Kryptographie für CTFs

Eine Einführung

KITCTF

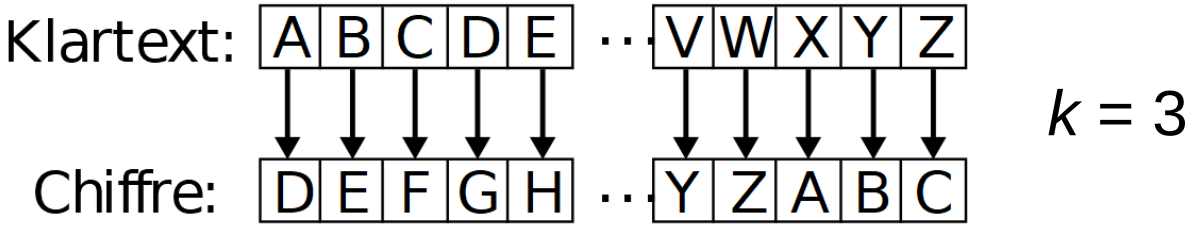
Einführung

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

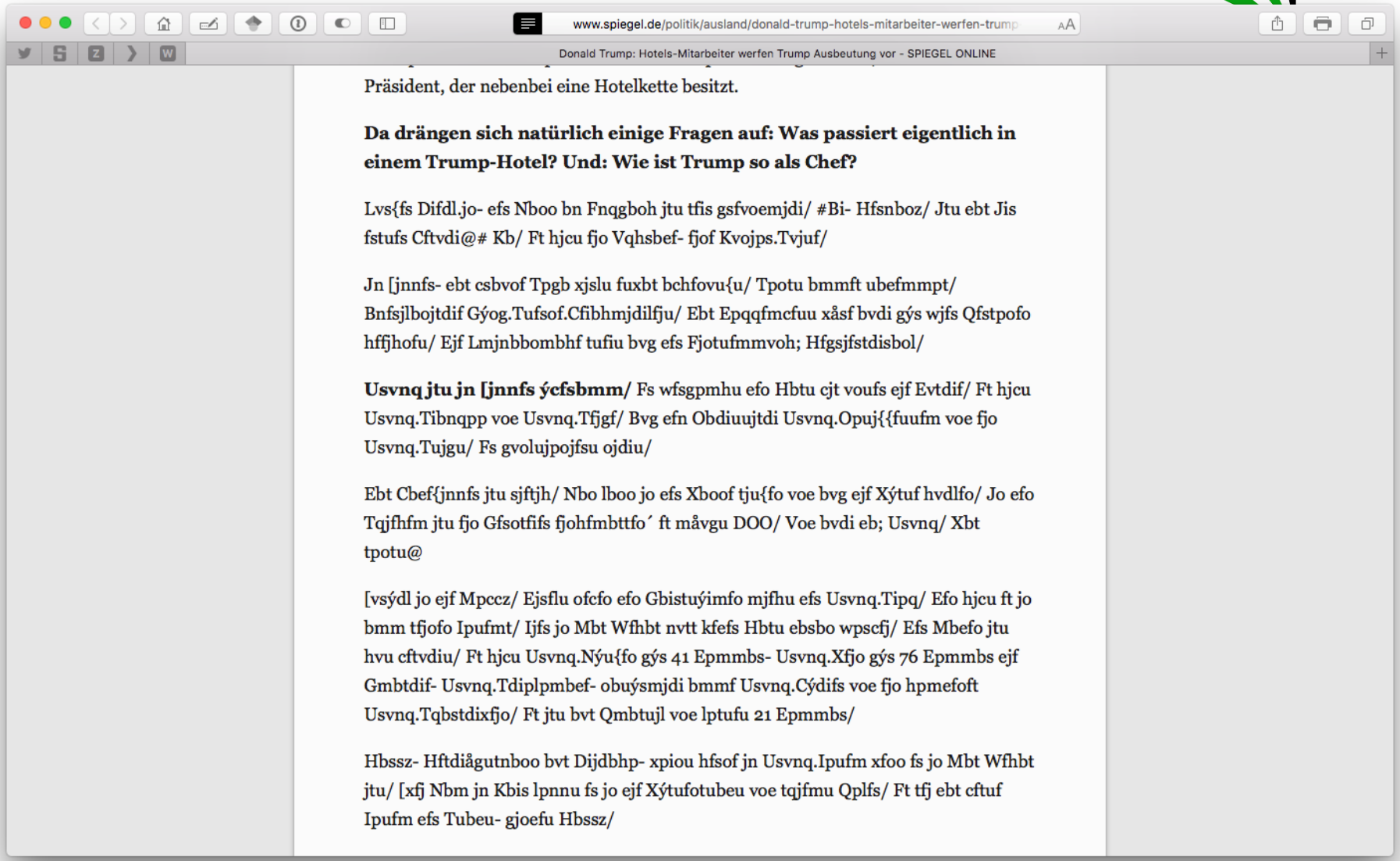
- Nicht Wissenschaftlich
  - Dafür Vorlesungen und Praktika aus „Kryptographie und Sicherheit“
- Die Grundlagen für CTF-Anfänger

Klassiker

- **Caesar-Chiffre**
  - Jeder Buchstabe wird um festen Werk *k* verschoben

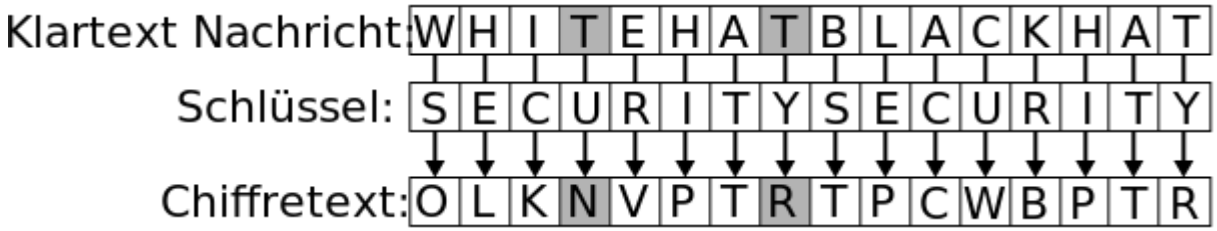


  - Brechen durch ausprobieren oder durch Häufigkeitsanalysen einfach möglich
  - Wird heutzutage immer noch verwendet (spiegel.de Paywall)


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 Difdl.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 csbvof Tpgb xjslu fuxbt bchfovu{u/ Tpotu bmmft ubefmmpt/ Bnfsjlbojtdif Gýog.Tufsof.Cfibhmjdilfju/ Ebt Epqqfmcfuu xåsf bvdi gýs wjfs Qfstpofo hffjhofu/ Ejf Lmjnbbombhf tufiu bvg efs Fjotufmmvoh; Hfgsjfstdisbol/
Usvnq jtu jn [jnnfs ýcfsbmm/ Fs wfsgpmhu efo Hbtu cjt voufs ejf Evtdif/ Ft hjcu Usvnq.Tibnqpp voe Usvnq.Tfjgf/ Bvg efn Obdiuujtdi Usvnq.Opuj{{fuufm voe fjo Usvnq.Tujgu/ Fs gvolujpojfsu ojdiu/
Ebt Cbef{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 Gbistuýimfo mjfhu efs Usvnq.Tipq/ Efo hjcu ft jo bmm tfjofo Ipufmt/ Ijfs jo Mbt Wfhbt nvtt kfefs Hbtu ebsbo wpscfj/ Efs Mbefo jtu hvu cftvdiu/ Ft hjcu Usvnq.Nýu{fo gýs 41 Epmmbs- Usvnq.Xfjo gýs 76 Epmmbs ejf Gmbtdif- Usvnq.Tdiplpmbef- obuýsmjdi bmmf Usvnq.Cýdifs voe fjo hpmefoft Usvnq.Tqbstdixfjo/ Ft jtu bvt Qmbtujl voe lptufu 21 Epmmbs/
Hbssz- Hftdiågutnboo bvt Dijdbhp- xpiou hfsof jn Usvnq.Ipufm xfoo fs jo Mbt Wfhbt jtu/ [xj Nbm jn Kbis lpnnu fs jo ejf Xýtufotubeu voe tqjfmu Qplfs/ Ft tfj ebt cftuf Ipufm efs Tubeu- gjoefu Hbssz/

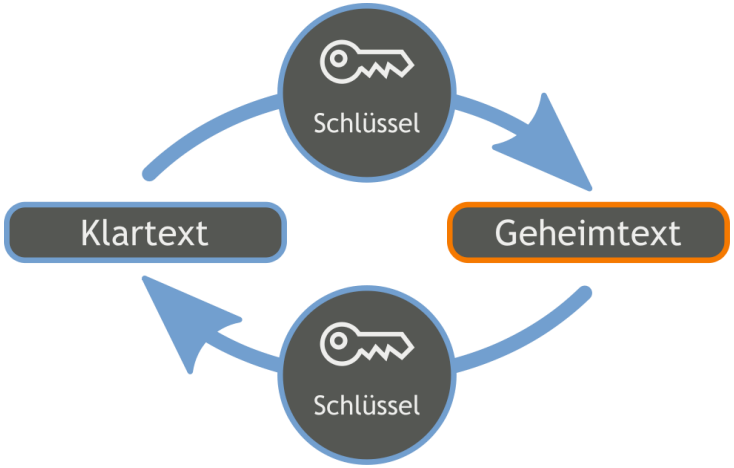
Klassiker

- **Vigenère-Chiffre**
  - Wähle Schlüsselwort und verschiebe jeden Buchstaben entsprechend dem Schlüsselbuchstaben



  - Schlüssellänge bestimmen und dann Caesar-Chiffre für jede Schlüsselposition einzeln brechen

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

- RC4, SEAL, Salsa20, CryptMT, …

- **Mögliche Angriffe:**
  - Bekannter Klartext:

    Aus einem bekannten Klartext m mit passendem Chiffrat 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.

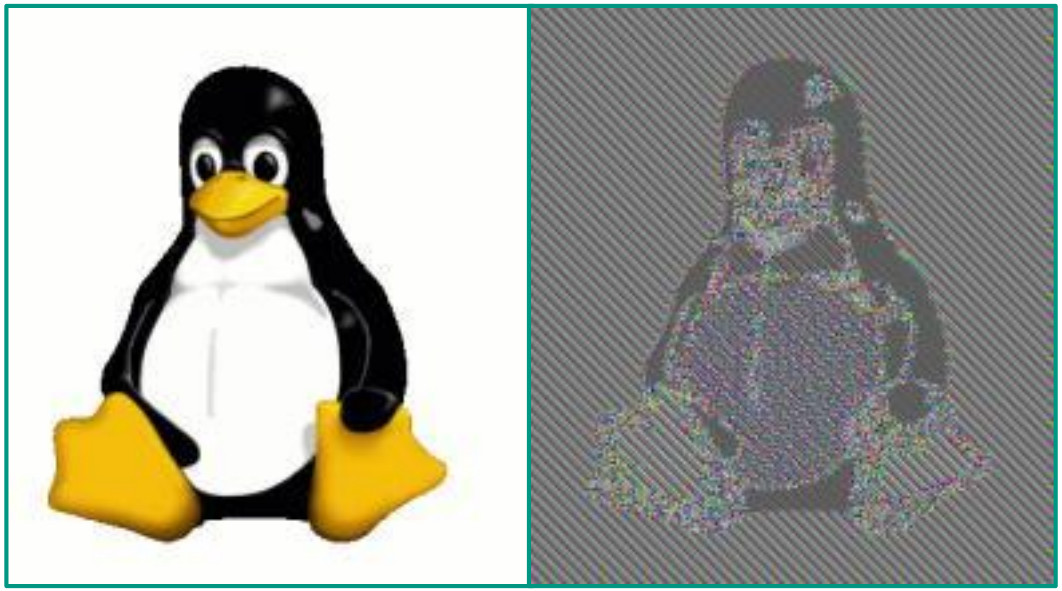
    $c_1 \oplus c_2 = m_1 \oplus m_2$

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)
  - ...

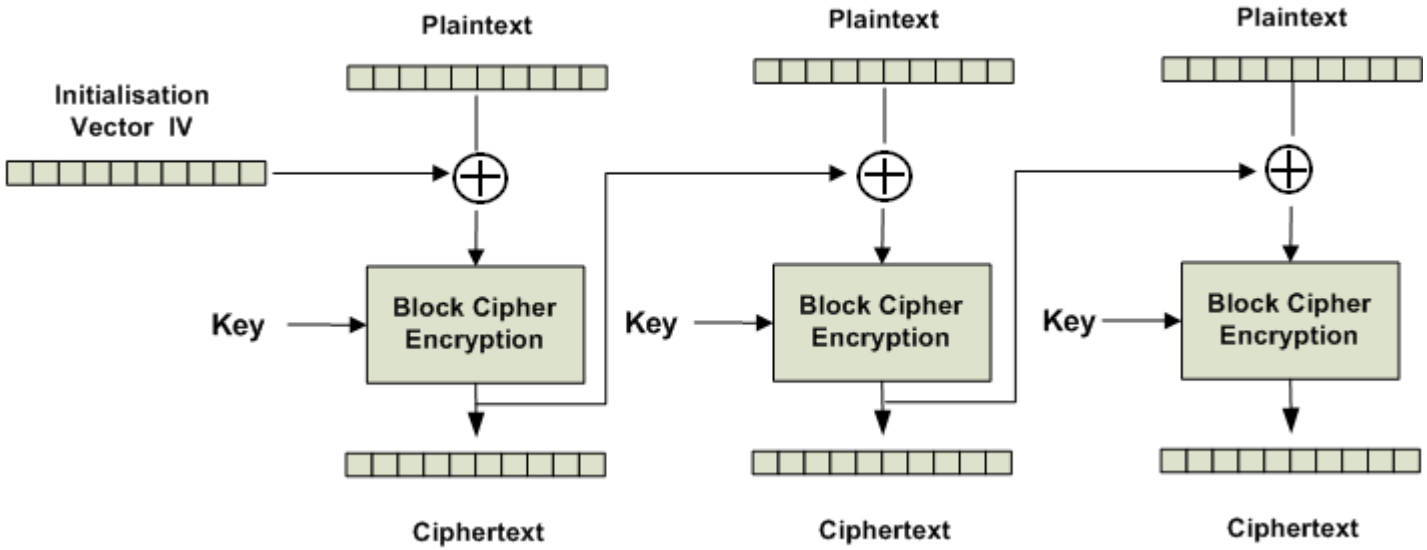
Electronic Code Book

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



Cipher Block Chaining

- Verschlüsseln: *Enc*(Block XOR dem vorigen Chiffrat-Block)
- Entschlüsseln: *Dec*(Chiffrat-Block) XOR vorigem Chiffrat-Block
- Initialisierungsvektor zufällig
- **Probleme:**
  - Verlust eines Chiffrat-Blocks führt zu Verlust 2er Klartextblöcke



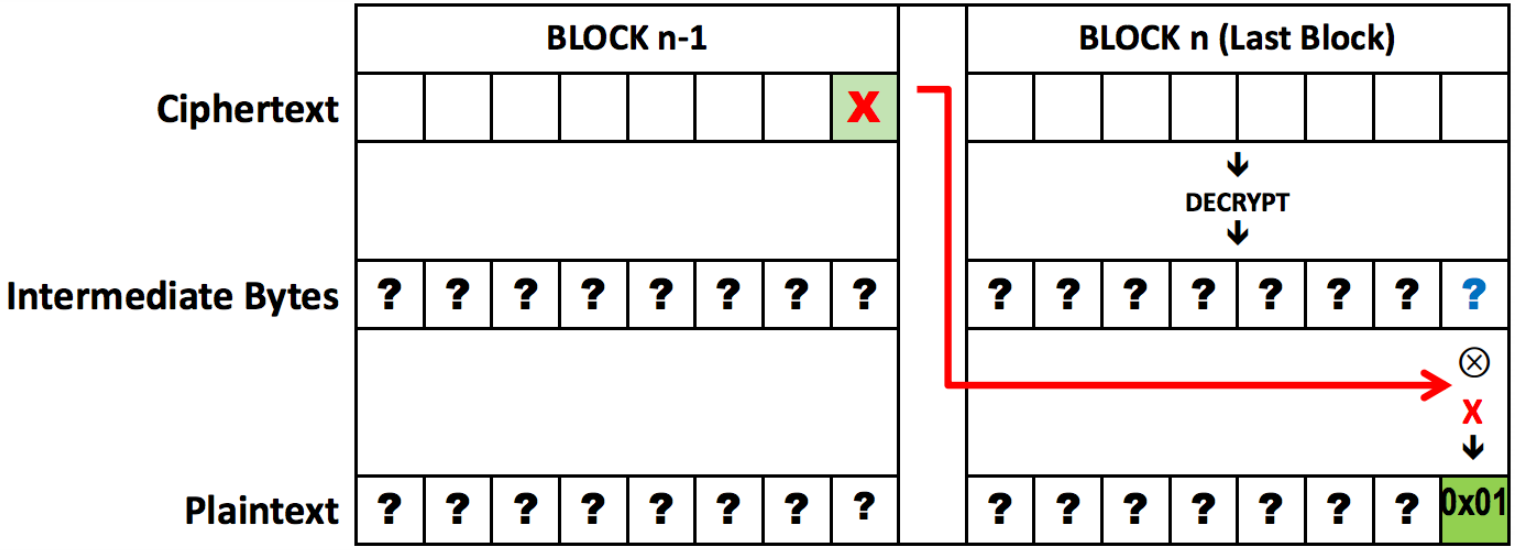
CBC Padding Oracle

- 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

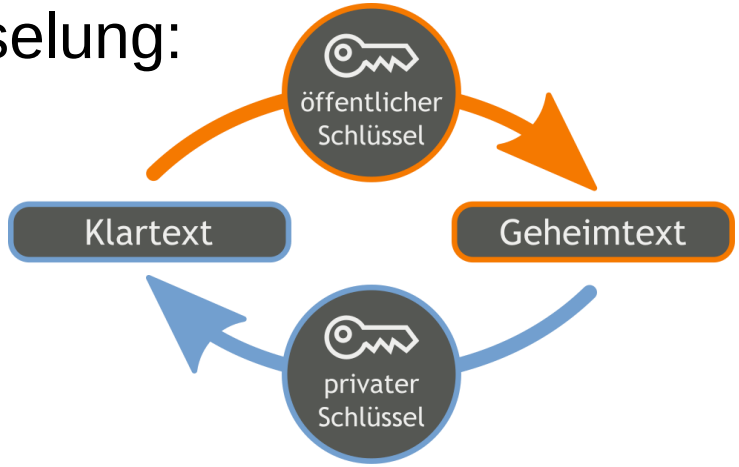


$? \oplus X = 0x01$

$? = 0x01 \oplus X$

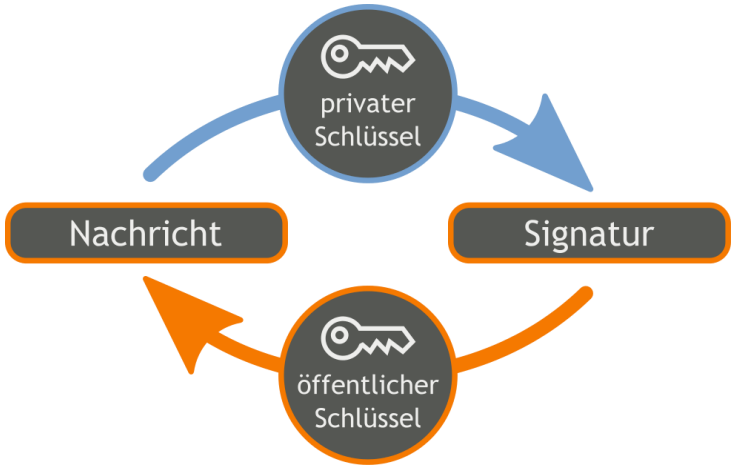
Asymmetrische Kryptosysteme

- 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 $ggT\big(e, \phi(N)\big) = 1 \ \wedge 1 < e < \phi(N)$ gilt
- Bestimme d so, dass $e \cdot d \equiv 1 \ \big(\mathrm{mod}\ \phi(N)\big)$ gilt. (erweiterter euklidischer Algorithmus)

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

- $ggT(a, b)$: Größter gemeinsamer Teiler von a und b
- $\phi(n) = \left|\left\{a \in \mathbb{N} \middle| 1 \leq a \leq n \ \wedge ggT(a, n) = 1\right\}\right|$
  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 $\mathrm{Enc}(m_1, pk) \cdot \mathrm{Enc}(m_2, pk) = \mathrm{Enc}(m_1 \cdot m_2, pk)$

Angriffe auf RSA

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

Und viele mehr!

Erinnerung: Security Fest CTF

- Do 31.5 12:00 CEST –
  Fr 01.6 18:00 CEST
- Freitag ab 11 Uhr treffen im ATIS oder von Remote
- Am besten #securityfest in Slack beitreten
- Wir freuen uns über jeden der Lust hat

Aufgaben

- ctf.bplaced.net (Crypto 20 + Crypto 30)
- Picoctf.com
- cryptopals.com
- overthewire.org/wargames/krypton