Kryptografie und -analyse, Zusammenfassung Vorlesung 4

Henry Haustein

Wie funktioniert die Vernam-Chiffre (one-time pad)?

Zeichenweise Addition von Klartext + Schlüssel modulo Alphabetgröße

Welche Bedingungen sind zu erfüllen, damit die perfekte Sicherheit erreicht wird?

folgende Bedingungen sind dafür notwendig:

- Schlüssel müssen echt zufällig sein
- Schlüssellänge = Nachrichtenlänge
- Einmalige Verwendung des Schlüssels

Welche allgemeinen Angriffe auf Blockchiffren gibt es und wie ist das jeweilige Vorgehen?

Angriffe:

- vollständige Schlüsselsuche: einfach alle möglichen Schlüssel ausprobieren
- Zugriff auf eine vorab berechnete Tabelle: Angreifer berechnet für eine Nachricht m alle verschlüsselten Texte c für jeden Schlüssel k. Dann lässt er sich vom Angegriffenen sein m verschlüsseln und schaut in seiner Tabelle nach und findet so den Schlüssel, den der Angegriffene benutzt hat
- Time-memory-tradeoff: Angreifer wählt zufällig und unabhängig voneinander n verschiedene Startschlüssel k_i und Klartextblock m, Verschlüsselt m mit allen Startschlüsseln, Schlüsseltexte $c_{i,1} = enc(k_{i,1}, m)$ dienen (nach geringfügiger Anpassung durch Transformation T) als neue Schlüssel $k_{i,2}$ für weitere Verschlüsselung, Pro Startschlüssel t Iterationen, Gespeichert wird pro *Kette* der Startschlüssel $k_{i,1}$ und der letzte Schlüsseltextblock $c_{i,t}$
- Kodebuchanalyse: Klartext-Schlüsseltext-Paare werden in einer Tabelle (*Kodebuch*) abgespeichert, Versuch, Teile des beobachteten Schlüsseltextes mit Hilfe des Kodebuches zu rekonstruieren

Wovon hängt der Aufwand dieser Angriffe jeweils ab?

von der Größe des Schlüsselraums

Was sind die charakteristischen Merkmale der Feistel-Chiffre? Was ist unter Selbstinversität zu verstehen? Wie funktionieren Verschlüsselung und Entschlüsselung?

charakteristische Merkmale:

- Zerlegung des Nachrichtenblocks in linke und rechte Hälfte
- Rundenfunktion f ist identisch bei Ver- und Entschlüsselung
- Pro Runde wird jeweils nur ein Teilblock modifiziert $\rightarrow$ ermöglicht effiziente Implementierung

Selbstinversität: Ver- und Entschlüsselung geschieht mit den gleichen Funktionen, nur Reihenfolge der Rundenschlüssel wird umgekehrt

Was versteht man unter Vollständigkeit, dem Avalanche-Effekt und Nichtlinearität?

Vollständigkeit: Eine Funktion $f : \{0,1\}^n \rightarrow \{0,1\}^m$ heißt vollständig, wenn jedes Bit des Outputs von jedem Bit des Inputs abhängt.

Avalanche-Effekt: Eine Funktion $f : \{0,1\}^n \rightarrow \{0,1\}^m$ besitzt dann den Avalanche-Effekt, wenn die Änderung eines Input-Bits im Mittel die Hälfte aller Output-Bits ändert. Wird durch Änderung eines Input-Bits jedes Output-Bit mit einer Wahrscheinlichkeit von 50% verändert, erfüllt f das strikte Avalanche-Kriterium.

Linearität: Eine Funktion $f : \{0,1\}^n \rightarrow \{0,1\}^m$ ist dann linear, wenn jedes Output-Bit y_i linear von den Input-Bits x_i abhängt:

$$y_i = a_{j1}x_1 + a_{j2}x_2 + \cdots + a_{jn}x_n + b$$

Wie können diese Kriterien beurteilt werden?

mit Hilfe der Abhängigkeitsmatrix: Die Abhängigkeitsmatrix einer Funktion $f : \{0,1\}^n \rightarrow \{0,1\}^m$ ist eine $(n \times m)$-Matrix, deren Einträge $a_{i,j}$ die Wahrscheinlichkeit angeben, dass bei einer Änderung des i-ten Eingabebits das j-te Ausgabebit komplementiert wird.

Überprüfung der Eigenschaften:

- Vollständigkeit: $\forall a_{ij} > 0$
- Avalanche-Effekt: $\frac{1}{nm} \sum_i \sum_j a_{ij} \approx 0.5$
- strikes Avalanche-Kriterium: $\forall a_{ij} > 0.5$
- Linearität: $\forall a_{ij} \in \{0,1\}$