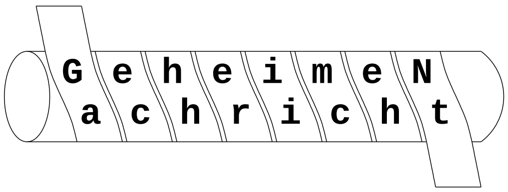
Kryptologie in der Antike

Skytale von Sparta und Transpositionen

Die von den alten Griechen benutzte *Skytale von Sparta* ist eine der ältesten Methoden zur Verschlüsselung von Nachrichten. Eine *Skytale* ist dabei ein Holzstab mit einem festgelegten Durchmesser. Um diesen wird spiralförmig ein Pergamentstreifen gewickelt, den der Absender von links nach rechts beschreibt.

Beispiel: Wir wollen den Text „GeheimeNachricht“ verschlüsseln.



Nach dem Abwickeln des Papierstreifens erhalten wir den Text „GaechherïimcehNt“.

Ist dem Empfänger die Dicke des Holzstabs bekannt, so kann er den Papierstreifen mit der verschlüsselten Nachricht um den Stab herum wickeln und die Nachricht genau so lesen, wie der Absender sie geschrieben hat.

Eine einfache Möglichkeit, diese Verschlüsselungstechnik ohne Holzstab nachzuahmen, besteht darin, den *Klartext* (d.h. den unverschlüsselten Text) zeilenweise aufzuschreiben und dann spaltenweise zu verschicken. Der Empfänger muss die Zeilenlänge kennen, um die erhaltene Nachricht zu entschlüsseln.

Die zu verschlüsselnden Buchstaben bleiben *wie* sie sind, aber nicht *wo* sie sind. Verschlüsselungsverfahren, die nach diesem Prinzip verfahren, heißen *Transpositions-Chiffren*.

Cäsar-Chiffre und Substitutionen

Eine weitere einfache Verschlüsselungsmethode wurde erstmals im Gallischen Krieg beschrieben (58–51 v. Chr.). Es handelt sich um den so genannnten *Cäsar-Chiffre*. Dabei wird jeder Buchstabe durch denjenigen Buchstaben ersetzt, der im Alphabet drei Positionen weiter hinten steht.

Beispiel: Wir wollen wieder „Geheime Nachricht“ verschlüsseln.

Klartext	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
Geheimtext	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

Der Geheimtext, den wir erhalten, lautet „Jhkhlph Qdfkulfkw“.

Beim Cäsar-Chiffre werden nicht die Positionen der Buchstaben verändert, sondern sie werden durch andere Buchstaben ersetzt. Solche Verschlüsselungsmethoden werden *Substitutions-Chiffren* genannt.

Natürlich ist nicht festgelegt, um wie viele Zeichen man das Alphabet verschieben muss. Auf diese Weise erhält man 25 verschiedene Codes. Der Schlüssel ist die Zahl, um wie viele Stellen verschoben wurde. Allerdings ist es für einen Angreifer natürlich möglich, alle 25 Schlüssel auszuprobieren.

Ganz allgemein kann man auch jedes Zeichen durch irgend ein Zeichen ersetzen. Dann gibt es 26 Fakultät ($= 26 \cdot 25 \cdot \ldots \cdot 2 \cdot 1 = 403.291.461.126.605.635.584.000.000$) viele Schlüssel. Der Schlüssel ist hierbei eine Tabelle, die angibt, welches Zeichen durch welches ersetzt wurde.

Lange Zeit glaubte man, dass es auf Grund der großen Anzahl möglicher Schlüssel unmöglich ist, ohne Kenntnis des Schlüssels an den Klartext zu kommen. Es ist aber relativ leicht möglich, solch einfache Substitutions-Chiffres zu knacken. Dies liegt daran, dass die Buchstaben des Alphabets nicht gleich häufig vorkommen. Beobachtet man, dass in einem Geheimtext der Buchstabe „R“ am häufigsten vorkommt, dann ist zu vermuten, dass „E“ durch „R“ ersetzt wurde. Ein solcher Ansatz wird *Häufigkeitsanalyse* genannt.

Bei dem vorgestellten Verfahren handelt es sich um eine so genannte *monoalphabetische Substitution*. Dies bedeutet, dass jeder Buchstabe immer durch den gleichen Buchstaben ersetzt wird. Um die Häufigkeitsanalyse zu erschweren, kann man für häufig vorkommende Buchstaben mehrere Zeichen zur Verschlüsselung verwenden, von denen bei jedem Vorkommen eins ausgewählt wird.

Beispiel: Da der Buchstabe „E“ besonders häufig vorkommt, ersetzen wir ihn nicht nur durch „H“, sondern wahlweise durch „?“. Aus „Geheime Nachricht“ könnte dann „Jhk?lp? Qdfkulfkw“ werden. Genauso können für weitere häufig vorkommende Buchstaben verschiedene Zeichen verwendet werden.

Bei diesen sogenannten *polyalphabetische Substitutionen* genügen die 26 Buchstaben nicht mehr zur Verschlüsselung. Man kann sich z.B. damit helfen, dass jeder Buchstabe z.B. durch ein Paar von Buchstaben verschlüsselt wird.

Aber auch ein solcher Kode ist verhältnismäßig einfach zu entschlüsseln: man kann Häufigkeiten von Buchstabenpaaren wie z.B. „ck“ oder „ei“ ausnutzen.