Klassische Kryptographie

Verschiebechiffren

Die einfachsten Verfahren sind Verschiebechiffren. Diese Art der Chiffrierung soll schon Julius Caesar benutzt haben. Man verschlüsselt dabei einen beliebigen Text, indem man das *Klartextalphabet* unter das *Geheimtextalphabet* schreibt – aber um *k* Stellen nach links oder 26 − *k* Stellen nach rechts verschoben.
Beispiel:

```
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
```

Hier wurde das Alphabet um 3 Stellen nach links verschoben. Man chiffriert nun eine Nachricht, indem man den Klartextbuchstaben durch den darunterstehenden Geheimtextbuchstaben ersetzt. Aus dem Wort klartext würde in unserem Fall NODUWHAW. Für k gibt es genau 26 Möglichkeiten. k wäre hier der Schlüssel. Man kann dieses äußerst simple Verfahren knacken, indem man einfach alle Möglichkeiten ausprobiert! Es gibt noch andere Möglichkeiten zum Knacken, aber dazu mehr im nächsten Kapitel.
Solche Chiffrierungen werden auch als additive Chiffrierungen bezeichnet, da wir eigentlich den Wert k zum Klartextbuchstaben addieren, um den Geheimtextbuchstaben zu erhalten. Dazu nummerieren wir das Alphabet von 0 bis 25 durch,

a = 0, b = 1, c = 2, d = 3, ... y = 24, z = 25.

Um zu verschlüsseln, addieren wir k zu einem Buchstaben:

a + 3 = D entspricht 0 + 3 = 3

Wenn die Summe größer als 25 ist, muss man diese Summe durch 26 teilen und den entstandenen Divisionsrest in einen Buchstaben zurückübersetzen. Dies nennt man auch modulo-Operation.
Beispiele:
(y + 4) mod 26 = (24 + 4) mod 26 = 3 = C
Zur Dechiffrierung subtrahiert man k vom Geheimtextbuchstaben. Dann addiert man 26 hinzu und führt eine Modulo-Operation durch:

k = 3, Geheimtextbuchstabe: B
(B − 3 + 26) mod 26 = (1 − 3 + 26) mod 26 = 24 = y
k = 19, Geheimtextbuchstabe: X
(X − 19 + 26) mod 26 = (23 − 19 + 26) mod 26 = 4 = e

Multiplikative Chiffren

Bei dieser Chiffrierung verwendet man statt Addition Multiplikation modulo 26 (siehe vorheriges Kapitel). Wir multiplizieren jeden Klartextbuchstaben mit dem Schlüssel *k*. Ein Beispiel mit *k* = 2:

```
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: B D F H J L N P R T V X Z B D F H J L N P R T V X Z
```

Auffallend ist hier, dass jeweils zwei unterschiedliche Buchstaben dasselbe Produkt ergeben! Daher können wir diese Substitution nicht als Chiffre verwenden. Für jede Chiffrierung muss nämlich gelten:
*Der Klartext muss mit Hilfe des Schlüssels **eindeutig** aus dem Geheimtext rekonstruierbar sein!*
Probieren Sie es trotzdem noch einmal, aber diesmal mit *k* = 3:

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	A	D																								

Formel:

Diese Chiffrierung funktioniert! Und sie funktioniert auch mit den Zahlen 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 und 25. Diese Zahlen haben die Eigenschaft, dass sie keine gemeinsamen Teiler mit 26 haben. 26 ist das Produkt der beiden Primzahlen 2 und 13, wir dürfen also keine Zahlen verwenden, die ein Vielfaches von 2 oder 13 sind. Man sagt, die Zahlen müssen *teilerfremd* zu 26 sein. Für diese Art der Chiffrierung gibt es somit nur exakt 12 Möglichkeiten. Bei der additiven Chiffrierung gibt es immerhin 26 Möglichkeiten! Man kann diese beiden Typen auch kombinieren, aber das bringt uns trotzdem nicht viel, wie wir gleich sehen werden.

Klassische Kryptographie

Kryptoanalyse

Betrachten Sie einmal folgenden Satz: ***dieser text ist streng geheim***.
Verschlüsselt mit dem ersten obigen Beispiel ergibt sich der Chiffretext:
WCSUSJ JSOJ CUJ UJNSGE ESDSCT.
Nun, auf den ersten Blick hat sich viel geändert, aber schauen Sie einmal genauer hin: Es gibt Buchstaben, die ihrer Häufigkeit wegen auffallen – z. B. das S und das J. Entschlüsselt sind das die Buchstaben e und t. Und genau da liegt das Problem: Leider kommen nicht alle Buchstaben mit gleicher Häufigkeit vor. Das e kommt mit einer Häufigkeit von durchschnittlich 17,4 Prozent, das s mit 7,3, r mit 7, a mit 6,5 usw. vor (siehe Tabelle unten). Das klägliche Schlusslicht dieser Reihe ist übrigens das q, das nur mit 0,02 Prozent vertreten ist. Um einen verschlüsselten Text zu knacken, untersucht man zunächst die Häufigkeiten von jedem Geheimtextzeichen und probiert dann verschiedene Buchstaben aus, die aufgrund ihrer Häufigkeit passen könnten.
Die Tatsache, dass sich die Häufigkeiten je nach Art des Textes (wissenschaftlich, politisch, privat ...) unterscheiden, stellt in der Regel kein großes Hindernis dar, da der Angreifer, der den Text abgefangen/gefunden hat, oft schon erraten kann, um was für eine Art es sich handelt. Kurze Texte sind schwieriger zu knacken, aber Computer können viele Möglichkeiten in kurzer Zeit durchprobieren (jeder normale Home-PC vielleicht 1 Million pro Sekunde) und daher auch Buchstaben ausprobieren, die normalerweise weniger häufig vorkommen.

Zeichen	englisch	deutsch	Zeichen	englisch	deutsch
a	8.04	6,47	**n**	7,09	9,84
b	1,54	1,93	**o**	7,60	2,98
c	3,06	2,68	**p**	2,00	0,96
d	3,99	4,83	**q**	0,11	0,02
e	12,51	17,48	**r**	6,12	7,54
f	2,30	1,65	**s**	6,54	6,83
g	1,96	3,06	**t**	9,25	6,13
h	5,49	4,23	**u**	2,71	4,17
i	7,26	7,73	**v**	0,99	0,94
j	0,16	0,27	**w**	1,92	1,48
k	0,67	1,46	**x**	0,19	0,04
l	4,14	3,49	**y**	1,73	0,08
m	2,53	2,58	**z**	0,09	1,14

deutsch				englisch			
er	409	**ein**	122	**th**	315	**the**	353
en	400	**ich**	111	**he**	251	**ing**	111
ch	242	**nde**	89	**an**	172	**and**	102
de	227	**die**	87	**in**	169	**ion**	75
ei	193	**und**	87	**er**	154	**tio**	75
nd	187	**der**	86	**re**	148	**ent**	73
te	185	**che**	75	**on**	145	**ere**	69
in	168	**end**	75	**es**	145	**her**	68
ie	163	**gen**	71	**ti**	128	**ate**	66
ge	147	**sch**	66	**at**	124	**ver**	64