



Kryptographie für CTFs

Eine Einführung

KITCTF



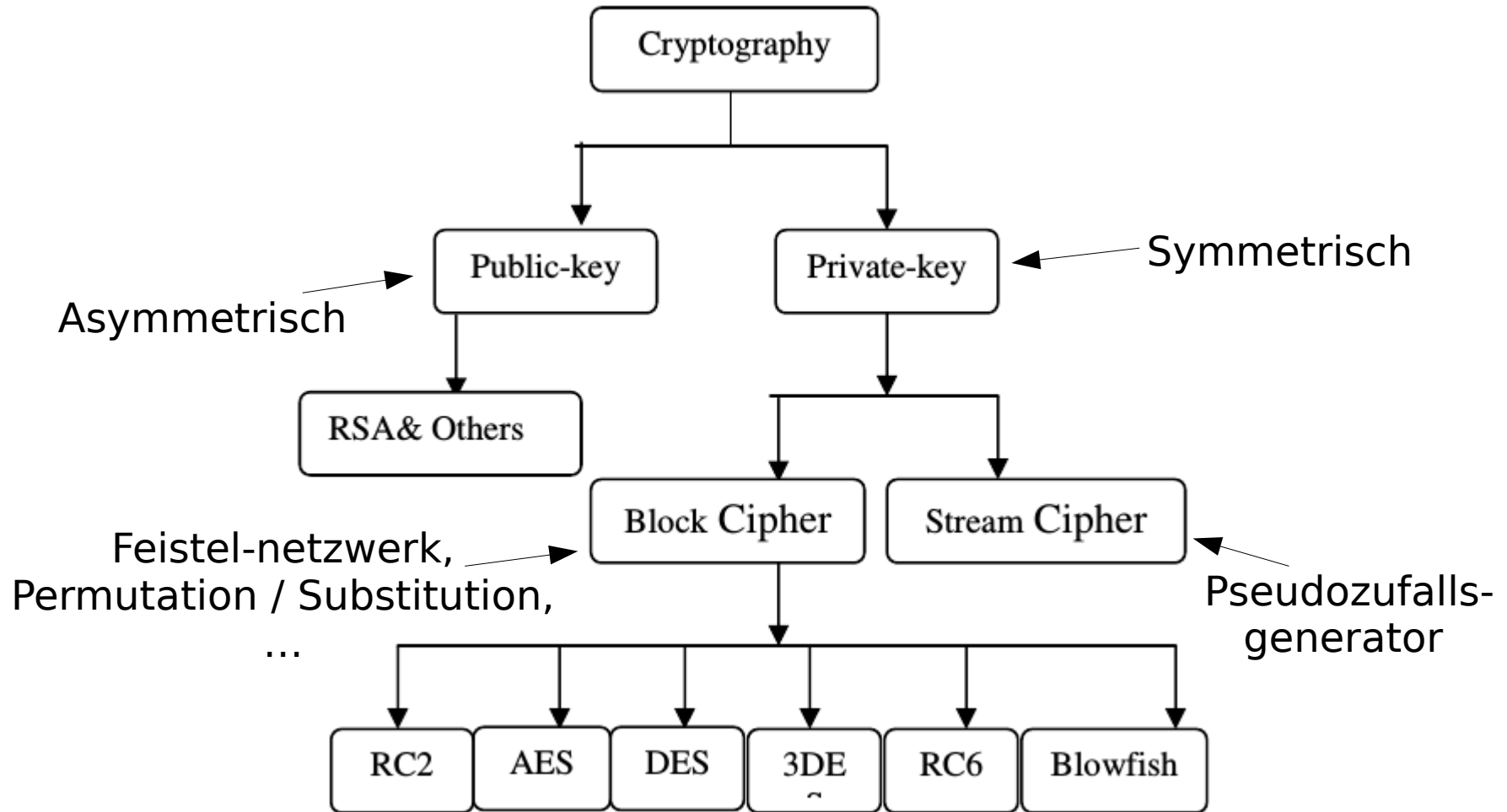
Einführung



“Cryptography is the practice and study of techniques for secure communication in the presence of third parties.” Wikipedia

- Nicht Wissenschaftlich
 - Dafür Vorlesungen und Praktika aus „Kryptographie und Sicherheit“
- Die Grundlagen für CTF-Anfänger

Übersicht — Erste Dimension



Übersicht — Zweite Dimension



- **Verschlüsselung**
- **Authentifizierung („Echtheit“)**

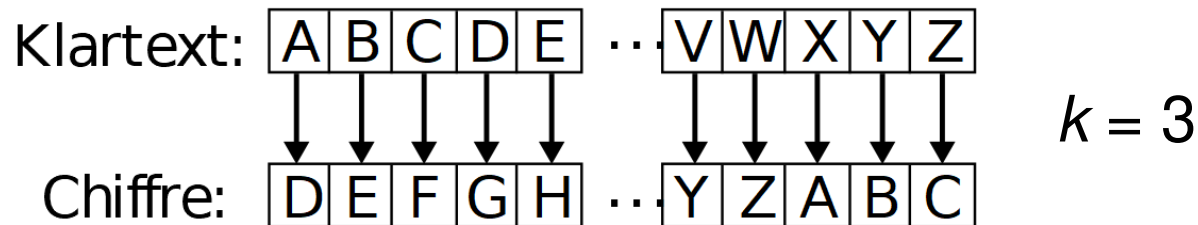
- **Hash-Funktionen**
- **Pseudozufallsgeneratoren**
- **Proof-of-Knowledge**
- **Commitments**
- **...**



Klassiker

■ Caesar-Chiffre

- Jeder Buchstabe wird um festen Wert k verschoben



- Brechen durch ausprobieren oder durch Häufigkeitsanalysen einfach möglich
- Wird heutzutage immer noch verwendet (spiegel.de Paywall)
- Beispiel für **Substitution**



www.spiegel.de/politik/ausland/donald-trump-hotels-mitarbeiter-werfen-trump

Donald Trump: Hotels-Mitarbeiter werfen Trump Ausbeutung vor - SPIEGEL ONLINE

Präsident, der nebenbei eine Hotelkette besitzt.

Da drängen sich natürlich einige Fragen auf: Was passiert eigentlich in einem Trump-Hotel? Und: Wie ist Trump so als Chef?

Lvs{fs Dfdl.jo- efs Nboo bn Fnqgboh jtu tfis gsfvoemjdi/ #Bi- Hfsnboz/ Jtu ebt Jis fstufs Cftvdi@# Kb/ Ft hjcu fjo Vqhsbef- fjof Kvojps.Tvjuf/

Jn [jnnfs- ebt esbvof Tpgb xjslu fuxbt behfovu{u/ Tpotu bmmft ubefmmt/ Bnfsjlbojtdif Gýog.Tufsof.Cfibhmjdilfju/ Ebt Epqqfmcfuu xâsf bvdi gýs wjfs Qfstpofo hffjhofu/ Ejf Lmjnbombhf tufiu bvg efs Fjotufmmvoh; Hfgsjfstdisbol/

Usvnq jtu jn [jnnfs ýcfsbmm/ Fs wfsgpmhu efo Hbtu ejt voufs ejf Evtdif/ Ft hjcu Usvnq.Tibnqpp voe Usvnq.Tfjgf/ Bvg efn Obdiuujtdi Usvnq.Opuj{{fuufm voe fjo Usvnq.Tujgu/ Fs gvolujpojfsu ojdiu/

Ebt Chef{jnnfs jtu sjftjh/ Nbo lboo jo efs Xboof tju{fo voe bvg ejf Xýtuf hvdlfo/ Jo efo Tqjfhfm jtu fjo Gfsotfifs fjohfmbttfo´ ft måvgu DOO/ Voe bvdi eb; Usvnq/ Xbt tpotu@

[vsýdl jo ejf Mpccz/ Ejsflu ofcfo efo Gbistuýmfo mjfhu efs Usvnq.Tipq/ Efo hjcu ft jo bmm tfjofo Ipufmt/ Ijfs jo Mbt Wfhbt nvt kfehs Hbtu ebsbo wpscjf/ Efs Mbefo jtu hvu cftvdiu/ Ft hjcu Usvnq.Nýu{fo gýs 41 Epmmbs- Usvnq.Xfjo gýs 76 Epmmbs ejf Gmbtdif- Usvnq.Tdiplmbef- obuýmjdi bmmf Usvnq.Cýdifs voe fjo hpmeft Usvnq.Tqbstdixfjo/ Ft jtu bvt Qmbtujl voe lptufu 21 Epmmbs/

Hbssz- Hftdiágutnboo bvt Dijdbhp- xpiou hsof jn Usvnq.Ipufm xfoo fs jo Mbt Wfhbt jtu/ [xfj Nbm jn Kbis lpnnu fs jo ejf Xýtufotubeu voe tqjfm Qplfs/ Ft tfj ebt cftuf Ipufm efs Tubeu- gjoefu Hbssz/

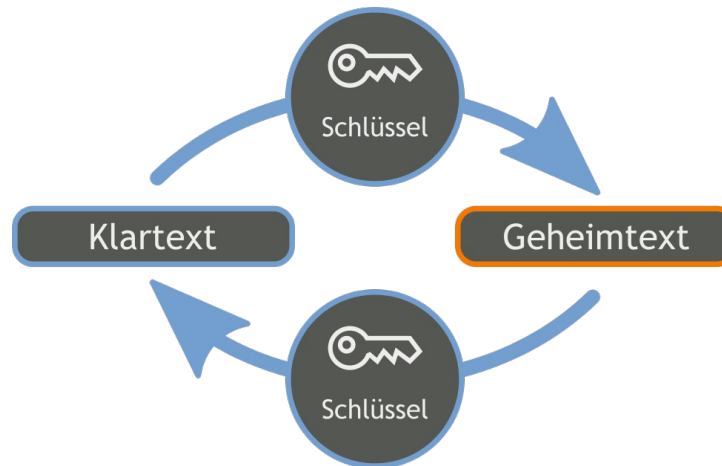
■ Vigenère-Chiffre

- Wähle Schlüsselwort und verschiebe jeden Buchstaben entsprechend dem Schlüsselbuchstaben

Klartext Nachricht:	W	H	I	T	E	H	A	T	B	L	A	C	K	H	A	T
Schlüssel:	S	E	C	U	R	I	T	Y	S	E	C	U	R	I	T	Y
Chiffretext:	O	L	K	N	V	P	T	R	T	P	C	W	B	P	T	R

- Schlüssellänge bestimmen und dann Caesar-Chiffre für jede Schlüsselposition einzeln brechen
- Noch ein Beispiel für **Substitution**

Symmetrische Verschlüsselungen



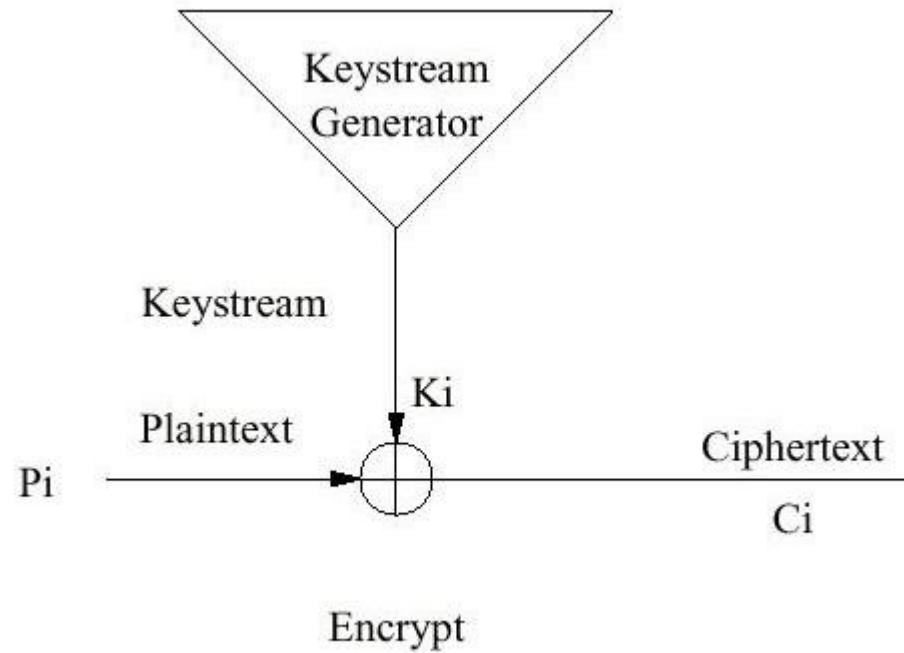
■ Blockchiffren

- Verschlüsselt Blöcke fester Länge
- Betriebsmodus wird zur Verschlüsselung längerer Daten verwendet

■ Stromchiffren

- Pseudozufälliger Schlüsselstrom wird aus Schlüssel abgeleitet
- Schlüsselstrom wird mit Klartext kombiniert

Stromchiffren



Stromchiffren



- RC4, SEAL, Salsa20, CryptMT, ...

- **Mögliche Angriffe:**

- Bekannter Klartext:

Aus einem bekannten Klartext m mit passendem Chifftrat c kann der Schlüsselstrom K rekonstruiert werden

$$K = m \oplus c$$

- Key-Reuse:

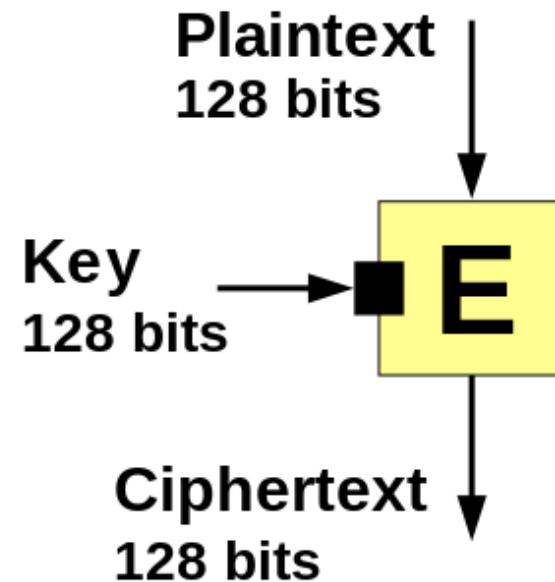
Sind c_1 und c_2 mit dem gleichen Schlüssel verschlüsselt worden, dann kann man $m_1 \oplus m_2$ wie folgt berechnen.

$$c_1 \oplus c_2 = m_1 \oplus m_2$$



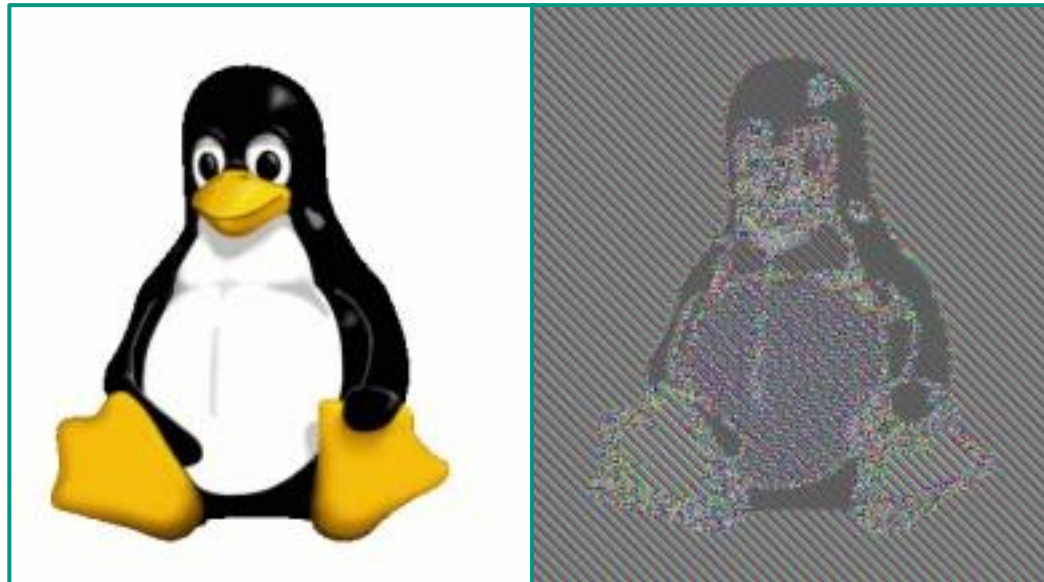
Blockchiffren

- DES, IDEA, RC5, AES, Blowfish, ...
- Block- und Schlüssellänge
- Padding: Erweitern der Nachricht auf Blocklänge
- Betriebsmodi
 - Electronic Code Book (ECB)
 - Cipher Block Chaining (CBC)
 - Counter Mode (CTR)
 - ...



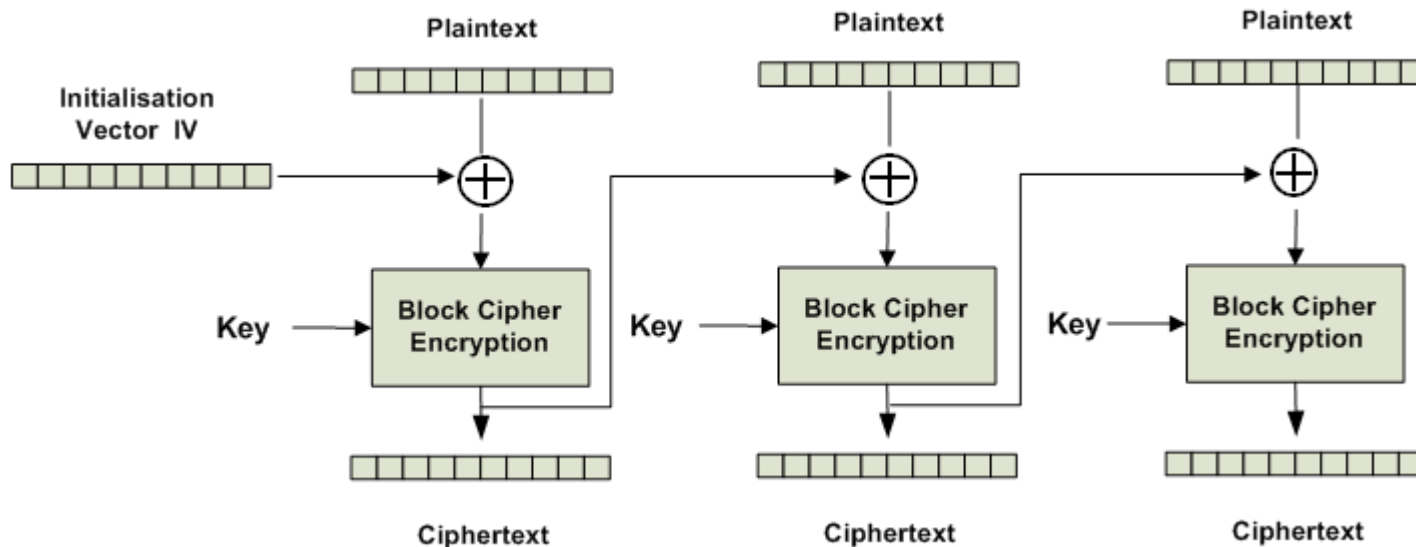
Electronic Code Book

- Verschlüsse jeden Block einzeln
- **Probleme:**
 - Dateneinfügen möglich
 - Deterministisch



Cipher Block Chaining

- Verschlüsseln: $Enc(\text{Block XOR dem vorigen Chifftrat-Block})$
- Entschlüsseln: $Dec(\text{Chifftrat-Block}) \text{ XOR vorigem Chifftrat-Block}$
- Initialisierungsvektor zufällig
- **Probleme:**
 - Verlust eines Chifftrat-Blocks führt zu Verlust 2er Klartextblöcke





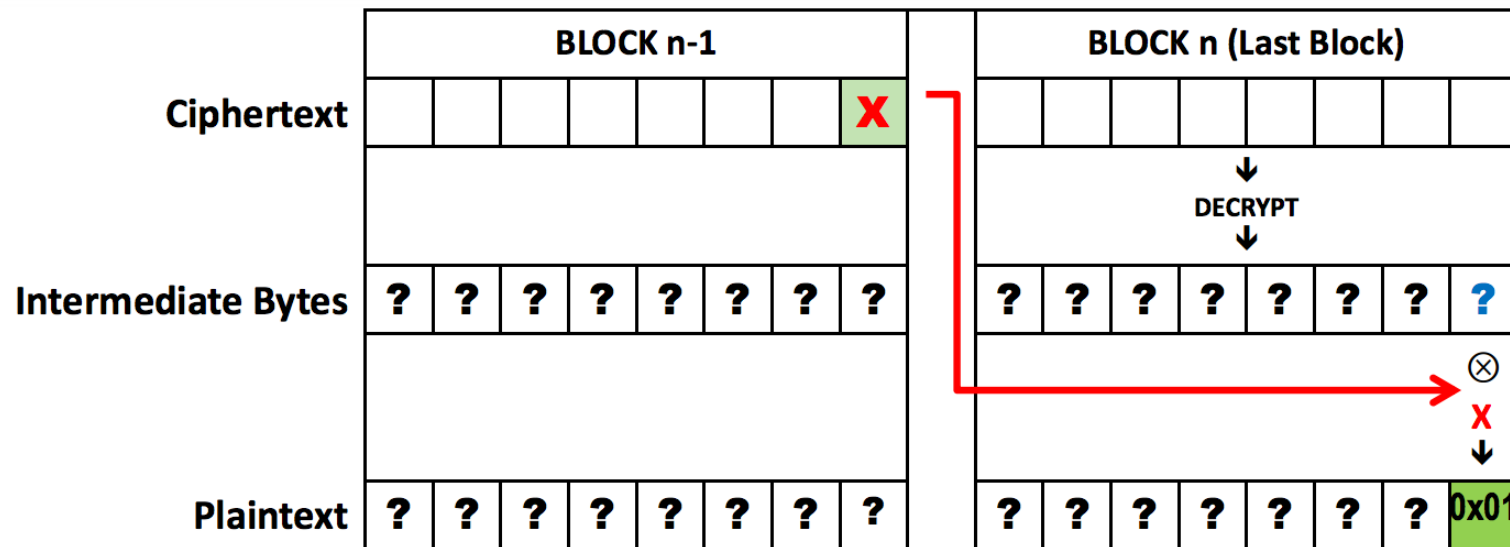
CBC Padding Oracle

- Padding: Klartext wird auf Blocklänge aufgefüllt.
- Bsp.: PKCS#7 x Byte fehlen zum vollen Block. Fülle jedes der Bytes mit dem Wert x .

	BLOCK #1								BLOCK #2							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
Ex 1	F	I	G													
Ex 1 (Padded)	F	I	G	0x05	0x05	0x05	0x05	0x05								
Ex 2	B	A	N	A	N	A										
Ex 2 (Padded)	B	A	N	A	N	A	0x02	0x02								
Ex 3	A	V	O	C	A	D	O									
Ex 3 (Padded)	A	V	O	C	A	D	O	0x01								
Ex 4	P	L	A	N	T	A	I	N								
Ex 4 (Padded)	P	L	A	N	T	A	I	N	0x08	0x08	0x08	0x08	0x08	0x08	0x08	0x08
Ex 5	P	A	S	S	I	O	N	F	R	U	I	T				
Ex 5 (Padded)	P	A	S	S	I	O	N	F	R	U	I	T	0x04	0x04	0x04	0x04

CBC Padding Oracle

- Über Änderung am vorletzten Block lässt sich über das Paddingorakel der letzte Block komplett bestimmen

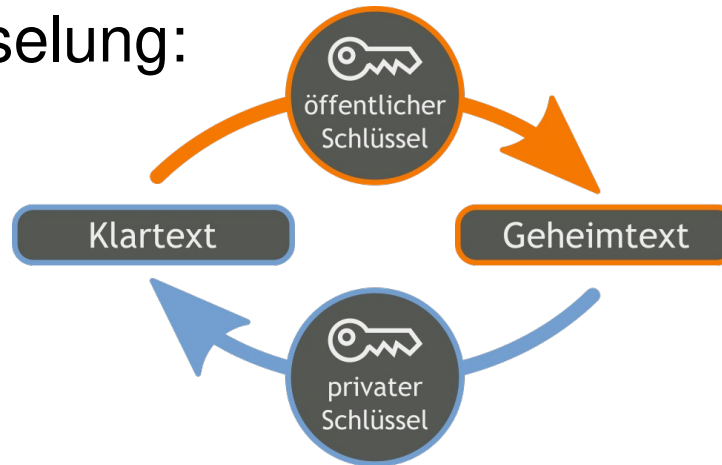


$$? \wedge X = 0x01$$

$$? = 0x01 \wedge X$$

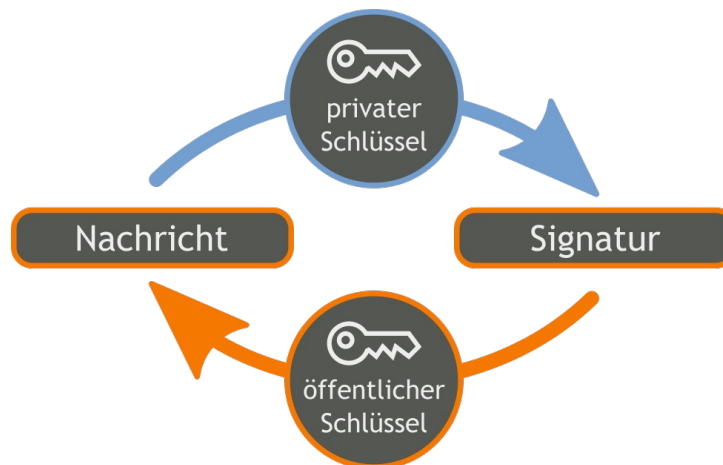
Asymmetrische Kryptosysteme

■ Verschlüsselung:



- RSA
- Elgamal
- McEliece
- ...

■ Signatur:



- RSA
- Elgamal
- DSA
- ...

RSA



- Wähle zwei Primzahlen p und q
- Bestimme $N = p \cdot q$
- Bestimme $\phi(N) = (p - 1) \cdot (q - 1)$
- Wähle e so, dass $ggT(e, \phi(N)) = 1 \wedge 1 < e < \phi(N)$ gilt
- Bestimme d so, dass $e \cdot d \equiv 1 \pmod{\phi(N)}$ gilt. (erweiterter euklidischer Algorithmus)

- Öffentlicher Schlüssel: N, e
- Privater Schlüssel: d

- $ggT(a, b)$: Größter gemeinsamer Teiler von a und b
- $\phi(n) = |\{a \in \mathbb{N} \mid 1 \leq a \leq n \wedge ggT(a, n) = 1\}|$
Anzahl aller Zahlen, die zu n teilerfremd sind. (eulersche Funktion)

RSA



■ Encryption:

$$c = m^e \bmod N$$

■ Decryption:

$$c^d \bmod N$$

$\Leftrightarrow m^{ed} \bmod N$, mit dem [kleinen fermatschen Satz](#)

$$\Leftrightarrow m^{ed \bmod \phi(N)} \bmod N$$

$$\Leftrightarrow m^1 \bmod N$$

(Mit $m < N$)

■ Holomorphie:

$c_1 = m_1^e \bmod N$ und $c_2 = m_2^e \bmod N$, so gilt

$$c_1 \cdot c_2 = m_1^e \cdot m_2^e \bmod N = (m_1 \cdot m_2)^e \bmod N.$$

Es gilt also $\text{Enc}(m_1, pk) \cdot \text{Enc}(m_2, pk) = \text{Enc}(m_1 \cdot m_2, pk)$

Angriffe auf RSA



Bedingung	Angriff	Komplexität
Keine	Faktorisierung	$\exp(\log(N)^{1/3}) \log \log(N)^{2/3}$
Kleines d	Wiener's Attack	Polynomiell
$m < N^{1/4}$	Wurzel ziehen	Polynomiell
Senden der gleichen Nachricht an viele Empfänger mit selben	Håstad's broadcast attack	Polynomiell

Und viele mehr!

Danke



- Leonard Schönborn für die Folien
- Stefan fürs Organisieren der Folien

Aufgaben



- ctf.bplaced.net (Crypto 20 + Crypto 30)
- [Picoctf.com](https://picoctf.com)
- cryptopals.com
- overthewire.org/wargames/krypton