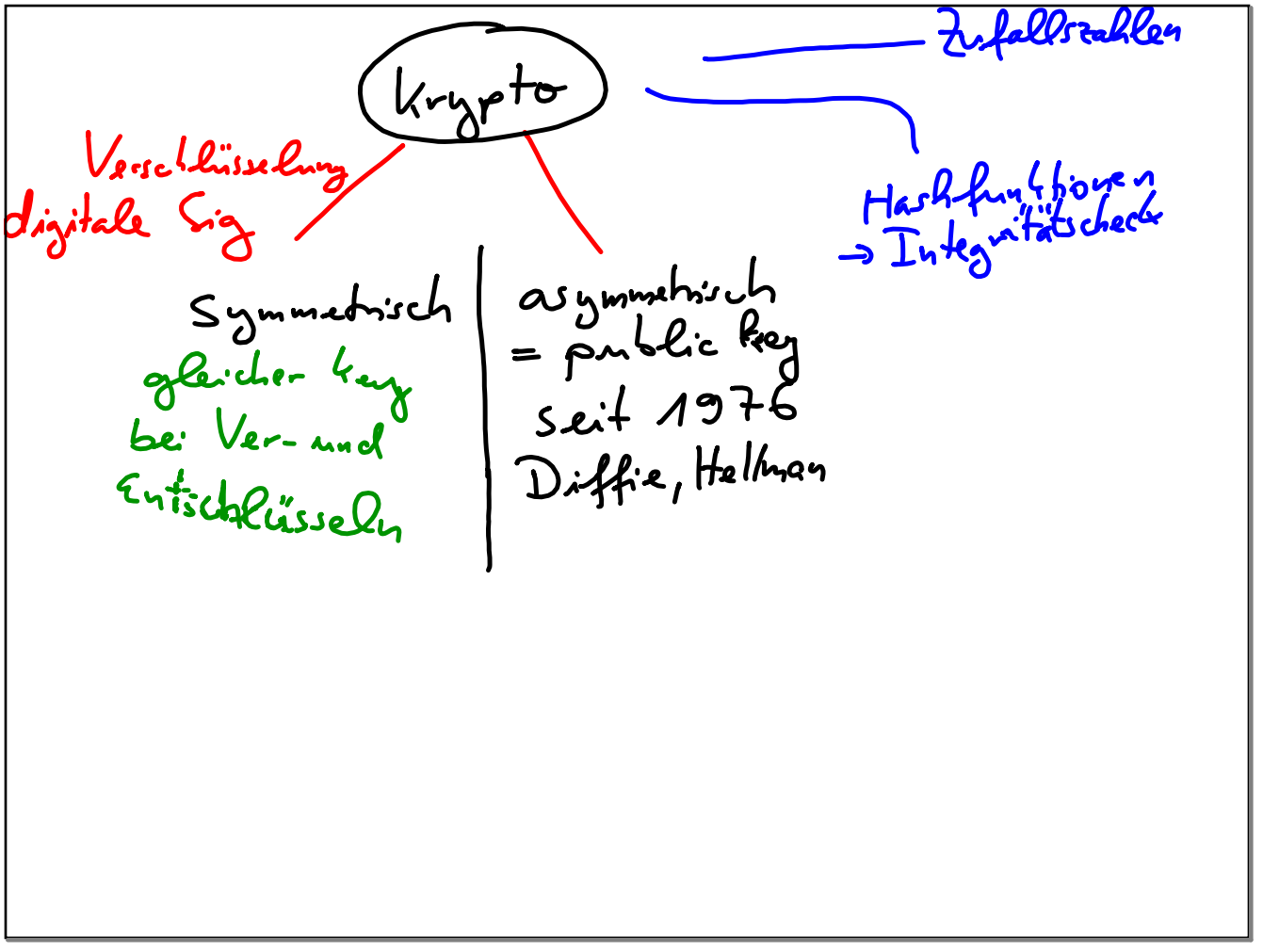
Cryptography Engineering

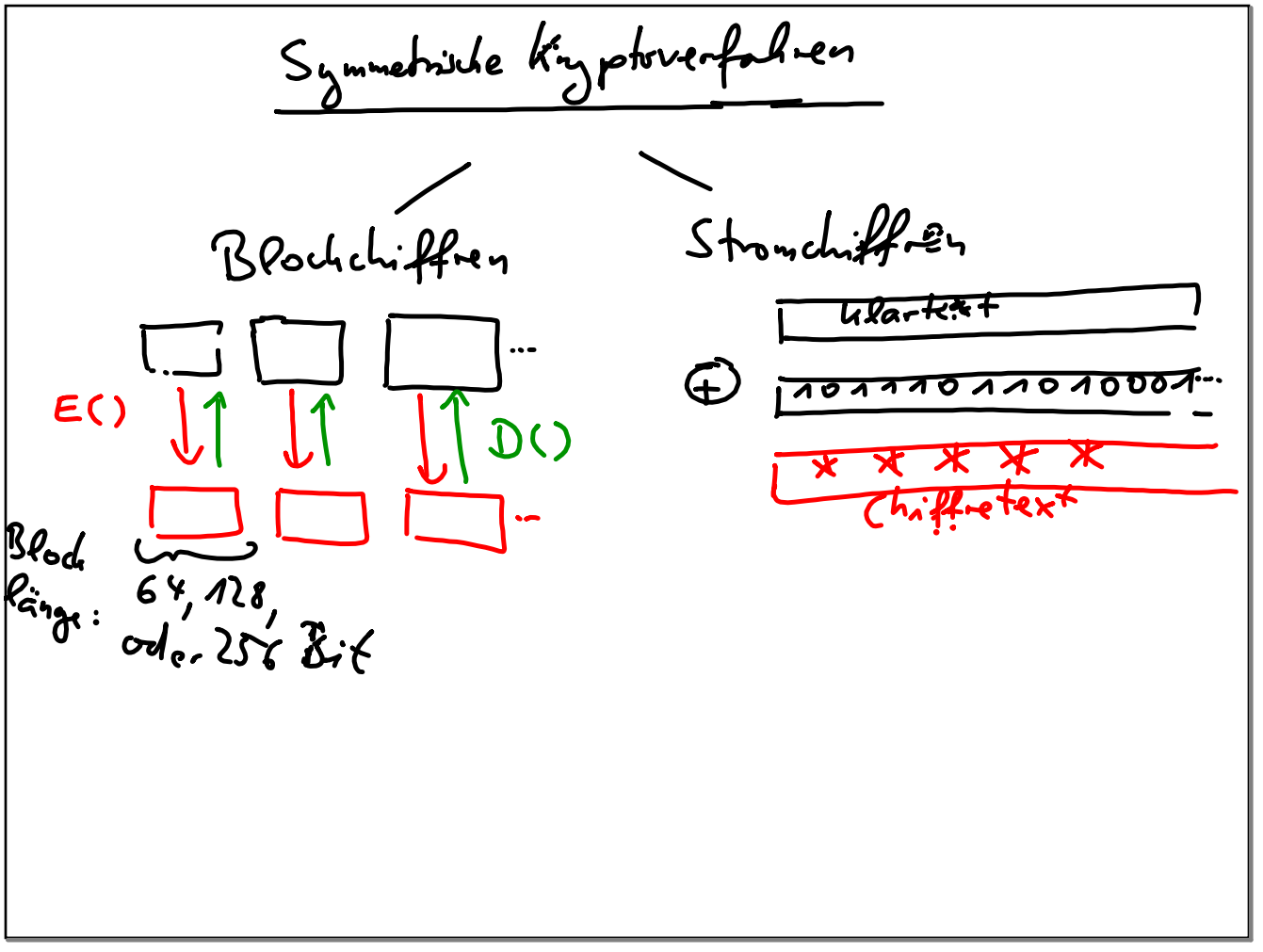
(Sicherheit und Kryptographie)

www-crypto → Registrierung

Übungen, u.a. Implementierung

openssl, PARI/gp


Krypto
Zufallszahlen
Verschlüsselung
digitale Sig
Hashfunktionen
→ Integritätscheck
Symmetrisch
gleicher Key
bei Ver- und
Entschlüsseln
asymmetrisch
= public key
seit 1976
Diffie, Hellman


Symmetrische Kryptoverfahren
Blockchiffren
Stromchiffren
E()
D()
Block
Länge:
64, 128,
oder 256 Bit
Klartext
Chiffretext

Stromchiffren:

$x\bar{y} \vee \bar{x}y$

$\oplus$	x	y	$x \oplus y$
	0	0	0
	0	1	1
	1	0	1
	1	1	0

Message m
ciphertext c
key k

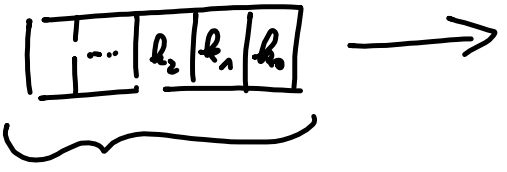
$m \oplus k = c$

$m \oplus k \oplus k = c \oplus k$

$m \oplus 0 = m$

Achtung:

$c \oplus m = k$



Startzustand = geheimer Schlüssel K

Keystream möglicherweise erst ab späterer Stelle verwendet

RC4: erste 1024 Bits nicht verwenden

heute genere!?D unsicher

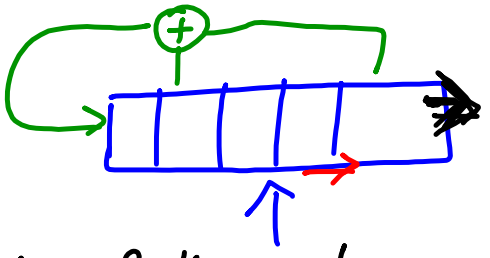
verwendbare Stromchiffren:

ESTREAM-Projekt

2.B.

Trivium

Grain v1



LFSR = linear. feedback shift register

linear: lineare Gleichungen

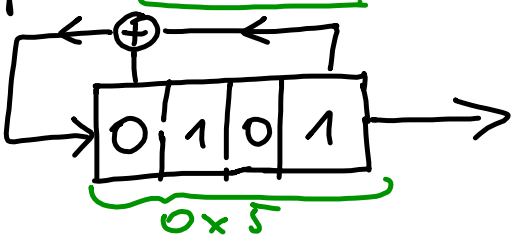
$x_1 \oplus x_2 \oplus x_3$

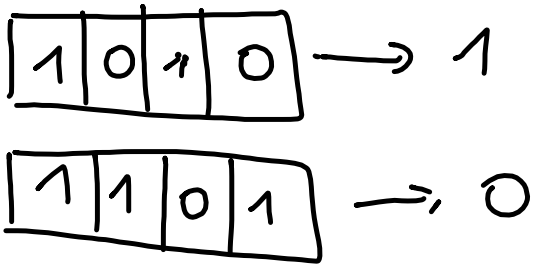
Grad 1

nicht $x_1 x_2 \oplus x_3$

Grad 2

Beispiel: 1 0 0 1 → 0x9



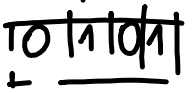


Übung:
wann Anfangszustand wieder erreicht?

15 Werte

1 0 1 0 1 1 0 0

1 0 0 1 1 1 1



$2^n - 1$ Werte bis periodisch

ist Idealfall?

Übung: LFSR - Implementierung

Format: hexadezimal für Design / Startzustand des LFSR

Stromchiffre : n LFSRs + Nichtlinearität