

Verschlüsselung

Verfahren damals und heute

Antike Techniken?

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

- **Steganographie**

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

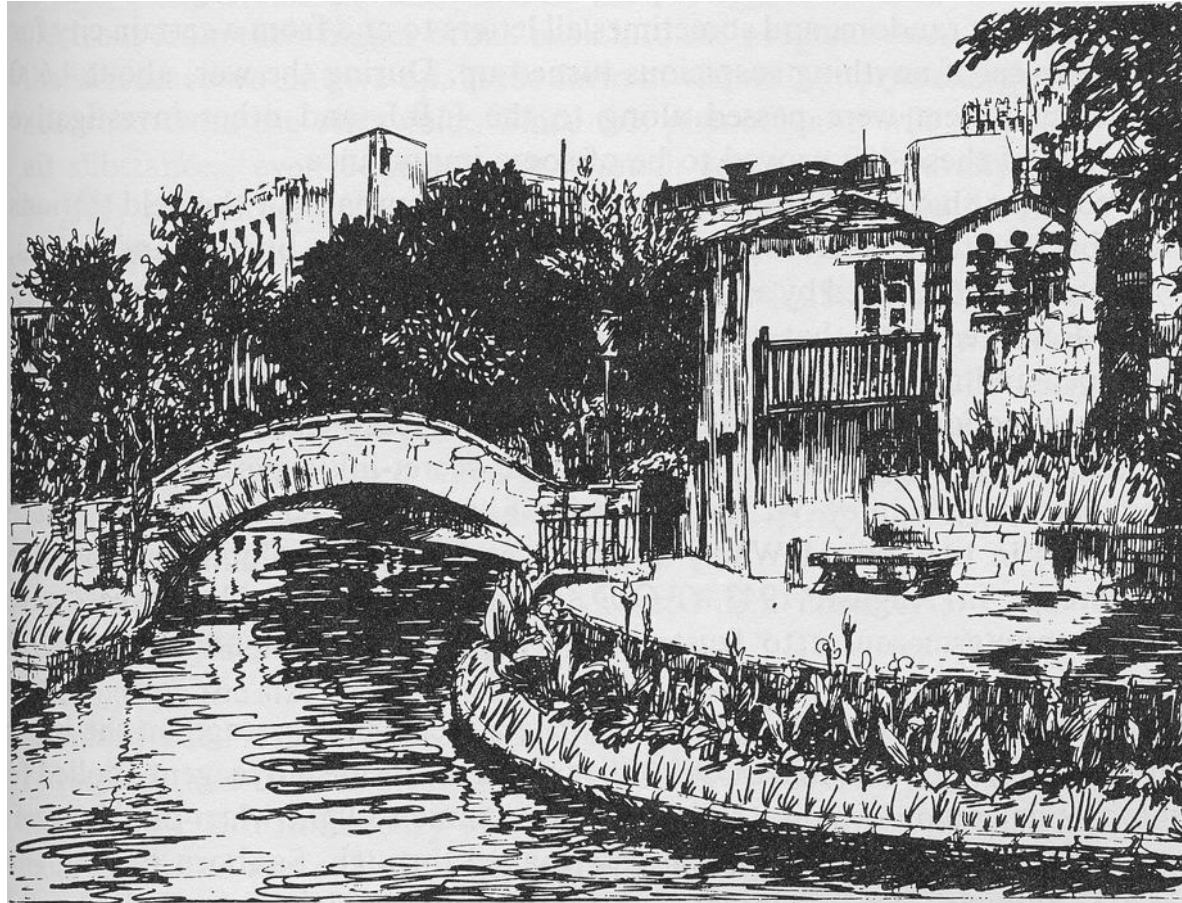


Quelle: <https://images.app.goo.gl/8LYPmZxxG2vD3HMZA>



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

Semagramme

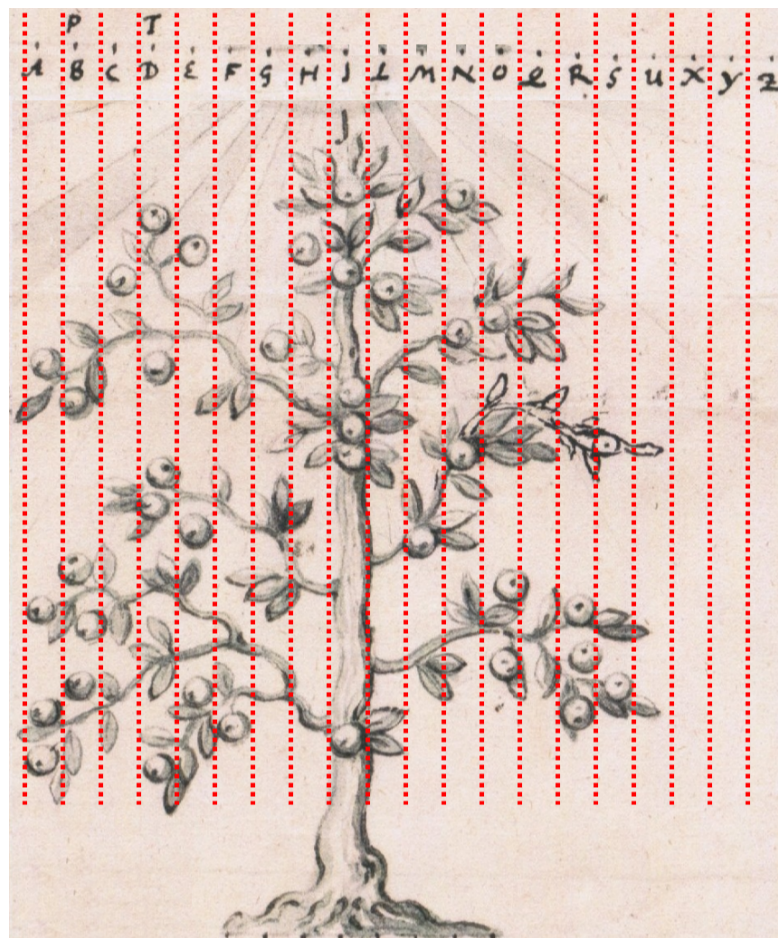


Quelle: <https://images.app.goo.gl/Rjx89RjJD7ReiSEF6>

Semagramme



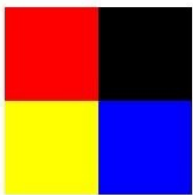
Quelle: <https://images.app.goo.gl/eybpaxbH5qlww1no6>



Quelle: <https://images.app.goo.gl/eybpaxbH5qlww1no6>

Steganographie – Digitale Bildformate

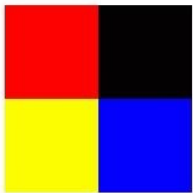
Original Image



11111111	00000000
00000000	00000000
00000000	00000000
11111111	00000000
11111111	00000000
00000000	11111111

Least Significant Bit Steganography

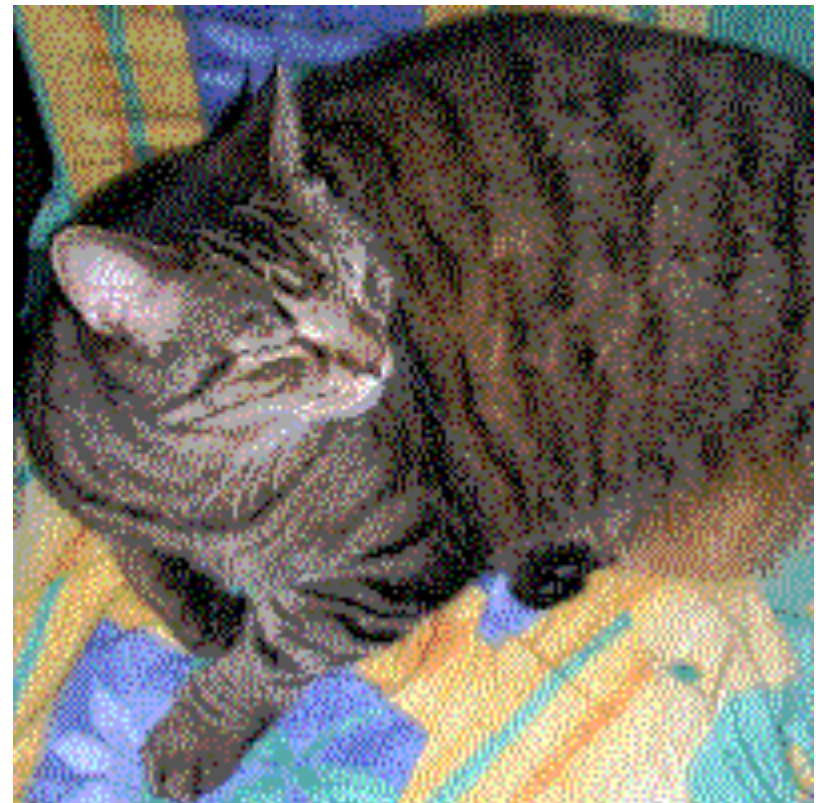
Stego Image



111111 01	000000 11
000000 10	000000 01
000000 00	000000 10
111111 00	000000 11
111111 01	000000 01
000000 01	111111 00

c **a** **t**
01 10 00 11 01 10 00 01 01 11 01 00

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

```
Terminal
File Edit View Terminal Tabs Help
root@blackslash:~# cd /root/stego
root@blackslash:~/stego# ls
secret.txt StegoCat.jpg StegoCat ORIGINAL.png
root@blackslash:~/stego# steghide --embed -ef secret.txt -cf StegoCat.jpg -e none -Z
Enter passphrase:
Re-Enter passphrase:
embedding "secret.txt" in "StegoCat.jpg"... done
root@blackslash:~/stego#
```

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

```
File Edit View Terminal Tabs Help
root@blackslash:~/stego# steghide --extract -sf stegoCat.jpg -xf extractSecret.txt
Enter passphrase:
wrote extracted data to "extractSecret.txt".
root@blackslash:~/stego# head extractSecret.txt
John,

If you want what you're looking for,
meet me at 2nd and Main at 9 PM tomorrow,
and come alone.

blackslash
root@blackslash:~/stego#
```

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 = $4 \cdot 10^{26}$ = 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:

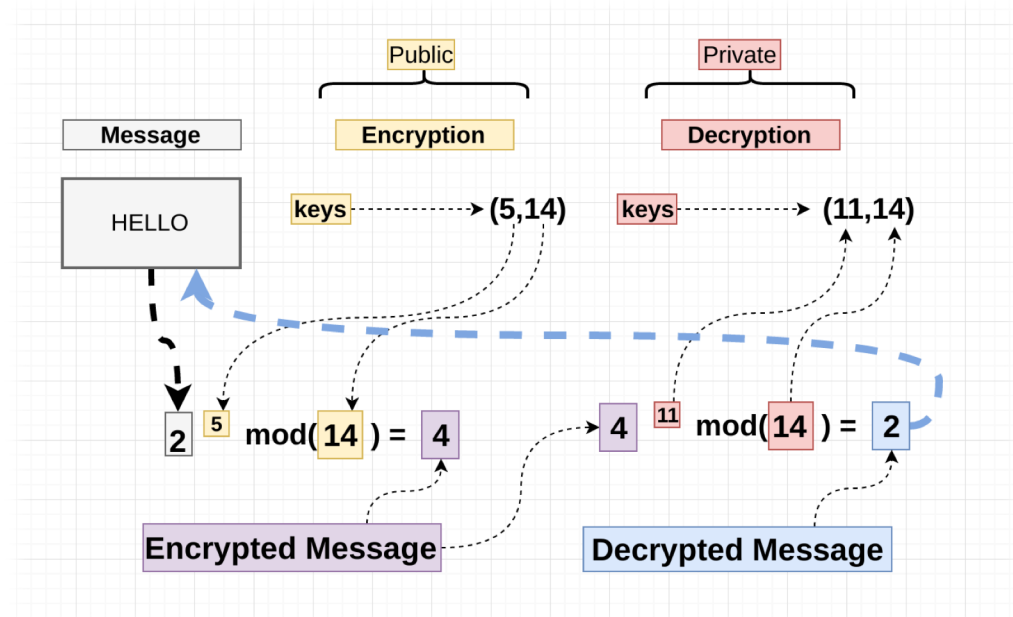
$p = 7$
 $o_1 = 3$
 $o_2 = 15$
 $n = 8$

Verschlüsseln:

$g = n^{o_1} \bmod o_2$
 $g = 8^3 \bmod 15 = 512 \bmod 15 = 2$

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