Verschlüsselung

Verfahren damals und heute

Antike Techniken?

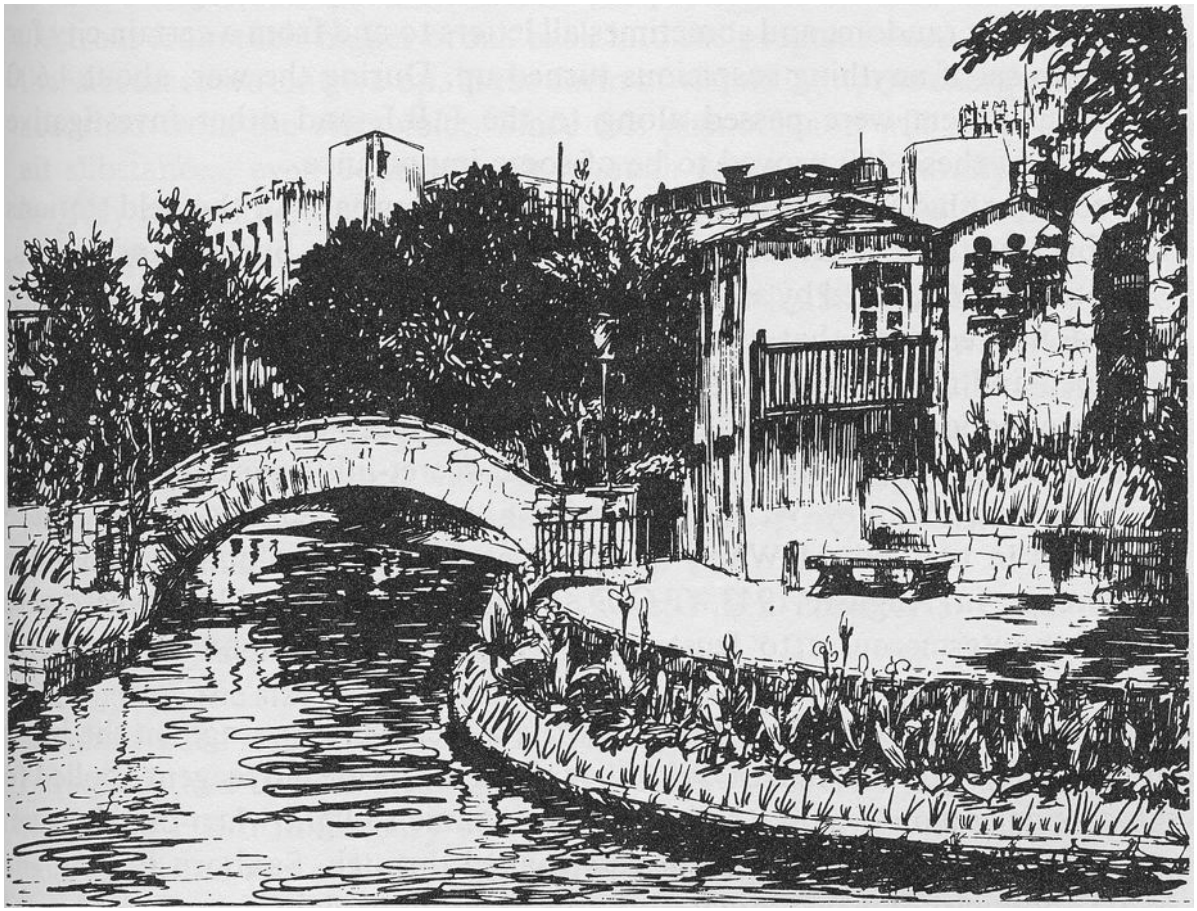
- Spartaner (ca. 900 v. Chr.) → **Skytale**

Quelle: https://images.app.goo.gl/8LYPmZxxG2vD3HMZA

- **Steganographie**
  - Unsichtbare Tinte
  - Wasserzeichen
  - Doppelter Boden
  - Wachstafeln
  - Gedichte
  - Bilder (Semagramme)

Quelle: https://images.app.goo.gl/LLNNjTFF386TMX3d8

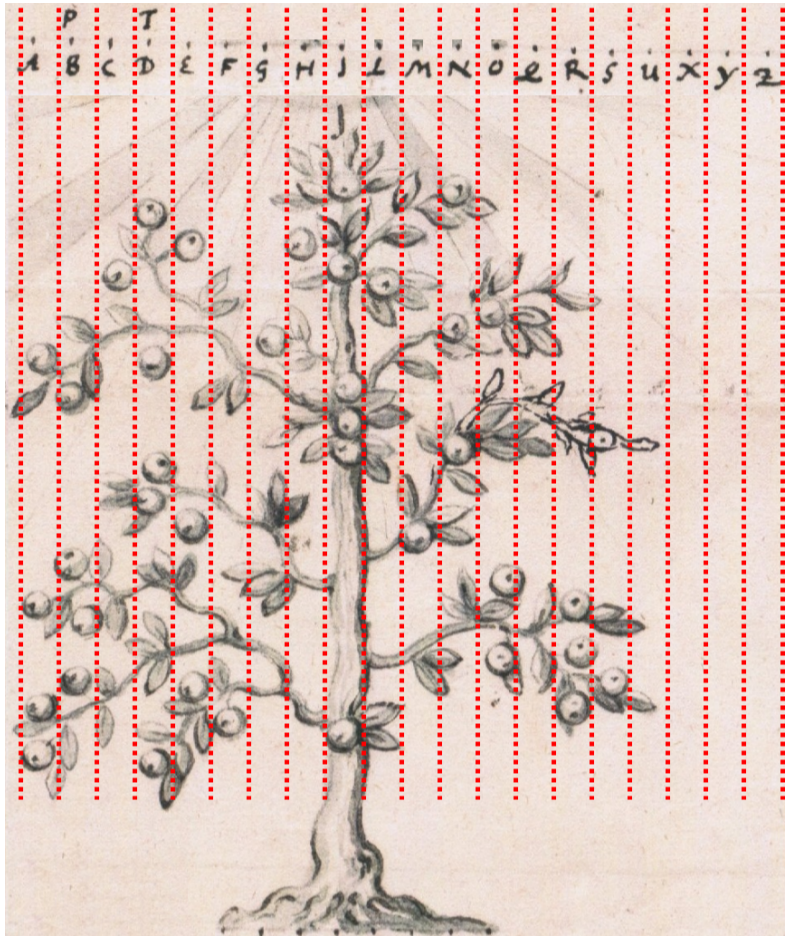
Semagramme



Quelle: https://images.app.goo.gl/RJx89RjJD7ReiSEF6

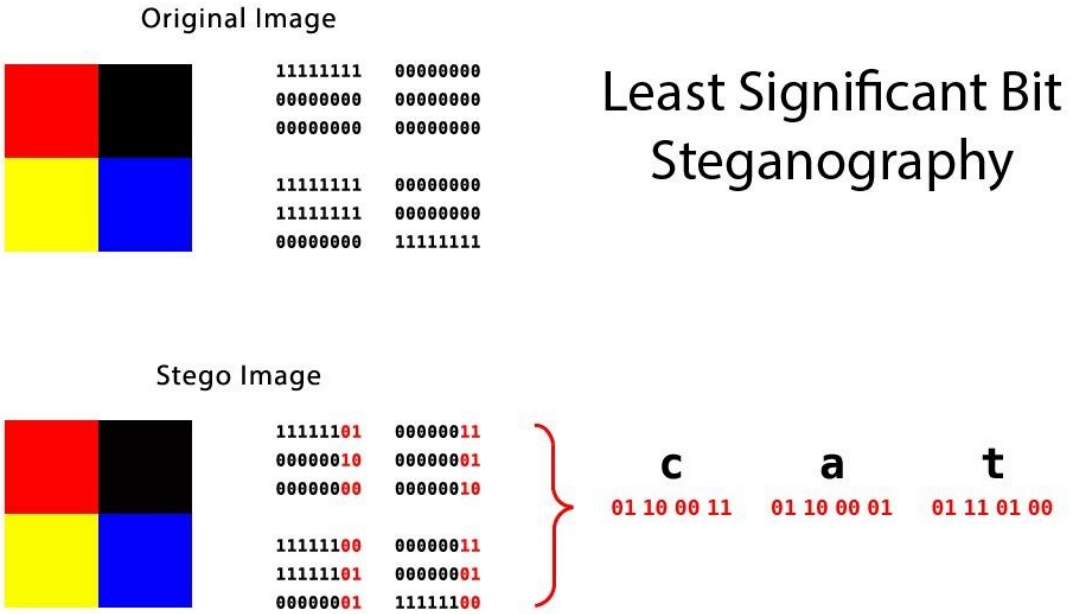
Semagramme

Quelle: https://images.app.goo.gl/eybpaxbH5qLwv1no6



Quelle: https://images.app.goo.gl/eybpaxbH5qLwv1no6

Steganographie – Digitale Bildformate

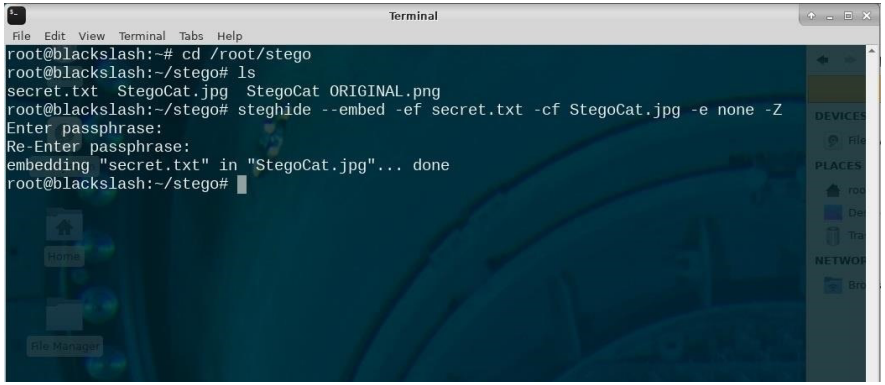


Quelle: https://bit.ly/2ShZcsN

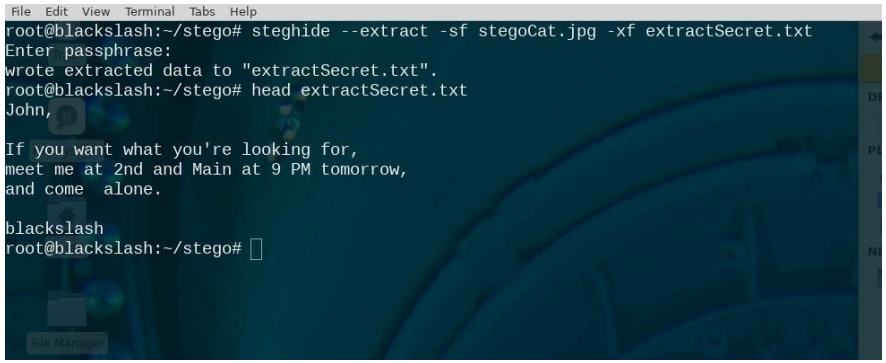
Quelle: https://images.app.goo.gl/eybpaxbH5qLwv1no6

Least Significant Bit wird in RGB-Werten verändert, um Nachricht zu übermitteln.

Steganographie - Konsole



Quelle: https://bit.ly/2SAaFCW



Quelle: https://bit.ly/2Sj2JH7

Quelle: https://bit.ly/2UTRpTR

Moderne Verschlüsselungsarten

- Monoalphabetische Verschlüsselung
  - Verschiebung (z.B. Cäsar Verschlüsselung – 26 Möglichkeiten – leicht zum Entschlüsseln)
  - Tausch (ohne Reihenfolge – 26! (faktorielle) Möglichkeiten = $4*10^{26}$ = 400 Quadrillionen
  - Kombination (benötigt Schlüsselwort und Schlüsselbuchstabe)
- Polyalphabetische Verschlüsselung
  - Blaise de Vigenère (1523–1596)
  - Giovan Battista Bellaso (1553)

- Problem dieser Verfahren → Schlüssel muss ebenfalls übertragen werden!
- Problemlösung → Public Key Verfahren → Briefkastensystem
  - **3 Arten** → **symmetrisch** (nur ein Schlüssel), **asymmetrisch** (ein öffentlicher und ein privater Schlüssel), **hybride** (RSA für Schlüsselübertragung – restliche Übertragung symmetrisch)

Public Key – RSA

- RSA → asymmetrisches Verfahren (von Ron Rivest, Adi Shamir & Leonard Adleman)

- Private (privater) Key: p
- Public (öffentliche) Keys: o_1, o_2
- Nachricht: n
- Geheimnachricht: g

Beispiel:

p = 7

o_1 = 3

o_2 = 15

n = 8

Verschlüsseln:

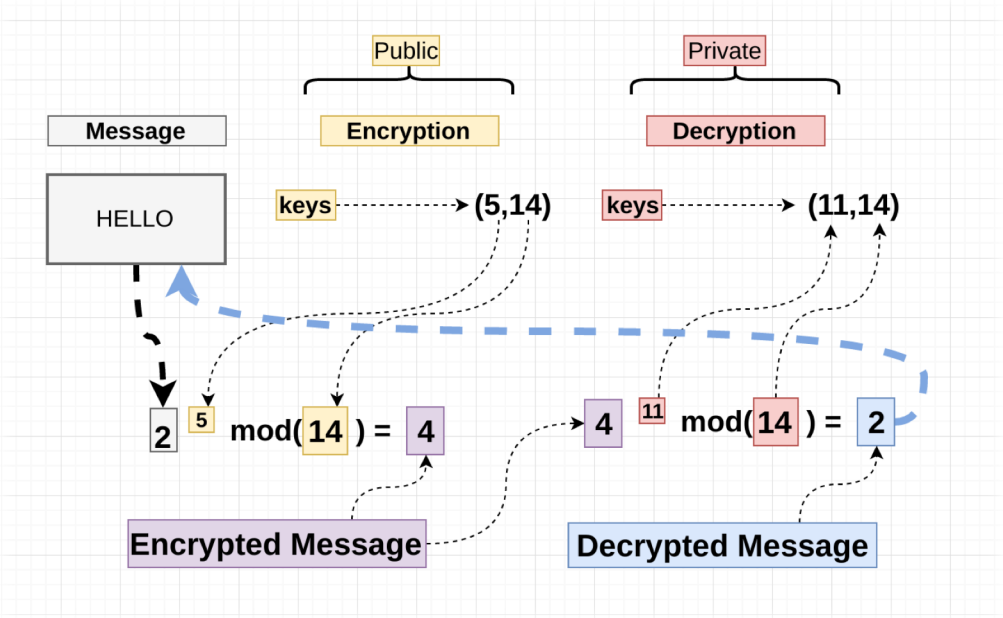
$g = n^{o1} \bmod o_2$

$g = 8^3 \bmod 15 = 512 \bmod 15 = 2$

Entschlüsseln:

$n = g^p \bmod o_2$

$n = 2^7 \bmod 15 = 128 \bmod 15 = 8$



Quelle: https://images.app.goo.gl/WfEcmjdzJBxNgHEe8

Sicherheit - Kompromittierung

- Verfahren wie RSA → sehr komplex bzw. verwenden hohe Zahlen als Schlüssel
  - Computer nicht in der Lage diese zu knacken

- Einfachere Verfahren wie die Cäsar-Verschlüsselung zum Teil sehr einfach zu knacken (= kompromittieren)

- Kompromittierung → mittels Brute-Force-Attacken (ständiges Ausprobieren) oder anderen Algorithmen