Datensicherheit, Zusammenfassung Vorlesung 9

Henry Haustein, Dennis Rössel

Welche Angriffsarten auf Kryptosysteme werden unterschieden?

Passiver Angreifer nutzt Wissen über System (Algorithmen, Protokolle), Öffentliche Schlüssel/Parameter und Beobachtung (unsicherer Kanal)

- Reiner Schlüsseltext-Angriff (ciphertext-only attack)
- Klartext-Schlüsseltext-Angriff (known-plaintext attack)

Aktiver Angreifer: bringt Inhaber der geheimen bzw. privaten Schlüssel dazu, die entsprechenden Operationen für selbst gewählte Daten auszuführen

- Gewählter Klartext-Schlüsseltext-Angriff (chosen-plaintext attack CPA; *Verschlüsselungsorakel*)
- Gewählter Schlüsseltext-Klartext-Angriff (chosen-ciphertext attack; *Entschlüsselungsorakel*)

Was bedeutet informationstheoretische (perfekte) Sicherheit?

Auch einem unbeschränkten Angreifer gelingt es nicht, das System zu brechen.

Was sind relevante Anforderungen an die Schlüssel bei einer informationstheoretisch sicheren Chiffre?

Ein System heißt informationstheoretisch sicher, wenn für alle Nachrichten und Schlüsseltexte gilt, dass die a posteriori Wahrscheinlichkeiten $p(m \mid c)$ der möglichen Nachrichten nach Beobachtung eines gesendeten Geheimtextes gleich der a priori Wahrscheinlichkeiten $p(m)$ dieser Nachrichten sind:

$$\forall m \in M, \forall c \in C: \quad p(m \mid c) = p(m)$$

Wie funktioniert die Vernam-Chiffre?

Jeder Schlüssel wird nur einmal verwendet, Schlüssellänge und Länge des Klartextes gleich, Schlüssel zufällig
$\Rightarrow$ XOR

Warum kann es bei asymmetrischen Verfahren keine informationstheoretische Sicherheit geben?

Schlüsselmanagement problematisch

Wie funktionieren Transpositionen und Substitutionen?

Transposition = Vertauschen der Zeichen des Klartextes
MM-Substitutionen (monoalphabetisch, monographisch): ein Buchstabe des Klartextes wird mit einem Buchstaben ersetzt. Die Buchstaben zu denen ersetzt wird kommen aus einem Alphabet ⇒ eineindeutige Zuordnung
PM-Substitutionen (polyalphabetisch, monographisch): wie MM-Substitutionen, nur dass die Buchstaben zu denen ersetzt wird, aus mehreren Alphabeten kommen ⇒ eindeutige Zuordnung

Wie kann das verwendete historische Verschlüsselungsverfahren anhand eines vorliegenden Schlüsseltextes identifiziert werden?

mittels Histogramm

Wie kann die Analyse von MM-Substitutionen bzw. PM-Substitutionen erfolgen?

MM-Substitution: Analyse von Buchstaben, Bi- und Trigrammen, Nutzung Redundanz bei fehlenden Zeichen

PM-Substitution: Schlüssellänge mit Kasiski-Test → MM-Analyse