Kryptographie SoS 2021

Techfak Bielefeld

14.4.2021

Ablauf: alles online.

- Vorlesung: Videos (immer mittwochs)
- Skript, Folien ← Webseite
- Tutorien: online, mit festen Terminen
- Übungen;

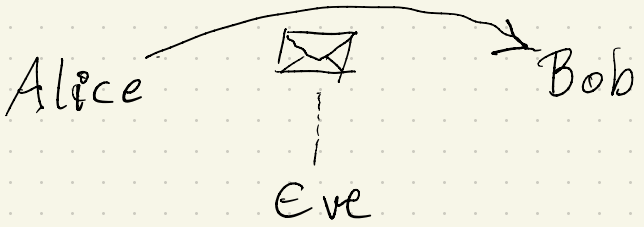
(Fragen: Tutoren, mich per email)

Einleitung Ziele der Vorlesung:

Theoretische Grundlagen, Algorithmen, Formeln.

(nicht: Implementierung, ~~penetration testing~~)

Ziele der Kryptographie



- Verschlüsseln
- Entschlüsseln (legal & illegal)
- Authentifikation (ist Alice wirklich Alice?)
- Anonymität

Zutaten:
- Algebra & Zahlentheorie (Kap. 2)
- Primzahltests (Kap. 3)
- Zufallszahlen (Kap. 4)
- (Hashfunktionen (Kap. 7))

Ein kryptographisches Verfahren heißt auch Protokoll.

Variablen:

K : Schlüssel (Key)

oder

e : Verschlüsselungsschlüssel (encode)

d : Entschlüsselungsschlüssel (decode)

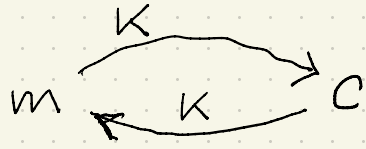
m : Nachricht (message)

c : verschlüsselter Text (aka Geheimtext, cipher)

$f(K, m) = c$: f ist verschlüsseln

$f^*(K, c) = m$: f^* ist entschlüsseln

Es gibt • symmetrische Verfahren



• asymmetrische Verfahren (insbes. public key-Verf.)

Bsp 1: Cäsarcode (über 2000 Jahre alt)

symm. Verf.; Buchstaben A B C D ... Z
zu Zahlen 0 1 2 3 ... 25

für jedes $m \in \{0, 1, 2, \ldots 25\}$

$c = f(K, m) = m + K \mod 26$ (Verschl.)

$m = f^*(K, c) = c - K \mod 26$ (Entschl.)

Bsp für's Bsp:

$f(9, \text{techfak}) = \text{CNLQOJT}$

techfak
+ 9999999
CNLQOJT

19 4 2 7 5 10
+ 9 9 9 9 9 9
2 13 11 16 14 19

[0] [9]

(Entschlüsseln analog:

CNLQOJT
− 9999999
techfak)

Bemark. Texte/Dateien $\longleftrightarrow$ Zahlen/Binär
UTF 8

- Cäsarcode nicht sicher: nur 26 Schlüssel testen; oder häufige Zeichenketten suchen.

Bsp 2: Vigenèrecode (≈ 400 Jahre)
(geknackt vor ≈ 150 Jahren)

Wie Cäsarcode, aber mehr als ein K:

$K = (K_1, K_2, \dots, K_\ell)$ [z.B. Wort: Key: (10, 4, 24)]

Verschlüssele $m = (m_1, m_2, \dots m_n)$

als $f(K, m) = (m_1 + K_1 \bmod 26;\ m_2 + K_2 \bmod 26; \dots$

$\dots m_\ell + K_\ell \bmod 26;\ m_{\ell+1} + K_1 \bmod 26 \dots)$

entschlüsseln analog:

techfak
+ keykeyk
DIARJYU

DIARJYU
− keykeyk
techfak

1.2 Was heißt „Code knacken"?

Früher: Verfahren geheim.

Heute: Verfahren bekannt, Schlüssel geheim.

Immer noch vier Szenarien:

- ciphertext only attack: Eve kennt nur einen oder mehrere Geheimtexte
- known plaintext attack Eve kennt ein (bzw. mehrere) Paare $c = f(k, m)$
- chosen plaintext attack: Eve kann f nutzen (kennt nicht k). Eve kann z.B. aaaa.....aa verschlüsseln
- chosen ciphertext attack: Eve kann f^* nutzen (ohne k zu kennen), möchte k ermitteln.

„Sicher" heißt: allen Szenarien widerstehen.

Hm. Nächster Versuch: effizient & sicher (& korrekt)

„Definition": Ein kryptographisches Verfahren ist effizient und sicher, wenn

- für alle m und c die $f(k,m)$ und $f^*(k,c)$ einfach zu berechnen sind, (effizient)
  (k bekannt)
- für fast alle c ist $f^*(k,c)$ schwer (sicher)
  (k unbekannt)

- einfach: in P; (bzw RP) (siehe A&D)
- schwer: in $NP \setminus P$ (Problem $P \stackrel{?}{=} NP$)
  (Theorie ↑) (↙ Praxis)

  Praktisch nicht machbar (z.B. alle amazon-server bräuchten 10^3 oder 10^6 Jahre)
- fast alle: Für $W = \{0, 1, \dots N\}$:
  Anteil der Ausnahmen geht gegen 0 für N gegen ∞.

Bsp 1.3: Fast alle $n \in W$ haben mehr als 6 Dezimalstellen. ✓

Denn: $$\lim_{N \to \infty} \frac{\text{Zahlen} \le N \text{ mit} \le 6 \text{ Dezimalstellen}}{\text{Zahlen} \le N}$$

$$= \lim_{N \to \infty} \frac{10^6}{N} = 0$$

Fast alle $n \in W$ sind keine Primzahlen ✓

Satz (später): Anzahl Primzahlen $\le N$ ist $O\left(\frac{N}{\log N}\right)$.

Also $\lim_{N \to \infty} \frac{N / \log N}{N} = \lim_{N \to \infty} \frac{1 / \log N}{1}$

$= \lim_{N \to \infty} \frac{1}{\log N} = 0.$

Bsp 1.4 Ein sicheres, effizientes, korrektes symmetrisches Verfahren:

One-Time-Pad OTP (Binärzahlen: siehe Skript)

Voraussetzungen:

- K genauso lang wie m
- K nur einmal nutzen
- K zufällig
- K geheim

Dann beweisbar sicher!

OTP: $m = (m_1, m_2, m_3, \ldots m_n)$ $(m \in \{0, 1, \ldots 25\})$

$K = (K_1, K_1, K_3, \ldots K_n)$

$f(m_i, K_i) = m_i + K_i \mod 26$

$f^*(c_i, K_i) = c_i - K_i \mod 26.$