DES – der *D*ata *E*ncryption *S*tandard

Steffen Glückselig, 22. Mai 2002

1 Geschichte

- 1970 entwickelt *Horst Feistel* das nach ihm benannte ‚Framework' für Verschlüsselungsverfahren.
- **IBM** entwickelt mit Unterstützung durch die US-Behörde **NSA** den DES-Algorithmus, der auf dem Feistel-Chiffre aufbaut.
- 1977 wird DES als Standard durch die US-Regierung zur Verschlüsselung von „nicht klassifizierten" Daten freigegeben.
- 1981 wird der Algorithmus veröffentlicht; 1994 erlaubt **NIST**[1] die Software-Implementierung.
- Seit 1999 wird einfaches DES als unsicher eingestuft. Es wird empfohlen auf 3DES oder AES umzurüsten.

2 Bechreibung des Algorithmus

Bei DES handelt es sich um eine symmetrische 64-bit[2] Blockchiffre (bzw. Produktchiffre[3]), die auf einem Feistel-Chiffre basiert. Den DES-Algorithmus kann man in drei Schritte untergliedern:

1. *initiale Permutation*, **IP**
2. 16-Runden Feistel-Chiffre mit spezifischer Verschlüsselungsfunktion f_K
3. Umkehrung der *initialen Permutation*, $\mathbf{IP}^{-1}$

Die Permutationen **IP**, $\mathbf{IP}^{-1}$, und $\mathbf{PC}_1$[4] sind für die kryptografische Stärke des Algorithmus nicht wesentlich, sondern sollen einen Angriff ohne spezielle Hardware erschweren.
Die Permutation **P** am Ende der DES-Verschlüsselungsfunktion und die **S(upstitutions)-Boxen** sind hingegen *zentral* für die Widerstandsfähigkeit des Algorithmus gegen kryptanalitische Angriffe.

3 Sicherheit

Seit seiner Veröffentlichung 1981 wird der DES-Algorithmus ausgiebig untersucht. Bisher konnten keine fatalen Schwächen gefunden werden.
Es gibt sogenannte *schwache* und *semi-schwache* Schlüssel, bei denen zweimaliges Verschlüsseln mit demselben Schlüssel einer Entschlüsselung gleichkommt bzw. bei denen ein Schlüssel als Inverses eines anderen fungiert:

$$\begin{aligned} E1(E1(P)) &= P && \text{für schwache Schlüssel} \\ E2(E1(P)) &= P && \text{für semi-schwache Schlüssel} \end{aligned}$$

Es gibt vier schwache und 12 semi-schwache Schlüssel.

Der Algorithmus hat also zwar keine fatale Schwäche, jedoch hat die RSA-**Challenge-III** vom Januar 1999 gezeigt, dass der DES-Schlüsselraum heutzutage innerhalb kürzester Zeit (gut 22 Stunden) Dank verteilter Berechnung vollständig durchsucht werden kann (durch **ElectronicFrontierFoundation** und **distributed.net**).
Da f_K mit der Hintereinanderausführung keine (Halb-)Gruppe bildet, d.h. es gibt kein k für feste k_1, k_2, so dass $DES_{k_1} \circ DES_{k_2} = DES_k$ gilt, ist 3DES (Triple-DES) in der Form

$$E_{k_1}[D_{k_2}[E_{k_3}[P]]]^5 \qquad \text{bzw.} \qquad E_{k_1}[E_{k_2}[E_{k_3}[P]]]$$

kryptographisch echt stärker.

---

[1] National Institute of Standards and Technology
[2] wegen der Festlegung von 8bit als Prüfsummenbits handelt es sich effektiv nur um 56-bit
[3] aus der Hintereinanderausführung verschiedener kryptografisch schwacher Operationen (Permutation, Verschiebung, Addition) resultierende starke Verschlüsselung
[4] wird bei der Generierung der Rundenschlüssel verwendet
[5] dieser Modus dient zur Kompatibilität zu einfachem DES: setze $\mathrm{k}_1 = \mathrm{k}_2 = \mathrm{k}_3$ oder $\mathrm{k}_2 = \mathrm{k}_3$.