DuD
Datenschutz und Datensicherheit

Data Encryption Standard (DES)

Dirk Fox

Gateway (Tor, Durchgang) ist ein Vermittlungscomputer, der zwei unterschiedliche, aber gleichartige Kommunikationssysteme verbindet. Dazu setzt er die Kommunikationsregeln (Protokolle) des einen in die des anderen um. So ermöglicht er den Teilnehmern beider Systeme, sich zu verständigen. In unserem „Gateway" werden Juristen technische und Technikern juristische Begriffe erläutert.

Historie

Der „Data Encryption Algorithm" (DEA) ist das erste und bis heute einzige in einem internationalen Standard spezifizierte Verschlüsselungsverfahren (DES). Auf Initiative des amerikanischen National Bureau of Standards (NBS), dem Vorläufer des heutigen National Institute of Standards and Technology (NIST), entwickelte IBM die Chiffre *Lucifer*, die 1975 zur Standardisierung vorgeschlagen wurde. Die National Security Agency (NSA) modifizierte den Algorithmus: Die internen Substitutionen wurden verändert, und die Schlüssellänge von 128 bit auf 56 bit verkürzt. Dieses Verfahren wurde – ungeachtet Protesten aus der Fachwelt – 1977 amerikanischer Standard [NSA_77].

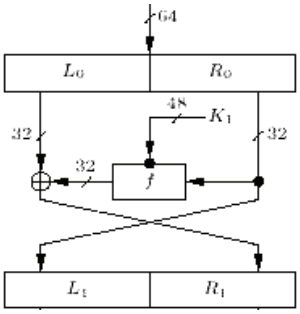
Funktionsweise

Der DES ist eine *Blockchiffre*. Das bedeutet, dass jeweils eine feste Zahl von Klartextzeichen in einem Verschlüsselungsschritt verschlüsselt wird. Die Blocklänge (= Zahl der in einem Schritt verschlüsselten Zeichen) beträgt 64 bit.

Der DES arbeitet nach dem Prinzip einer *Feistel-Chiffre*. Das bedeutet, dass ein Klartextblock zunächst in zwei Teile zu 32 bit zerlegt wird. Diese beiden Blockhälften L (links) und R (rechts) werden dann in mehreren Durchläufen (Runden) wie folgt verarbeitet (siehe Bild):

- Die rechte Blockhälfte wird zur linken.
- Die linke Blockhälfte wird, verknüpft mit dem Ergebnis einer Verschlüsselungsfunktion *f*, angewendet auf die rechte Blockhälfte, zur rechten.

Die interne Verschlüsselungsfunktion *f* hängt dabei ab von einem Teilschlüssel *k*, der aus dem DES-Schlüssel abgeleitet wird. *f* arbeitet nach dem Prinzip einer *Produktchiffre*, d. h. verwendet unterschiedliche Transformationsarten für die Verschlüsselung der Blockhälfte. Beim DES kommen hier Transpositionen (Vertauschungen) und



Substitutionen (Ersetzungen) zur Anwendung. Die Substitutionen werden durch sogenannte S-Boxen festgelegt; sie sind der kryptographische Kern des DES. Etwas formaler ausgedrückt passiert also in jeder der insgesamt 16 DES-Runden *i* das Folgende:

$$L_{i-1} \Rightarrow R_i$$
$$f(k_i, R_{i-1}) \text{ XOR } L_{i-1} \Rightarrow L_i$$

Die 16 Teilschlüssel k_i werden dabei aus dem DES-Schlüssel *k* abgeleitet.

Sicherheit

Die Sicherheit des DES wurde bereits kurz nach seiner Veröffentlichung kritisiert. Diffie und Hellman skizzierten 1977 die Konstruktion eines DES-Chips, der 2^{48} Schlüssel in weniger als sechs Minuten durchprobieren könnte [DiHe_77]. Durch die Geheimhaltung der Entwurfskriterien der (für die kryptographische Stärke des DES entscheidenden) S-Boxen bis Anfang der 90er Jahre hielt sich außerdem der Verdacht, dass die NSA eine Hintertür eingebaut hätte.

Systematische Methoden zur Kryptoanalyse des DES, die schneller als ein Durchprobieren aller Schlüssel arbeiten, wurden allerdings erst 1990 gefunden: Das Verfahren der *Differentiellen Kryptoanalyse* von Biham und Shamir erlaubt eine Entschlüsselung in 2^{37} Schritten, sofern 2^{47} ausgewählte Klar- und Schlüsseltextpaare vorliegen – eine in der Praxis wenig realistische Annahme. Auch bei der *Linearen Kryptoanalyse* von Matsui sind 2^{43} bekannte Klar- und Schlüsseltextpaare erforderlich, um den Entschlüsselungsaufwand auf 2^{43} Schritte zu verringern.

Den „Todesstoß" versetzte dem DES allerdings der Nachweis, dass mit heutiger Computerleistung ein vollständiges Durchsuchen des Schlüsselraums in kurzer Zeit möglich ist: 1997 gelang eine Entschlüsselung im Internet nach 140 Tagen, Anfang 1998 benötigte ein vergleichbarer Angriff nur noch 39 Tage. Im Juli 1999 schließlich präsentierte die Electronic Frontier Foundation (EFF) eine DES-Entschlüsselungsmaschine mit 1.800 Spezialchips („Deep Crack"), die einen DES-Schlüssel in weniger als 56 Stunden fand.

Heutiger Stand

Der DES ist auch heute noch das meistgenutzte symmetrische Verschlüsselungsverfahren. Seit Oktober 1999 empfiehlt das NIST bis zur Verabschiedung des Advanced Encryption Standards (AES) die Ersetzung des DES im kommerziellen Bereich durch Triple DES – eine dreifache DES-Verschlüsselung mit einem, zwei oder drei verschiedenen DES-Schlüsseln. Dadurch wächst die Schlüssellänge auf bis zu 168 bit [NIST_99].

Literatur

[DiHe_77] Diffie, W.; Hellman, Martin E.: *Exhaustive cryptanalysis of the NBS data encryption standard*. Computer, 6/1977, S. 74-84.

[NBS_77] National Bureau of Standards (NBS): *Data Encryption Standard (DES)*. Federal Information Processing Standards Publication (FIPS-PUB) 46-1, US Department of Commerce, Jan. 1977.

[NIST_99] National Institute of Standards and Technology (NIST): *Data Encryption Standard (DES)*. Federal Information Processing Standards Publication 46-3 (FIPS-PUB), Oct. 1999.