Übungen zur Kryptologie 1 Sommersemester 2002
Johannes Köbler/Olaf Beyersdorff

Übungsblatt 11

Aufgabe 38

a) Ermitteln Sie den 64-Bit-Schlüsselblock, der (bei ungerader Parität) zum 56-Bit-DES-Schlüssel `01 23 45 67 89 AB CD` (Hexadezimaldarstellung) gehört.

b) Zeigen Sie: $\mathrm{DES}(\overline{K}, \overline{x}) = \overline{\mathrm{DES}(K, x)}$. ($\overline{x}$ ist die bitweise Negation von x.)

c) Zeichnen Sie das Berechnungsdiagramm des DES-Schlüsselgenerators, der die Rundenschlüssel $K^1, \ldots, K^{16}$ in der umgekehrten Reihenfolge generiert.

Aufgabe 39 (schriftlich, 10 Punkte)

a) Alice verschlüsselt die Klartextblöcke $x_1, x_2, \ldots, x_n$ mit einer Blockchiffre zu Kryptotextblöcken $y_1, y_2, \ldots, y_n$ und sendet sie an Bob, der sie wieder entschlüsselt. Wie viele Klartextblöcke werden durch einen bei der Übertragung von Block y_i auftretenden Fehler maximal verfälscht, wenn der ECB-, CBC-, CFB- bzw. OFB-Mode benutzt wird.

b) Wie wirkt sich der Verlust eines Blockes y_i bei der Übertragung auf den von Bob berechneten Klartext aus?

Aufgabe 40

Sei S eine Blockchiffre mit Blocklänge l und Schlüssellänge k. Wir betrachten einen Angriff bei *bekanntem Klartext*, d.h. es steht eine ausreichende Zahl von Klartext-Kryptotext-Paaren (x_i, y_i), $i = 1, \ldots, n$ zur Verfügung.

a) Bestimmen Sie grob die erwartete Anzahl von Schlüsseln K mit $S(K, x_i) = y_i$ für $i = 1, \ldots, n$. Wie lässt sich im Fall $n \geq k/l$ mittels $n2^k$ Verschlüsselungen der Schlüssel bestimmen?

b) Um die Sicherheit zu erhöhen wird nun das Kryptosystem $S \times S$ verwendet, d.h. es gibt nun 2^{2k} Schlüssel (K, K'). Zeigen Sie, wie sich im Fall $n \geq 2k/l$ mittels $n2^{k+1}$ Ver- und Entschlüsselungen der Schlüssel bestimmen lässt. Wie viel Speicherplatz benötigt Ihr Algorithmus?

c) Überlegen Sie sich, wie man den Platzbedarf in b) reduzieren kann, wenn man mehr Rechenzeit zur Verfügung stellt.

Suchen Sie nach einer möglichst allgemeinen Beziehung für diesen so genannten Time-Memory-Tradeoff.