– Eine Methode, die bis heute erfolgreich angewandt wird, ist die *Steganographie*. Dabei wird die Geheimnachricht in einer harmlosen Nachricht versteckt. Zum Beispiel könnte man gewisse Teile eines Textes dadurch kennzeichnen, dass man über oder unter ihr mit einer Nadel ein kleines Loch anbringt; diese Buchstaben ergeben die Geheimnachricht. Oder man könnte gewisse Rasterpunkte (Pixel) eines elektronisch übertragenen Bildes auszeichnen, die, wenn sie isoliert werden, etwas ganz anderes zeigen als das umgebende Bild. Die Grundidee der Steganographie ist, dass nur derjenige, der weiß, *dass* etwas versteckt ist, und weiß, *wo* er suchen muss, etwas findet.

2. Verschlüsselung «ohne Schlüssel»

Die Methoden, die wir von nun an behandeln werden, suchen nicht die Existenz einer vertraulichen Nachricht zu verbergen. Im Gegenteil: In fast herausfordernder Weise wird der Gegner provoziert: Die Nachricht wird offen übermittelt, aber so verändert, dass der Gegner keine Chance hat, den Klartext zu ermitteln – so hoffen jedenfalls Sender und Empfänger.

Wir betrachten einige Beispiele:

– *Die spartanische Skytala*

Es wird berichtet, dass die Generäle der Spartaner auf folgende Weise geheim miteinander kommuniziert haben:

Der Sender einer Nachricht wickelt ein Band um einen Zylinder (die Skytala), etwa einen Holzstab. Dann schreibt er die Nachricht längs des Stabes auf das Band. Anschließend wird das Band abgewickelt und so dem Empfänger übermittelt. Da die Buchstaben darauf in einer völlig wirren Anordnung zu sehen sind, kann niemand den Klartext herausfinden. Der Empfänger muss einen Zylinder gleichen Durchmessers besitzen; wenn er das Band um diesen wickelt, kann er die Nachricht ohne Schwierigkeiten lesen.

– *Der Code des Polybios*

Der griechische Geschichtsschreiber Polybios (ca. 200–120 v. Chr.) schrieb nicht nur die erste Universalgeschichte der Welt, sondern erfand auch – nebenbei – den folgenden Code.

Die Buchstaben werden in Kästchen geschrieben, so dass insgesamt ein 5×5-Quadrat ausgefüllt wird. Da es in der deutschen Sprache genau 26 Buchstaben gibt, wir aber nur 25 Plätze haben, schreiben wir I und J in dasselbe Kästchen. Die Zeilen und Spalten werden mit 1, 2, 3, 4, 5 nummeriert.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Ein Buchstabe wird durch zwei Ziffern ersetzt, und zwar durch die Ziffer neben ihm und durch die Ziffer über ihm.

Zum Beispiel schreiben wir statt M die Zahl 32. Dieser Code kann auch akustisch übermittelt werden, indem man die Ziffern durch die entsprechende Anzahl von Klopfzeichen ersetzt:

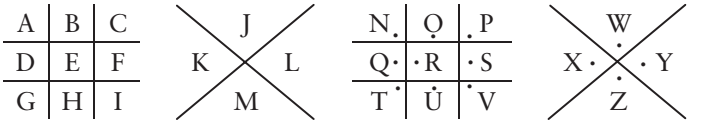
•• •• • ••••• •• ••• • ••••• •• •••• ••• ••

Oft wurde versucht, die Nachricht in eine Folge von Geheimzeichen zu verwandeln, die niemand zu deuten vermag. Allen Geheimzeichencodes liegt die Vorstellung zugrunde, dass die Geheimzeichen selbst die Nachricht schützen – eine Vorstellung, bei der aufgeklärte Zeitgenossen ein Stirnrunzeln nicht unterdrücken können.

Auch dazu zwei Beispiele.

– *Der Freimaurer-Code*

Beim sogenannten Freimaurer-Code wird jeder Buchstabe nach folgendem Schema durch einen Buchstaben ersetzt:



Zum Beispiel ist

nichts anderes als das Wort KRYPTOGRAPHIE.

– *Der Code von E. A. Poe*
In seiner Erzählung «Der Goldkäfer» lässt Edgar Allan Poe (1809–1849) den Helden Legrand folgende Geheimschrift lösen, bei der jedes Zeichen einem Buchstaben der englischen Sprache entspricht:

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8
¶60))85;1‡(;:‡*8†83(88)5*†;46(;88*96
?;8)‡(;485);5*†2:*‡(;4956*2(5*–4)8
¶8*;4069285);)6†8)4‡‡;1(‡9;48081;8:
8‡1;48†85;4)485†528806*81(‡9;48;(8
8;4(‡?34;48)4‡;161;:188;‡?;

Der Text wird in der Erzählung gründlich analysiert; der Klartext lautet:

A good glass in the bishop's hostel in the devil's seat forty-one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death's-head a bee-line from the tree through the shot fifty feet out.

Man wird allerdings dem Kommentar zustimmen müssen, dass der Text damit nicht enträtselt wurde. Lesen Sie aber selbst, wie Legrand das Kryptogramm entschlüsselt und was er aus ihm herausliest.

3. Was ist Kryptographie?

Im Folgenden sehen Sie drei Geheimtexte. Alle drei wurden aus demselben Klartext erhalten. Der erste Text wurde mit einer Geheimsprache erhalten und ist ganz einfach zu entschlüsseln: Spätestens dann, wenn Sie den Satz laut lesen, offenbart er seinen Sinn und widerspricht damit sich selbst:

Dodiesoseror Sosatotzoz isostot gogehoheimom.

Die beiden folgenden Zeilen sehen gleich kryptisch aus. Keine scheint sich vor der anderen durch besondere Klarheit auszuzeichnen:

U Z V J V I J R K Q Z J K X V Y V Z D
T F Z Z G R E D F Y A B X I F F H X Y

Und doch: Der erste dieser beiden Texte ist so einfach verschlüsselt, dass man ihn auch im Klartext hätte notieren können, während der zweite einen unknackbaren Code darstellt!

4. Cäsar oder Der Beginn der Kryptographie

Obwohl der Cäsar-Code zu den unsichersten Verschlüsselungsverfahren der Weltgeschichte gehört, kann man behaupten, dass mit diesem Code die Kryptographie begonnen hat. Denn dieser Code, der von C. J. Cäsar (100–44 v. Chr.) benutzt wurde, basiert auf zwei radikalen Entscheidungen:

– *Keine Geheimzeichen!*
Geheimzeichen beschwören zwar eine Aura des Geheimnisvollen, bieten aber im Grunde keine Sicherheit. Es mag schwer sein, sich die Zeichen zu merken oder sie nachzuzeichnen, aber nüchtern betrachtet, ist dies der einzige Vorteil. Der Code wird um keinen Deut besser, wenn man jedes Geheimzeichen durch ein gut lesbares Zeichen darstellt.

Dem Cäsar-Code liegt eine radikale Entscheidung zugrunde: Die Klartextzeichen und die Geheimtextzeichen sind dieselben, für beide werden die Buchstaben benutzt.

– *Eingebaute Variabilität!*
Bei den bisher von uns betrachteten Codes war es so: Wenn ein Angreifer den Code geknackt hat (das bedeutet, die Übersetzung von Klartextzeichen in Geheimtextzeichen kennt), dann muss man einen neuen Code entwerfen und dies dem Empfänger mitteilen. Das ist nicht nur umständlich, sondern bietet auch keinerlei quantifizierbare Sicherheit.

Auch hier traf Cäsar eine radikale Entscheidung (vorsichtiger gesagt: Wir interpretieren sein Verfahren so): Sein «Code» besteht nicht nur aus einer einzigen Übersetzungsvorschrift, sondern aus einer ganzen Menge. Der Wechsel der einzelnen Vorschriften ist sozusagen in das System eingebaut. Wir werden das später durch den Begriff «Schlüssel» beschreiben.

Übrigens bezeichnet man in der Kryptographie – auch in nichtmilitärischen Situationen – jeden Unbefugten, der versucht, einen Code zu analysieren, als Angreifer (manchmal auch als Kryptoanalytiker). Der Angreifer spielt eine wichtige Rolle; tatsächlich kann man jedes kryptographische Verfahren als ein Dreipersonenspiel betrachten: Sender und Empfänger versuchen, sich gegen den Angreifer zu schützen, während es die Aufgabe des Angreifers ist, den Schutzwall von Sender und Empfänger zu durchbrechen.

Nun müssen wir Cäsars revolutionären Code aber beschreiben. Man benutzt zwei Alphabete, das Klartextalphabet (das ist das Alphabet in natürlicher Reihenfolge; zur Abkürzung nennen wir es KTA) und das Geheimtextalphabet (GTA), das wir darunter schreiben:

KTA: 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
GTA: 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

Das Geheimtextalphabet ist ebenfalls das gewöhnliche Alphabet, nur um ein paar Stellen verschoben. In unserem Beispiel beginnen wir unter dem Klartext-A mit dem Geheimtextbuchstaben D, setzen dann das Alphabet wie gewohnt mit E, F, G, … fort, bis wir am Ende angelangt sind, und beginnen dann wieder