Kryptographie in CTFs

Eine Einführung

Benedikt Waibel | 25.05.2023

Überblick

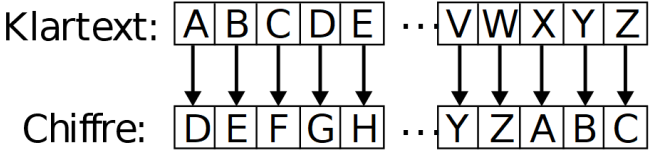
- Sicherheitsziele
- Kryptographische Verfahren
  - Klassische Kryptographie
  - Zufall
  - Symmetrische Kryptographie
  - Asymmetrische Kryptographie
- Typische Schwachstellen
- Tools
- Ausblick
- Aufgaben

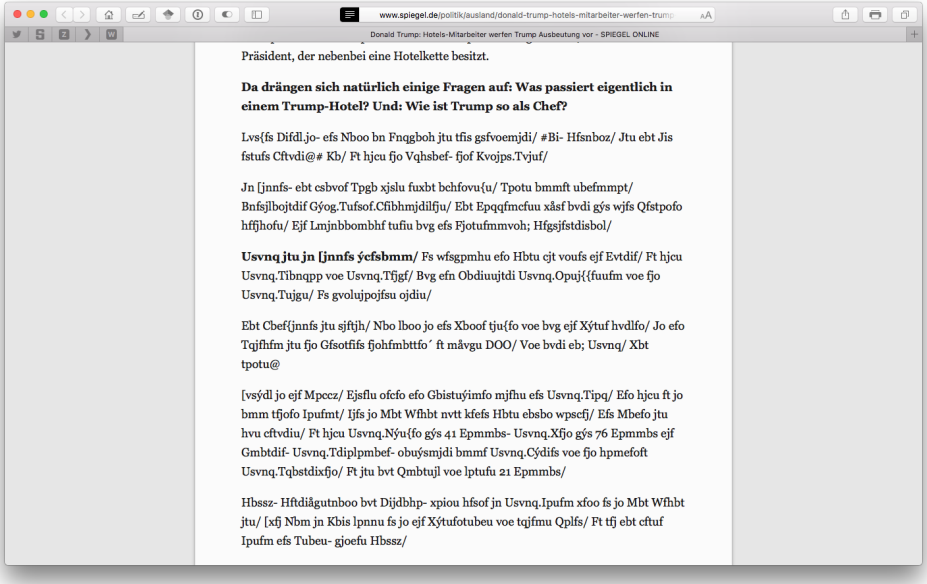
Sicherheitsziele

- CIA (Confidentiality, Integrity, Availability)
- Authenticity
- Welche Sicherheit braucht meine Anwendung?
- Welche Sicherheit bietet ein kryptographisches Verfahren? Was sind die Bedingungen?

Klassische Kryptographie

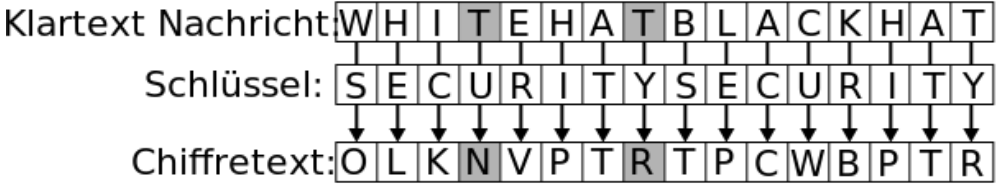
- **Caesar-Chiffre**
  - Jeder Buchstabe wird um einen festen Wert k verschoben
  - Wird heutzutage manchmal noch verwendet (spiegel.de Paywall)
  - *Angriffe*: Ausprobieren (Bruteforce), Häufigkeitsanalyse




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/ [xfj Nbm jn Kbis lpnnu fs jo ejf Xýtufotubeu voe tqjfmu Qplfs/ Ft tfj ebt cftuf Ipufm efs Tubeu- gjoefu Hbssz/

Klassische Kryptographie

- **Vigenère-Chiffre**
  - Wähle Schlüsselwort und verschiebe jeden Buchstaben entsprechend dem Schlüsselbuchstaben
  - *Angriffe*: Schlüssellänge bestimmen, Caesar-Chiffre für jede Schlüsselposition



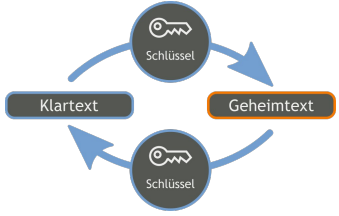
Klassische Kryptographie

- **XOR-Chiffre:**
  - Verschlüssele Klartext durch XOR mit Key
  - *Angriffe*: analog zu Vigenère (Bruteforce, Häufigkeitsanalyse pro Key Byte)
- **One Time Pad (OTP):**
  - Verwende Schlüssel mit gleicher Länge wie Klartext
  - **Informationstheoretische Sicherheit**, wenn der Schlüssel gleichverteilt zufällig generiert ist und nur einmal verwendet wird

Zufall

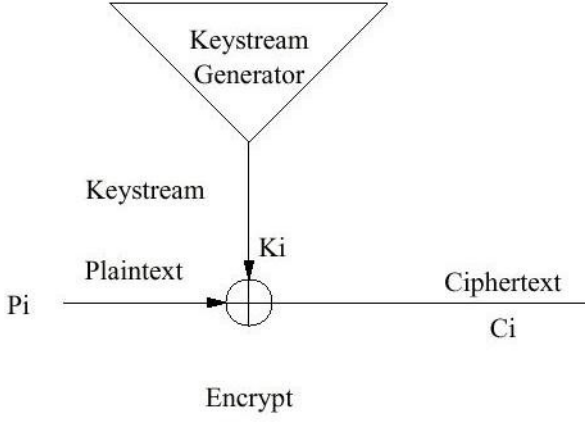
- Zufällige Eingaben an vielen Stellen für Chiffren benötigt
- unsichere Pseudozufallszahlengeneratoren (PRNGs) Standardquelle in vielen Sprachen
- Kryptographisch sichere RNGs:
  - /dev/urandom
  - Hardware RNGs
  - RNGs der meisten Krypto-Bibliotheken (z.B. secrets in python)
- *Angriffe*: Zustand wiederherstellen, Side Channels

Symmetrische Verschlüsselungen



- **Stromchiffren**
  - Pseudozufälliger Schlüsselstrom wird aus Schlüssel abgeleitet
  - Schlüsselstrom wird mit Klartext kombiniert
- **Blockchiffren**
  - Verschlüsselt Blöcke fester Länge
  - Betriebsmodus wird zur Verschlüsselung längerer Daten verwendet

Stromchiffren

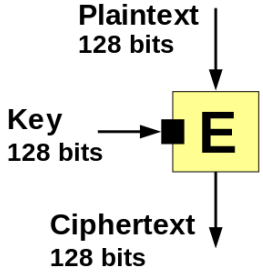


Stromchiffren

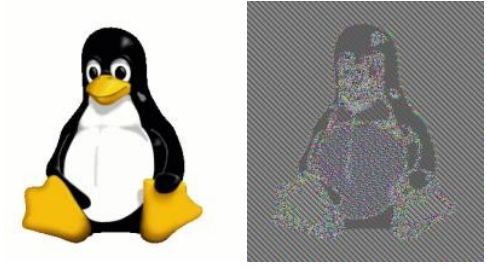
- RC4, SEAL, Salsa, CryptMT
- Linear Feedback Shift Register (LFSR)
- *Angriffe*:
  - Bekannter Klartext: Aus einem bekannten Klartext m mit zugehörigem Chiffrat c kann der Schlüsselstrom K rekonstruiert werden
  - Key-Reuse: zwei Nachrichten mit gleichem Schlüsselstrom verschlüsselt, liefert XOR-Differenz zwischen Klartexten

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)
  - Galois Counter Mode (GCM)
- *Angriffe*: auf Chiffre (differentielle, lineare Kryptoanalyse), auf Betriebsmodus



Electronic Code Book

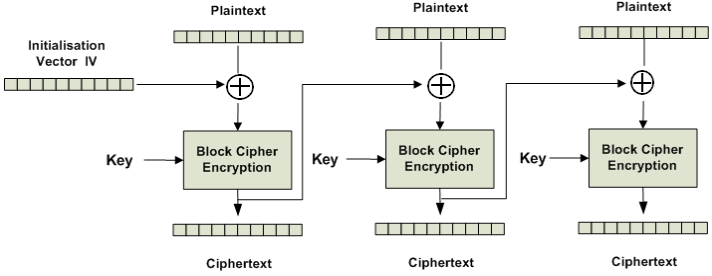


- Verschlüsselt jeden Block einzeln
- *Probleme:*
  - Daten Einfügen möglich
  - Deterministisch

Cipher Block Chaining

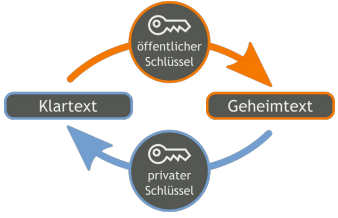
Für Klartextblöcke P_i, Chiffratblöcke C_i, $i \in \{1, \ldots n\}$, $C_0 = IV$

- Verschlüsseln: $C_i = Enc(P_i \oplus C_{i-1})$
- Entschlüsseln: $P_i = Dec(C_i) \oplus C_{i-1}$
- Initialisierungsvektor zufällig
- *Probleme:* Verlust eines Chiffratblocks führt zu Verlust 2er Klartextblöcke
- *Angriffe:* POODLE

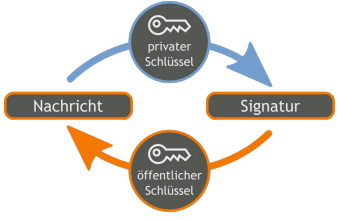


Asymmetrische Kryptosysteme

- Verschlüsselung:



- Signatur:



RSA

- Wähle zwei Primzahlen p und q
- Bestimme $N = p * q$
- Bestimme $\Phi(N) = (p-1) * (q-1)$
- Wähle e so, dass $ggT(e, \Phi(N)) = 1 \wedge 1 < e < \Phi(N)$ gilt
- Bestimme d so, dass $e * d \equiv 1 (mod \Phi(N))$ gilt. (Erweiterter Euklidischer Algorithmus)
- Öffentlicher Schlüssel: N, e
- Privater Schlüssel: d
- $ggT(a, b)$: größter gemeinsamer Teiler von a und b
- $\Phi(N) = |\{a \in \mathbb{N} | 1 \leq a \leq n \wedge ggT(a, N) = 1\}|$
  Anzahl aller Zahlen, die zu n teilerfremd sind bzw. Gruppenordnung (Eulersche Funktion)

RSA

- **Encryption:**

$$c = m^e \, mod N$$

- **Decryption:**

$$\begin{aligned} & c^d \, mod N \\ \Longleftrightarrow \; & m^{ed} \, mod N \\ \Longleftrightarrow \; & m^{edmod\Phi(N)} \, mod N \\ \Longleftrightarrow \; & m^1 \, mod N \end{aligned}$$

Mit dem kleinen fermatschen Satz

- **Homomorphie:**
$c_1 = m_1^e mod N$ und $c_2 = m_2^e mod N$, so gilt
$c_1.c_2 = m_1^e.m_2^e mod N = (m_1.m_2)^e mod N$.
Es gilt also $Enc(m_1, pk).Enc(m_2, pk) = Enc(m_1.m_2, pk)$

Angriffe auf RSA

Bedingung	Angriff	Komplexität
Keine	Faktorisierung	$\sim exp(log(N)^{\frac{1}{3}}(loglogN)^{\frac{2}{3}})$
Kleines $d (d < \frac{1}{3}N^{\frac{1}{4}})$	Wiener's Attack	Polynomiell
$m < N^{\frac{1}{e}}$	Wurzel ziehen	Polynomiell
Senden der gleichen Nachricht an viele Empfänger mit selbem e	Hastad's Broadcast Attack	Polynomiell

Elliptic Curves

- Elliptic Curve equation: $y^2 = x^3 + ax + b$
- Group: Generator point G, point addition and multiplication with natural number
- Cyclic EC group over $\mathbb{Z}_p$, $p > 3$
- Point (x, y) on curve iff $y^2 \equiv x^3 + ax + b \mod p$, plus (imaginary) point at infinity O, $a, b \in \mathbb{Z}_p$ with $4a^3 + 27b^2 \not\equiv 0 \mod p$

Typische Schwachstellen

- Implementierungsfehler: inkorrekt selbst implementiert, falsch eingebunden
- Denkfehler: Verfahren falsch verwendet oder für unpassende Anwendung
- Algebra: Bedingung für Sicherheit von Verfahren verletzt, mehr Mathe oder theoretische Informatik nötig, "read the paper"

Tools

- CyberChef
- `https://factordb.com`
- sagemath (free open-source mathematics software system)
- Z3 (theorem prover)

Ausblick

- Post-Quanten-Sicherheit (z.B. Lattice)
- Pairing Based Cryptography
- Zero Knowledge
- Wünscht euch gerne Themen im Content-Plan oder bietet selber Talks/Workshops an!

Aufgaben

- https://cryptohack.org
- https://cryptopals.com
- https://picoctf.com
- https://overthewire.org/wargames/krypton