), der International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), Rivest Cipher Nr.4 (RC4).

3.2 Assymetrische Kryptologie

Bei einem assymetrischen Kryptosystem besteht zwischen dem Schlüssel zum Verschlüsseln (öffentlicher Schlüssel) und zum Entschlüsseln (privater Schlüssel) kein einfacher Zusammenhang. Der zeitliche Aufwand aus, dem öffentlichen Schlüssel den privaten Schlüssel zu errechnen, ist so hoch, daß es sich nicht lohnt, die Verschlüsselung auf diesem Weg zu knacken.

Der Vorteil dieses Verfahrens ist, daß kein sicherer Kanal für einen Schlüsselaustausch vorhanden sein muß. Der Nachteil bei diesem Verfahren ist aber, daß der Schlüssel bei gleicher Sicherheit länger sein muß als bei der symmetrischen Kryptologie. Aus einem längeren Schlüssel ergibt sich auch ein höherer Aufwand beim Ver- und Entschlüsseln. Bekannte Vertreter der assymetrischen Verfahren ist Diffie/Hellmann, ElGamal, Rivest-Shamir-Adleman (RSA). Auf das letztgenannte Verfahren werde ich nun genauer eingehen.

3.2.1 Rivest-Shamir-Adleman

Dieses Verfahren ist das wohl verbreitetste Public-Key-Verfahren. 1977/78 wurde dieses Verfahren von Ron Rivest, Adi Shamir und Len Adleman am MIT entwickelt. Die Sicherheit von RSA beruht auf dem Problem des diskreten Logarithmus und der Schwierigkeit, eine große Zahl in ihre Primfaktoren zu zerlegen. Deshalb darf die Schlüssellänge nicht zu klein gewählt werden. Die Schlüssel werden wie folgt erstellt:

- Es werden zwei verschiedene große Primzahlen p und q zufällig gewählt, wobei die Differenz nicht zu klein sein soll, und daraus das Produkt m gebildet.
- Dann wird eine zufällige Zahl e ermittelt, die kleiner ist als m teilerfremd zu $\varphi = (p - 1) \cdot (q - 1)$ ist.
- Danach wird das multiplikative Inverse d zu e gebildet, d.h. $(e \cdot d) \equiv 1 \pmod{\varphi}$
- Der öffentliche Schlüssel ist dann e und m und der private Schlüssel ist d und m . Die Primzahlen p und q können vergessen werden, sie dürfen jedoch niemals bekannt werden.

Die Verschlüsselung und Entschlüsselung gestaltet sich bei RSA relativ einfach:

- Da RSA nur Zahlen in Zahlen verschlüsselt, muß die Nachricht in numerische Blöcke zerlegt werden, die kleiner als m sein müssen.
- Zur Verschlüsselung nutzt man nun die Funktion $C \equiv M^e \pmod{m}$.
- Zur Entschlüsselung nutzt man die Funktion $M \equiv C^d \pmod{m}$.

Schlüsselerstellung

$$p = 3$$

$$q = 5$$

$$m = p \cdot q = 15$$

$$\varphi = (p - 1) \cdot (q - 1) = 10$$

$$e = 3, 3 < 15, \text{ggT}(3, 10) = 1$$

$$d = 7, \text{damit gilt } (e \cdot d) \equiv 1 \pmod{\varphi}$$

Ver- und Entschlüsselung

$M = 7$ wird verschlüsselt.

$$7^3 \equiv 13 \pmod{15}$$

$$C = 13$$

$C = 13$ wird wieder entschlüsselt.

$$13^7 \equiv 7 \pmod{15}$$

Wie erwartet: $M = 7$.

4 Ausblick

Schon früh (ca. 500 v.Chr.) wurden erste Verschlüsselungsverfahren (Skytale) entwickelt, die zunächst fast nur zu militärischen Zwecken verwendet wurden. Auch heute noch, ca. 2500 Jahre nach den Anfängen der Kryptographie, wird immer noch geforscht. Auch die Methoden der Kryptoanalyse verbessern sich immer weiter. Aber heutzutage gewinnt die Kryptologie auch im Bereich der Wirtschaft oder im privaten Bereich immer mehr Einfluss. Durch die Computertechnik und die Nachrichtenübermittlung durch das Internet ist es nämlich im Gegensatz zum herkömmlichen Posttransport jedem möglich, die Nachrichten abzuhören. Deshalb ist die Verschlüsselung heute notwendig.

Die Entwicklung in der Kryptologie ist immer noch nicht abgeschlossen. Ein neues Verfahren in der Kryptologie ist die Quantenkryptographie, eine Methode zum sicheren Schlüsselaustausch zwischen Kommunikationspartnern.

Aber die Kryptologie ist auch bedroht. So wollen z.B. viele Regierungen wie die von Irak, Myanmar, die Volksrepublik China, USA und Frankreich Verschlüsselung verbieten oder ineffektiv machen, da sie befürchten, daß Terroristen, Kriminelle und Regierungskritiker auf diese Art und Weise unkontrolliert miteinander kommunizieren können. Da es heutzutage für einen Staat möglich ist, die gesamte elektronische Kommunikation der Bevölkerung zu überwachen, ist dies eine Einschränkung des Grundrechts auf Vertraulichkeit des Wortes. Es ist also notwendig, daß wir uns dafür einsetzen, daß die Kryptologie in Deutschland weiterhin straffrei verwendet werden darf. Ich möchte es auch jedem nahelegen, daß er von der Möglichkeit Gebrauch machen soll, seine E-Mails z.B. mit PGP (<http://www.pgp.com/>) oder GnuPG (<http://www.gnupg.org/>) zu verschlüsseln, damit die Privatsphäre gewahrt bleibt.

Literaturverzeichnis

[1] <http://home.nordwest.net/hgm/krypto/index.html>

[2] Wikipedia