Blockchiffren

Designziele:

- Konfusion, Verschleiern des Zusammenhangs zwischen Klar- und Chiffretext.
- Diffusion, Verteilen der Information im Klartext über den Chiffretext.
- Lawineneffekt, jedes Bit im Chiffretext soll von jedem Bit des Klartexts und des Schlüssels abhängen.
- Noch mehr: Jedes Bit des Chiffretext soll sich mit Wahrscheinlichkeit $1/2$ ändern, wenn irgendein Bit des Klartexts oder des Schlüssels geändert wird.

$\Rightarrow$ soll sich wie eine zufällige Funktion verhalten.

Blockchiffren Konstruktion

Der Eingabeblock wird durch mehrfache Anwendung einer Rundenfunktion bearbeitet. Für jede Runde wird ein Rundenschlüssel anhand eines Schlüsselschemas erzeugt.

Die Rundenfunktionen stellt im allgemeinen kein sicheres Verschlüsselungsverfahren dar, erst die mehrfache Anwendung ergibt die Sicherheit.

Bei den Rundenfunktionen werden im wesentlichen Feistel- und Substitutions-Permutationsnetzwerke unterschieden.

Die i-te Runde: $m_i = g(m_{i-1}, k_i)$.

Feistel Netzwerke

Blöcke in zwei gleiche Hälften auteilen:

- $m_i = (L^i, R^i)$.

Verschlüsseln:

- $L^i = R^{i-1}$
- $R^i = L^{i-1} \oplus f(R^{i-1}, k_i)$.

Entschlüsseln:

- $L^{i-1} = R^i \oplus f(L^i, k_i)$.
- $R^{i-1} = L^i$.

f muß nicht injektiv sein.

Substitutions-Permutationsnetzwerke

Block und Schlüssel mit XOR verknüpfen:

- $m_i = m_{i-1} \oplus k_i$.

Blöcke in mehrere Teilblöcke aufteilen:

- $m_i = (m_{i,j})_j$.

Auf die Teilblöcke eine Substitutionschiffre anwenden:

- $(\pi_S(m_{i,j}))_j$.

Die Bits der zusammengefaßten Teilblöcke permutieren:

- $m_{i+1} = \pi_P((\pi_S(m_{i,j}))_j)$.

(Die Permutation π_P wird in der letzten Runde aus Symmetriegründen nicht angewendet, dafür m_r und k_{r+1} mit XOR verbunden.)

Data Encryption Standard - DES

- Entwickelt um 1977
- Ist de-facto der internationale Standard für Bankensicherheit.
- Vermutlich der am meisten analysierte kryptographische Algorithmus.

- Kurze Geschichte:
  - Ausschreibung für ein Verfahren durch NBS (heute NIST).
  - Vorgänger Lucifer bei IBM entwickelt (Feistel, Coppersmith).
  - Untersuchung durch NSA und Veränderung der S-Boxen.
  - Geheimhaltung der Design-Kriterien bis in die 90er (Hintertür-Spekulationen).
  - 1990 Entdeckung der differentiellen Kryptanalyse, war NSA schon damals bekannt ...

DES

Blocklänge 64 Bit, Schlüssellänge 56 Bit.
Feistel Chiffre mit 16 Runden.

Die Feistel-Funktion $f : \{0,1\}^{32} \times \{0,1\}^{48} \to \{0,1\}^{32}$ ist definiert wie folgt:

1. R^{i-1} wird auf 48 Bit erweitert und permutiert, so daß 16 Bit doppelt auftreten (Diffusion, Lawineneffekt).
2. XOR mit dem Rundenschlüssel k_i und Aufteilung in 8 Blöcke B_i von je 6 Bit.
3. Anwendung der S-Box $S_i : \{0,1\}^6 \to \{0,1\}^4$ auf B_i, $C_i = S_i(B_i)$.
4. Anwendung der Permutation P auf $C_1 \ldots C_8$, Ergebnis ist $f(R^{i-1}, k_i)$.

DES

Nach dem letzten Feistelschritt werden L^{16} und R^{16} vertauscht.

Dem gesamten Feistel Netzwerk wird eine Permutation $IP \in S(\{0,1\}^{64})$ vorgeschaltet und IP^{-1} nachgeschaltet.
Dies hat keine kryptographische Bedeutung.

Zusammenfassend also:

1. IP auf Block anwenden: $(L^0, R^0) \leftarrow IP(m)$.
2. 16 Runden Feistel-Netzwerk.
3. $R^{17} \leftarrow L^{16}$ und $L^{17} \leftarrow R^{16}$.
4. IP^{-1} auf Block anwenden: $c \leftarrow IP^{-1}(L^{17}, R^{17})$.

DES

Die k_i sind 48 Bit Schlüssel und setzen sich aus einer Auswahl permutierter Bits aus k zusammen:

1. k wird in zwei 28 Bit Blöcke aufgeteilt.
2. Diese werden in Anhängigkeit der Rundenanzahl rotiert.
3. Aus den 56 Bit werden 48 gemäß einer festen Regel ausgewählt.

Schwache Schlüssel:

- Linke und rechte Hälfte von k nur Einsen oder Nullen.

Keine weiteren schwachen Schlüssel bekannt.
Es gibt noch 6 semi-schwache Schlüsselpaare (k, l) mit $\mathcal{E}(k, \cdot) = \mathcal{E}(l, \cdot)$.

DES

Sicherheit von DES:

- Probleme im wesentlichen nur wegen zu kleiner Schlüssellänge.
- Stark gegen differentielle Kryptanalyse.
- Differentielle und lineare Kryptanalyse brauchen $> 2^{40}$ Klartexte, nicht praktikabel.
- Brute-Force (2^{56} Schritte) praktikabel.

Hardware:

- Deep Crack (1998): 250.000 Dollar, ein Schlüssel in 50h.
- Man kann davon ausgehen, daß es heute (bei den entsprechenden Organisationen) Hardware gibt, die das viel schneller schafft.

DES

Sicherheit von DES:

- Exportversionen von DES haben sogar nur 40 Bit Schlüssel!
- Triple-DES (EDE) mit ca. 112 Bit effektiver Schlüssellänge.

Moore’s Law: Rechenleistung verdoppelt sich alle 18 Monate.

Also alle 15 Jahre 10 Bit Reduktion der Sicherheit im bezug auf die benötigte Zeit.

Heutzutage werden mindestens 128 Bit Schlüssellänge und Blocklänge angestrebt.

Advanced Encryption Standard - AES

Reaktion auf den auslaufenden DES (langsamen Tripel-DES).

1997 Ausschreibung vom NIST für Nachfolger von DES.

- Blockchiffre mit 128 Bit Blocklänge, 128/192/256 Bit Schlüssellänge.
- Offene Dokumentation, Referenzimplementierungen.
- Bedingung: nicht patentiert, frei verwendbar.
- Offener, internationaler Prozess.
- 1999: Fünf Kandidaten: MARS, RC6, Rijndael, Serpent, Twofish.
- 2000/2001: Rijndael wird AES.

Alle fünf Kandidaten wurden als sicher eingestuft.

Wird von US Behörden benutzt (für „sensitive“, nicht „classified“ Daten). Weite Verbreitung (zu erwarten).