

Kryptographie entdecken

Alex Tray

Gruppe Cryptanalysis (MC O)

Vorlesungen:

Mathe Z - Wahrscheinlichkeit (2. Semester)

Kryptographie (5. Semester)

Kryptanalyse I und II (immer :))

Praktikum: bochum-challenge.es



Worst case:
You get free
pizza 🍕
Best case:
You find
your dream
job

Discover your possibilities at **STUDENT.CONNECT**
Wednesday, 4-6 PM, company presentations, networking & free food

Student.Connect
11.14-16

More info:
Google • Smart Mechatronics • Zolltron •
Materna • TÜV IT • CP Institute • Carbyto •
Finanz Informatik • dataglobal • G DATA •
WERK X



Was ist Kryptographie?

Verschlüsselung
(Vertraulichkeit)

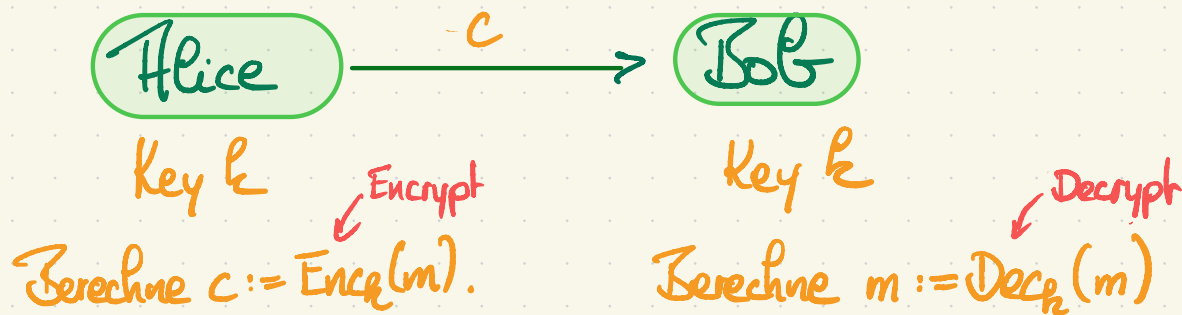
Authentisierung
(Zugangskontrolle)

Digitale Signaturen
(Authentizität
Nicht-Fälschbarkeit)

Krypto-Währungen
(Anonymität)

... und vieles mehr

Verschlüsselung



Beispiel: Cäsar-Chiffre (58 v. Chr.)

Key $k=3$

$m = \text{KRYPTO}$

Enc: Verschiebe um k nach vorne. $\text{Enc}_k(m) = \text{NUBSWR}$

Dec: Verschiebe um k nach hinten. $\text{Dec}_k(m) = \text{KRYPTO}$

Kodierung: Wie sage ich es meinem Rechner?

A	B	C	-----	Y	Z
↓	↓	↓		↓	↓
0	1	2		24	25

$Enc(m_0 \dots m_n)$

Rest bei Division durch 26

$(m_0 + k \bmod 26, \dots, m_n + k \bmod 26)$

$Dec(c_1 \dots c_n) =$

$(c_0 - k \bmod 26, \dots, c_n - k \bmod 26)$

Problem: Nur 26 Schlüssel.

K R Y P T O
↓
 $m = (10, 17, 24, 15, 19, 14)$
↓ Enc_3
 $(13, 20, \cancel{27}_1, 18, 22, 17)$
N U B S W R
↓ Dec_3
 $(10, 17, \cancel{-2}_{24}, 15, 19, 14)$
K R Y P T O

Permutationsschiffre (auch: Substitutionsschiffre)

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
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
T	C	D	E	A	S	Q	R	B	U	V	P	H	G	I	O	F	W	L	K	J	Y	Z	H	N	X

K R Y P T O

↓ Enc

V W N O K I

Schlüssel: $26 \cdot 25 \cdot 24 \cdot \dots \cdot 1 = 26! \approx 2^{88.4}$

Zum Vergleich: $2^{91.6}$ Hash-Berechnungen für Bitcoin 2025 (17 Milliarden €)

Frage: Warum ist die Permutationsschiffre trotzdem unsicher?

Vigenère - (16. Jhd) und One-Time-Pad (1882) Verschlüsselung

Schlüssel: $k = (k_0, k_1, k_2) = (1, 25, 2)$

$$\text{Enc}(m_i) = m_i + k_{i \bmod 3} \bmod 26, i = 0, \dots, n$$

K	R	Y	P	T	O
$\downarrow k_0=1$	$\downarrow k_1=25$	$\downarrow k_2=2$	$\downarrow k_0=1$	$\downarrow k_1=25$	$\downarrow k_2=2$
L	Q	H	Q	S	Q

Schlüssel: 26^l für Schlüssellänge l

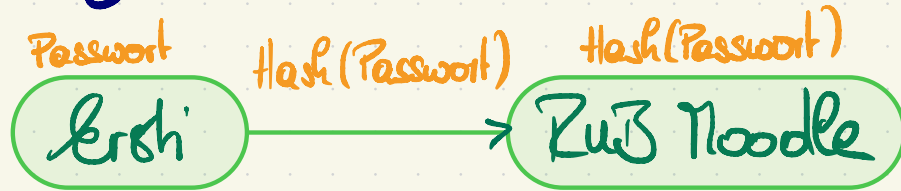
Spezialfall: $m = (m_0 \dots m_n), k = (k_0 \dots k_n)$
One Time Pad

Entschlüsselung:

L	Q	H	Q	S	Q
$\downarrow 1$	$\downarrow 25$	$\downarrow 2$	$\downarrow 1$	$\downarrow 25$	$\downarrow 2$
K	R	Y	P	T	O

L	Q	H	Q	S	Q
$\downarrow 20$	$\downarrow 12$	$\downarrow 0$	$\downarrow 5$	$\downarrow 7$	$\downarrow 18$
R	E	H	L	L	Y

Authentisierung (Nachweis der Identität)



Hash : beliebiger String $\rightarrow \{0, 1\}^{256}$

Eigenschaften : Leicht zu berechnen, schwer zu invertieren.
Hashwert sieht „zufällig“ aus.

Secure Hash Algorithm Bitlänge

SHA - 256 (KRYPTO):

75a7cc49 c9dd9 (256 Bit = 64 Hex-Zeichen)

Prinzip von Bitcoin

Gegeben : Nachricht m von verschiedenen Transaktionen (Block)

Gesucht : r , so dass $\text{Hash}(m, r) = 0^{19} \{0, 1, \dots, f\}^{45}$

Mining algo

REPEAT

Wähle beliebiges r .

UNTIL $\text{Hash}(m, r)$ beginnt mit 19 Nullen.

Laufzeit : Erwartet $(2^4)^{19} = 2^{76}$ Hash-Auswertungen.

Block Reward : 3,125 BTC (231.000 €)