Datensicherheit, Zusammenfassung Vorlesung 10

Henry Haustein, Dennis Rössel

Was ist unter *iterierter Blockchiffre* zu verstehen?

Verschlüsselung geschieht in mehreren Runden, Anzahl der Runden relevant für Sicherheit, Rundenfunktion mit Rundenschlüssel

Was sind Beispiele für allgemeine Ansätze zur Analyse von Blockchiffren? Was ist jeweils das Ziel und der Ablauf?

vollständige Schlüsselsuche, vorab berechnete Tabelle, Time-Memory-Tradeoff

Was sind die charakteristischen Eigenschaften der Feistel-Chiffre?

selbstinvers, Vertauschung linker und rechter Hälfte

Was bedeutet Selbstinversität?

Verschlüsselung = Entschlüsselung, nur Reihenfolge der Rundenschlüssel wird umgekehrt

Was charakterisiert den Algorithmus DES?

Feistelchiffre mit 16 Runden, 64 Bit Blöcke, Schlüssel 64 Bit mit 8 Paritätsbits

Wie ist die Sicherheit des DES-Algorithmus zu bewerten?

nicht mehr sicher wegen Schlüssellänge

Was ist das Ziel der Mehrfachverschlüsselung? Genügt eine doppelte Verschlüsselung?

mehrere Schlüssel zu knacken; nein wegen Meet-in-the-Middle-Angriff

Wie ist der Ablauf des Meet-in-the-Middle-Angriffs?

alle Verschlüsselungen des Klartextes, alle Entschlüsselungen des Ciphertextes berechnen $\Rightarrow$ abgleichen