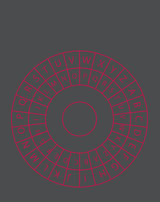
VERSCHLÜSSELUNG

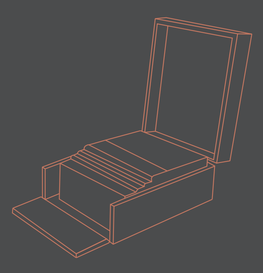
Was

CAESER



Bei der Caesar-Verschlüsselung handelt es sich um ein symmetrisches Verfahren. Das bedeutet, dass der gleiche Schlüssel für der Ver- und Ent- schlüsselung genutzt wird. Tatsächlich leitet sich diese Verschlüsselung vom Feldherrn Gaius Julius Caesar ab, der dieses Verfahren für seine militärischen Korrespondenzen nutzte, um sicher zu kommunizieren. Hierbei wurde jedem Buchstaben des eigentlichen Alphabetes ein anderer Buchstabe zugeordnet, sodass der Klartext dadurch verschlüsselt werden konnte. Doch durch die Analyse der Buchstaben konnte man die Häufigkeit bestimmter Buchstaben erkennen und somit diese Verschlüsselung schnell aushebeln

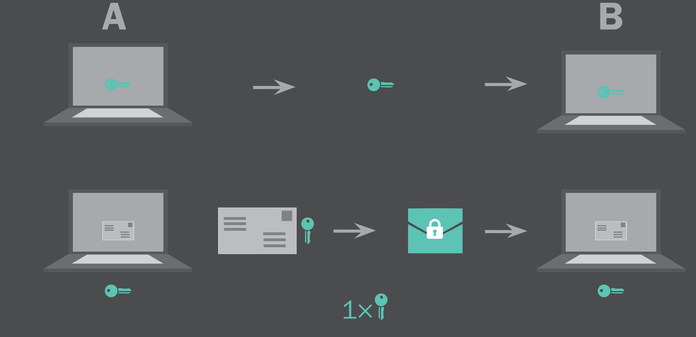
ENIGMA



Die deutschen Einsatzkräfte nutzen diese Verschlüsselungsmaschine, um militärische Nachrichten zu übermitteln. Ein ENIGMA-Kasten ist 340 mm × 280 mm × 150 mm groß und besteht aus einer Tastatur, einem Walzensatz mit drei austauschbaren Walzen und einem Lampenfeld zur Anzeige. Die Walzen sind drehbar angeordnet und weisen auf beiden Seiten für die 26 Großbuchstaben elektrische Kontakte auf, die durch 26 isolierte Drähte im Inneren der Walze paarweise und unregelmäßig miteinander verbunden sind, beispielsweise (Walze III) Kontakt A mit B, B mit D, und so weiter. Drückt man eine Buchstabentaste, so fließt elektrischer Strom über die gedrückte Taste durch den Walzensatz und lässt eine Anzeigelampe aufleuchten. Der aufleuchtende Buchstabe entspricht der Ver - schlüsselung des gedrückten Buchstabens. Da sich bei jedem Tastendruck die Walzen ähnlich wie bei einem mechanischen Kilometerzähler weiterdrehen, ändert sich das geheime Schlüsselalphabet nach jedem Buchstaben. Geknackt wurde die Enigma von den Allierten im Zweiten Weltkrieg

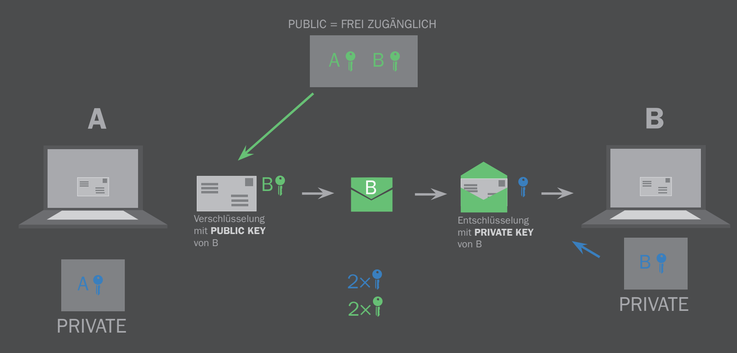
AES

AES ist die Abkürzung für 'Advanced Encryption Standard' und gilt als beliebter kryptografischer, symmetrischer Verschlüsselungs-Standard in der IT-Welt. Zahlreiche Verschlüsselungs-Lösungen wie TrueCrypt arbeiten schon seit längerem mit AES. Ein erheblicher Erfolgsfaktor war neben dem Einsatz durch die US-Regierung im Jahr 2002 auch die Tatsache, dass seit 2003 auch geheime Daten mit AES geschützt werden können.

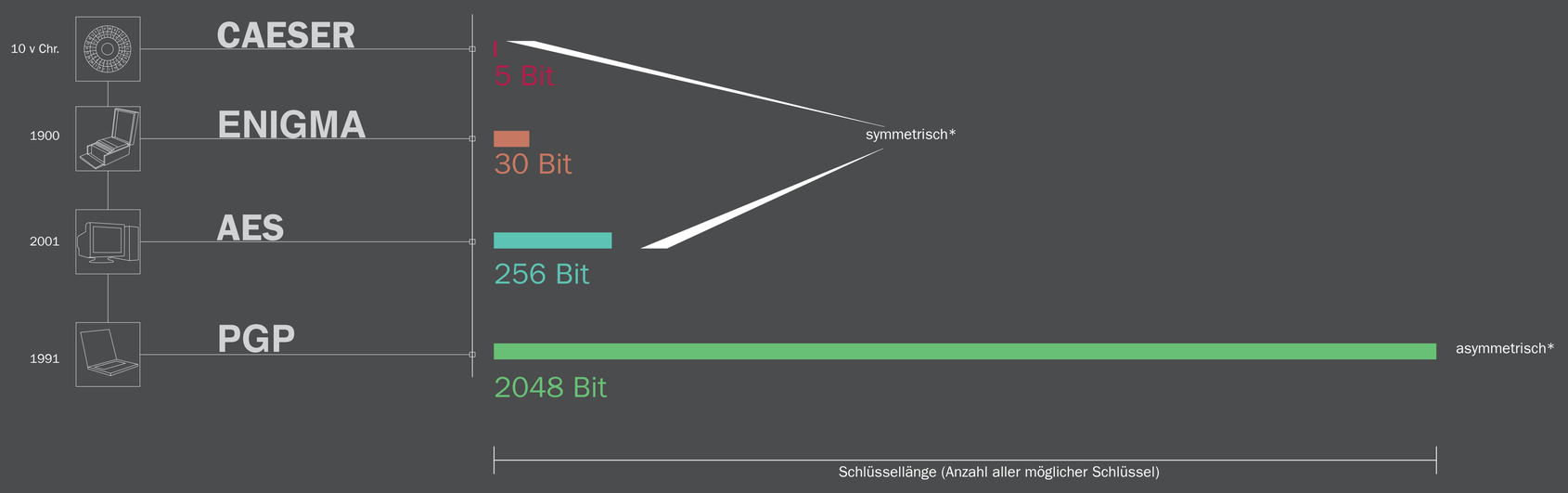


PGP

PGP steht für "Pretty Good Privacy". Es handelt sich dabei um ein Programm des US-Amerikaners Phil Zimmermann. Die erste Version fand bereits am 5. Juni 1991 ihren Weg in verschiedene Mailboxen.
PGP ermöglicht es, Nachrichten so zu verschlüsseln, dass nur der echte Empfänger sie lesen kann. Dabei kommen Verschlüsselungsalgorithmen zum Einsatz, an denen sich selbst der amerikanische Geheimdienst die Zähne ausbeißt. Nicht zuletzt deshalb versuchten die USA lange Zeit, den Export von PGP um jeden Preis zu verhindern. Jedoch ist der Versuch gescheitert.



Wie sicher ?



Was ist symmetrisch?

Symmetrisch ist eine Verschlüsselung dann, wenn beide Teilnehmer ein und den gleichen Schlüssel für das Ver- und Entschlüsseln benutzen, z.B. AES. (Das gängige Schlüssel-Schlosselprinzip)

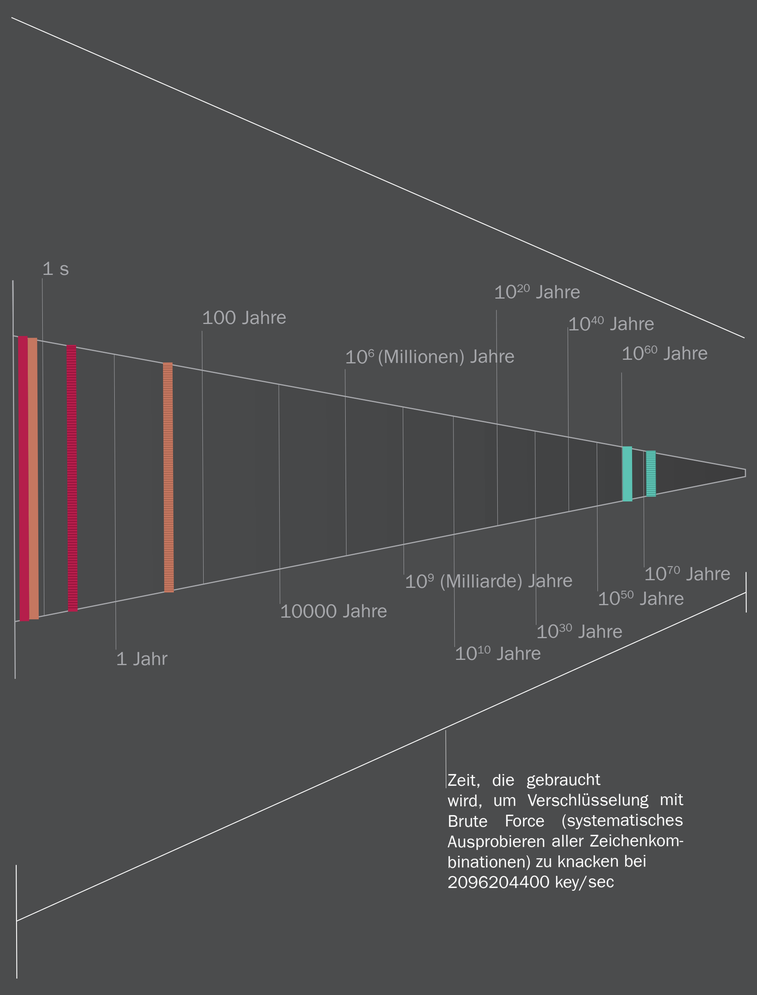
Was ist asymmetrisch?

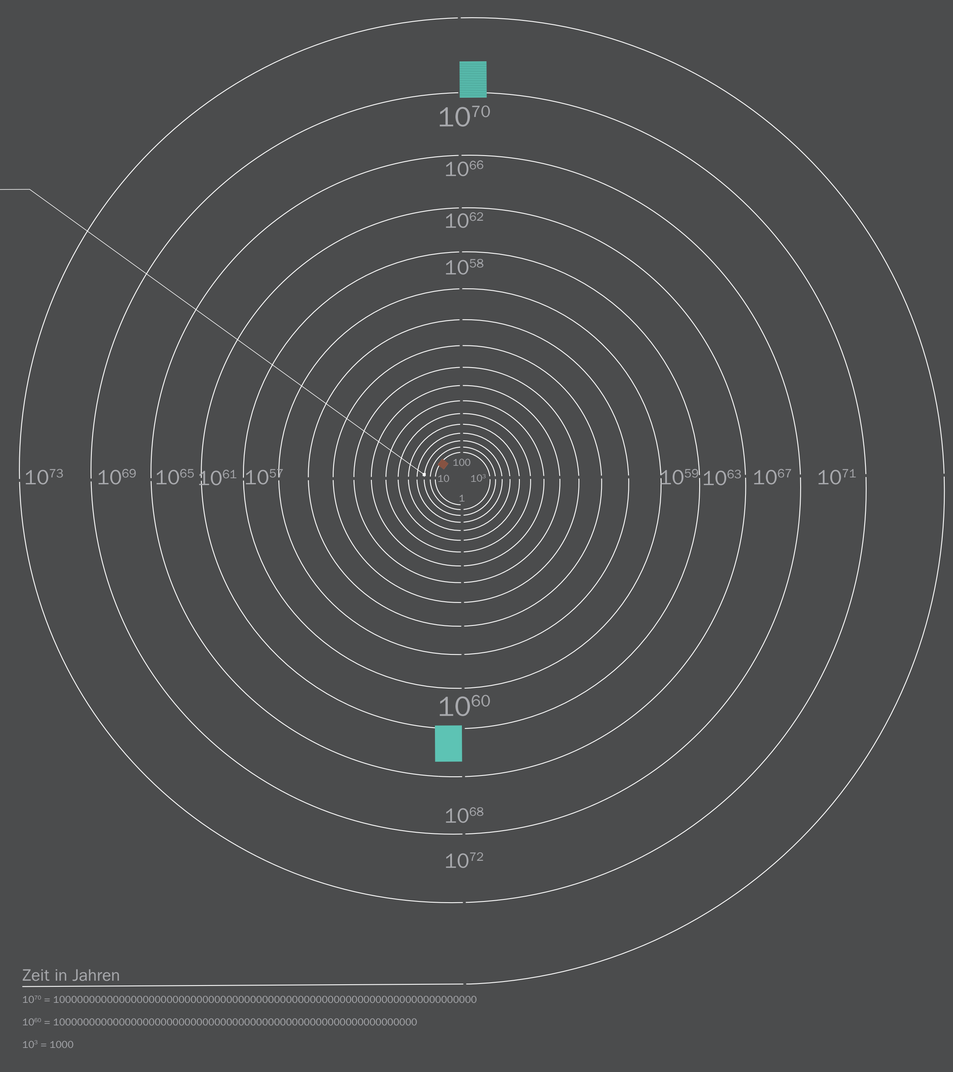
Hierbei werden nicht die gleichen Schlüssel zum Ver- und Entschlüsseln benutzt, sondern jeweils zwei Schlüsselpaare generiert, die öffentlich und privat sind (siehe PGP) und nur bedingt miteinander zusammenhängen. Dies macht die asymmetrische Verschlüsselung um einiges sicherer, als die symmetrische, da nicht alles von einem Schlüssel abhängig ist.

Was ist ein Bit

Ein Bit ist eine Informationseinheit und gibt die Anzahl möglicher Kombinationen von 0 und 1 an.

1 Bit	2 Kombinationen
2 Bit	4 Kombinationen
4 Bit	16 Kombinationen
8 Bit	256 Kombinationen
16 Bit	65536 Kombinationen
32 Bit	4294967296 Kombinationen





1 entschlüsselnder PC vs. 1 verschlüsselter PC

11.930 ns (nano) | 256.1 ms (milli) | 1.75×10^60 Jahre | keine Werte

1 entschlüsselnder PC vs. 7 Milliarden verschlüsselte PCs

13.51 s | 56.808 Jahre | 1.225×10^70 Jahre

Tipps

Mail-Verschlüsselung

PGP-Verschlüsselung mit
THUNDERBIRD/ENIGMAIL/GNUPG (WIN)
oder GPG Tools (MAC)

Festplatten-Verschlüsselung

TRUECRYPT (WIN/MAC)
FILEVAULT (MAC)

Sichere Passphrase

möglichst lang (Sätze/Wortgruppen)
Sonderzeichen
keine Wörter
so willkürlich, wie nur möglich

Spuren verwischen

Bleachbit(WIN)

Browser

TOR Bundle (WIN/MAC)