Die Caesar-Verschüsselung

Die Verwendung der Verschlüsselung für militärische Zwecke geht auf den römischen Feldherrn Julius Caesar[1] zurück, der sie bereits im gallischen Krieg[2] verwendete. Er verfasste eine Nachricht an den mit seinen Leuten belagerten Quintus Cicero, der kurz davor stand, sich zu ergeben.

a) Einfache Caesar-Verschlüsselung

Bei diesem einfachen Verschlüsselungsverfahren wird einfach jeder Buchstabe des Klartextalphabeths durch einen, um eine festgelegte Anzahl Stellen weiter hinten im Alphabeth stehenden Buchstaben ersetzt. Die Stellenverschiebung nennt man Caesar-Verschiebung.

Beispiel mit Caesar-Verschiebung 3:

Klartextalphabeth:	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
Geheimtextalphabeth:	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
Klartext:	veni, vidi, vici
Geheimtext:	YHQL, YLGL, YLFL

Die Nachteile dieses recht simplen Verfahrens lassen sind nicht schwer zu erkennen. Das Hauptproblem ist, dass der gleiche Buchstabe im Klartext immer wieder zum gleichen Buchstaben im Geheimtext übersetzt wird. Ein weiteres Problem besteht darin, dass der Sender und der Empfänger wissen müssen, um wieviele Stellen das Alphabet verschoben werden muss. Die Stellenverschiebung kann auch als Schlüssel aufgefasst werden. Wie teilt der Sender dem Empfänger mit welche Verschiebung er verwendet hat? Auf jeden Fall so, dass es niemand anderst mitbekommt. Man nennt das das Problem des Schlüsseltausches.

b) Caesar-Verschlüsselung mit beliebig vertauschtem Geheimtextalphabet

Um die oben beschriebene einfache Verschlüsselung zu verbessern kam man auf die Idee, nicht nur das Alphabet um eine Anzahl Stellen zu verschieben, sondern als Geheimtextalphabet ein beliebig durcheinandergewürfeltes Alphabet zu verwenden.

Beispiel mit beliebig vertauschtem Geheimtextalphabet

Klartextalphabeth:	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
Geheimtextalphabeth:	J L P A W I Q B C T R Z Y D S K E G F X H U O N V M
Klartext:	et tu, brutus?
Geheimtext:	WX XH, LGHXHF?

Leider werden dadurch die oben erwähnten Nachteile nicht aus dem Weg geräumt. Immernoch wird der gleiche Klartextbuchstabe in den jeweilig gleichen Geheimtextbuchstaben übersetzt. Auch das Problem des Schlüsseltausches ist nicht behoben, im Gegenteil. Der Sender muss sicherstellen, dass der Empfänger weiss, wie das beliebig durcheinandergewürfelte Geheimtextalphabet aussieht. D. h. die beiden müssen es vorgängig abmachen.

---

1 100 – 44 v Chr.

2 58 – 51 v Chr.

c) Caesar-Verschlüsselung mit Schlüsselwort

Damit beim Tauschen des Schlüssels nicht das ganze Alphabet ausgetauscht werden muss wie bei b), und die Verschlüsselung doch nicht so simpel ist wie bei der Caesar-Verschiebung, kann die Caesar-Verschlüsselung mit Schlüsselwort verwendet werden.

Der Sender und der Empfänger machen vorgängig miteinander ein Schlüsselwort (oder auch Wörter) ab. Z.B. `julius caesar.` Zur Herstellung des Geheimalphabets werden nun aus dem Schlüsselwort alle Leerzeichen und mehrmals vorkommenden Buchstaben entfernt. Im Beispiel bleibt noch `juliscaer.` Diese Buchstabenfolge ist nun der Beginn des Geheimtextalphabeths. Anschliessend wird das Alphabet mit den noch nicht benutzen Buchstaben , alphabetisch beim letzten Buchstaben des Schlüsselworts beginnend, aufgefüllt.

Klartextalphabeth:	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
Geheimtextalphabeth:	***J U L I S C A E R*** T V W X Y Z B D F G H K M N O P Q
Klartext:	errare humanum est
Geheimtext:	SFFJFS EKXJYKX SGH

Auch bei diesem Verfahren bleibt der Nachteil bestehen, dass gleiche Klartextbuchstaben identische Geheimtextbuchstaben haben.

Weiterführende Links (16.11.2006)

http://willy.chemie.uni-konstanz.de/fotos/caesar.htm

http://www.oszhdl.be.schule.de/gymnasium/faecher/informatik/krypto/krypt_1.3.htm