IT-Sicherheit

Stromchiffren

Version vom 14.11.2017

Symmetrische Chiffren (Definition)

Eine Chiffre ist ein Paar aus zwei effizienten Algorithmen (E, D), wobei

- E häufig randomisiert ist
- D immer deterministisch ist

Ein symmetrisches Kryptosystem besteht aus dem Tupel (M, C, K, E, D). Dabei bezeichnet

- M die Menge möglicher Klartexte
- C die Menge möglicher Chiffrate
- K die Menge der möglichen Schlüssel.

Es muss gelten: $\forall k \in K, \forall m \in M: D\big(k, E(k, m)\big) = m$

One Time Pad

Erster Beispiel eines Verschlüsselungsalgorithmus (Vernam, 1917)

- Schlüssel ist (mindestens) so lang wie zu verschlüsselnde Nachricht.
- E: Nachricht und Schlüssel werden mit XOR verknüpft, um das Chiffrat zu erhalten.
- D: Chiffrat und Schlüssel werden mit XOR verknüfpft, um den Klartext zu erhalten.

msg: 0 1 1 0 1 1 1

key: 1 0 1 1 0 1 0 $\oplus$

CT:

Eigenschaften des One Time Pad

- Sehr schnelle Verschlüsselung
- sehr schnelle Entschlüsselung
- sehr langer Schlüssel

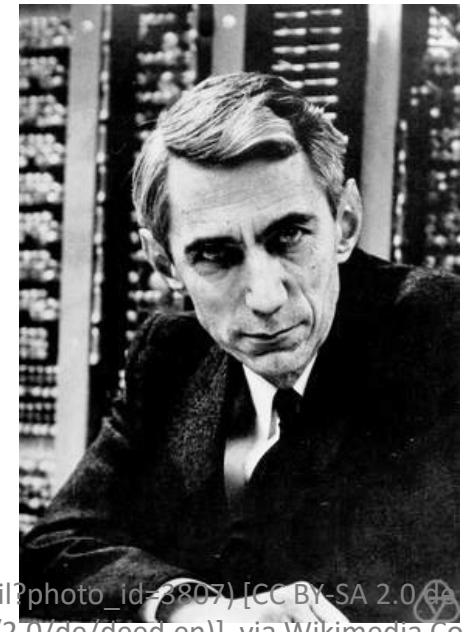
- Ist das One Time Pad sicher?
- Wie ist eigentlich ein sicherer Chiffre definiert?

Definitionsversuch „sicherer Chiffre“

- Definition der Möglichkeiten des Angreifers
  erste Variante: „Angreifer hat Zugriff auf Chiffrat“
- Mögliche Sicherheitsanforderungen
  1. Angreifer kann Schlüssel nicht bestimmen.
  2. Angreifer kann nicht den (gesamten) Klartext bestimmen.

Idee von Claude Shannon:

Chiffrat darf keine Informationen über Klartext preisgeben.



Perfect Secrecy (Shannon 1949)

Definition:

Ein Chiffre (E,D) über (K,M,C) verfügt über „Perfect Secrecy“, wenn $\forall m_0, m_1 \in M \ (|m_0| = |m_1|)$ und $\forall c \in C$ gilt:

$$\Pr[E(k, m_0) = c] \ = \ \Pr[E(k, m_1) = c]$$

$$\text{wobei } k \xleftarrow{R} K$$

OTP hat Perfect Secrecy

Beweisskizze:

Sei $m \in M$ und $c \in C$. Wie viele Schlüssel gibt es, die m auf c abbilden?

verhindert weitgehend praktischen Einsatz von OTP

Die schlechte Nachricht:
Für alle Chiffren mit Perfect Forward Secrecy gilt: $|K| \geq |M|$

Stromchiffren

Idee:

- One Time Pad verwenden, jedoch mit kürzerem Schlüssel

➔Ersetze zufälligen Schlüssel mit einem „pseudo-zufälligen“ Generator (PRG – pseudo random generator)

Können Stromchiffren Perfect Secrecy aufweisen?

NEIN, denn der Schlüssel (Initialisierungswert des PRG) ist kürzer als die Nachricht.

➔Neue Definition von „sicherer Cipher“ notwendig!

➔Sicherheit hängt von den Eigenschaften des PRG ab!

PRG darf nicht vorhersagbar sein

Definition:

Ein PRG $G: K \rightarrow \{0,1\}^n$ ist vorhersagbar, wenn ein Algorithmus A existiert, der

1. höchstens polynomiales Laufzeitverhalten aufweist
2. aus einer bekannten Folge von i-1 Bits des PRG das Bit Nr. i mit einer nicht zu vernachlässigenden Wahrscheinlichkeit vorhersagen kann:

$$\exists A, \exists i, 1 \leq i < n, \text{so dass}$$
$$\Pr_{\substack{R \\ k \leftarrow K}}\left[A\left(G(k)\Big|_{1,\ldots,i}\right) = G(k)\Big|_{i+1}\right] \geq \frac{1}{2} + \epsilon$$

„nicht zu vernachlässigend“ bedeutet typischerweise $\epsilon < \frac{1}{2^{30}}$

Übergang OTP → Stromchiffre

Das Ersetzen des Schlüssels mit der Ausgabe des PRG führt from One-Time-Pad zum Stromchiffre:

- OTP

$$E(k,m) = m \oplus k, \qquad D(k,c) = c \oplus k$$

- Stromchiffre
  mit PRG $G: K \rightarrow \{0,1\}^n$

$$E(k,m) = m \oplus G(k), \qquad D(k,c) = c \oplus G(k)$$

Achtung:
Niemals Stomchiffren-Schlüssel wiederverwenden!

Szenario:
Schlüssel k wird wiederverwendet, Angreifer fängt Chiffrate ab:

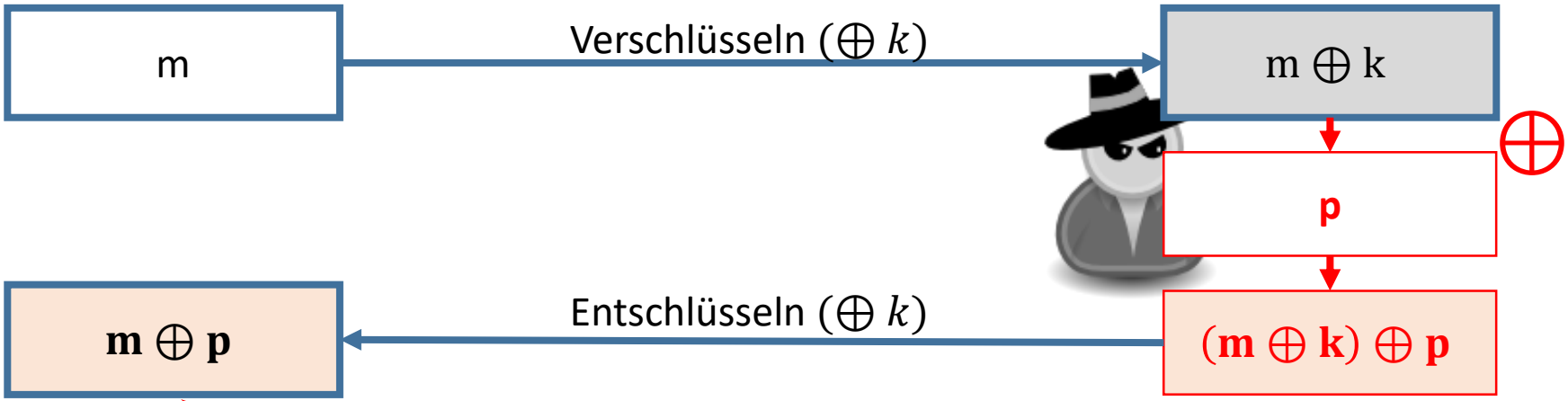
$$c_1 \leftarrow m_1 \oplus PRG(k)$$
$$c_2 \leftarrow m_2 \oplus PRG(k)$$

Was ergibt $c_1 \oplus c_2$?

$$m_1 \oplus m_2$$

Viele Dateien / Klartexte enthalten soviel Redundanz, dass ein Angreifer aus $m_1 \oplus m_2$ die beiden Klartexte m_1, m_2 rekonstruieren kann!

Achtung: Stromchiffren/OTP bieten keinen Integritätsschutz!



Änderungen am Chiffrat bleiben unerkannt und können **vorhersagbare Änderungen** am Klartext bewirken!

Beispiele für Stromchiffren

- RC4
  - Seed von 128 bit
  - Verwendung in https und WEP
  - mehrere Schwächen bekannt
- CSS
  - verwendet für DVD-Verschlüsselung, GSM Verschlüsselung (A5/1,2), und Bluetooth (E0)
  - erfolgreich gebrochen!

- Salsa20
- Sosemanuk

} eStream