Kryptografie und -analyse, Zusammenfassung Vorlesung 5

Henry Haustein

Wie funktioniert der Algorithmus DES prinzipiell?

Feistel-Chiffre mit 16 Runden, Einteilung der Nachricht in Blöcke der Länge 64 Bit, Schlüssel der Länge 64 Bit, aber nur 56 Bit frei wählbar, 16 Teilschlüssel werden erzeugt. Permutation vor der ersten und nach der letzten Runde

Was ist die größte Schwäche des DES?

kurzer Schlüssel, nur 56 Bit sind frei wählbar.

Wie soll durch die Mehrfachverschlüsselung (3-DES) eine Steigerung der Sicherheit erreicht werden?

Es müssen mehr Schlüsselbits berechnet werden

Warum genügt es nicht, zweimal zu verschlüsseln?

Sicherheitsgewinn ist nur 1 Bit wegen Meet-in-the-middle-Angriff

Was ist das Prinzip der differentiellen Kryptoanalyse?

gewählter Klartext-Schlüsseltext-Angriff, Prinzip

- Verwendung von beliebigen Klartextpaaren mit bestimmten Differenzen
- Analyse der Auswirkungen der Klartext-Differenzen auf die Differenzen der resultierenden Schlüsseltextpaare
- Ermittlung wahrscheinlicher Schlüssel

Wie funktioniert die differentielle Kryptoanalyse einer einzelnen Runde des DES?

Differenz nach Expansion bestimmen, aus Output der S-Boxen wahrscheinlichsten Input bestimmen, Input der S-Box $\oplus$ Output nach Expansion = Schlüssel

Wie werden dabei mögliche Belegungen der Inputvektoren der S-Boxen ermittelt?

Die Output-Differenz aus den S-Boxen ist beobachtbar. Die Input-Differenz vor den S-Boxen $x_S \oplus x_S^*$ ist auch berechenbar, weil $(x_E \oplus k) \oplus (x_E^* \oplus k) = x_E \oplus x_E^*$ mit x_E nach der Expansion. In einer Differenzentabelle kann man dann für die berechnete Input-Differenz und der zugehörigen Output-Differenz alle Kombinationen von x_S und x_S^* ablesen, die genau die Output-Differenz erzeugen.

Wie werden im Anschluss mögliche Schlüsselbits bestimmt?

Da wir x_E, x_E^* und mögliche x_S, x_S^* nun kennen und folgender Zusammenhang gilt: $x_E \oplus k = x_S$, können wir mögliche Schlüssel berechnen: $k = x_E \oplus x_S$. Wenn man dies für mehrere Nachrichten macht, findet sich irgendwann nur ein Schlüssel, der bei allen Nachrichten als möglicher Schlüssel funktioniert.

Was sind n-Runden-Charakteristiken?

Bisher ließen sich alle Möglichkeiten absolut berechnen, aber bei mehr als 5 Runden ist dies nicht mehr möglich. Man muss dann mit Wahrscheinlichkeiten arbeiten und die Differenzen über mehrere Runden verfolgen. Man nennt das Charakteristik.

Die Menge der Eingangs- und Ausgangsdifferenzen über n Runden bezüglich irgendeines Klartextpaares, sowie der Klartext- und der Geheimtextdifferenz nennt man n-Runden-Charakteristik Ω.

Wie bestimmt man die Wahrscheinlichkeit einer n-Runden-Charakteristik?

Jeder Charakteristik Ω kann man eine Wahrscheinlichkeit p^Ω zuordnen, dass ein zufälliges Klartextpaar mit der gegebenen Differenz Ω_P genau die in der Charakteristik angenommenen Differenzen in den einzelnen Runden aufweist. Die Wahrscheinlichkeit einer n-Runden-Charakteristik p^Ω ist dabei das Produkt der Wahrscheinlichkeiten aller 1-Runden-Charakteristiken p_i^Ω aus denen sich die n-Runden-Charakteristik Ω zusammensetzt:

$$p^\Omega = \prod_{i=1}^{n} p_i^\Omega$$

Die Wahrscheinlichkeit einer 1-Runden-Charakteristik ist p_D, also die Wahrscheinlichkeit, dass die Eingangsdifferenz dieser Charakteristik die Ausgangsdifferenz dieser Charakteristik verursacht.

Ein Sonderfall sind sogenannte iterative Charakteristiken, mit $\Omega_1 = \Omega_2$, welche immer wieder an sich selbst angehängt werden können. Die vertauschten Hälften der Klartextdifferenz sind also gleich der Geheimtextdifferenz derselben Charakteristik. Diese lassen sich also leicht zu beliebig großen n-Runden-Charakteristiken zusammenhängen. Während bei nicht-iterativen Charakteristiken die Wahrscheinlichkeit mit größerem n, bedingt durch den Avalanche-Effekt, immer schneller abnimmt, bleiben die Wahrscheinlichkeiten der Teilcharakteristiken aus denen iterative Charakteristiken zusammengesetzt sind gleich. Iterative Charakteristiken werden deshalb bei einem Angriff bevorzugt eingesetzt.