Aufgaben

3.1. In Abschnitt 3.5.2 wurde gesagt, dass die S-Boxen die einzigen nichtlinearen Komponenten von DES sind und dass diese Eigenschaft für die Sicherheit von großer Bedeutung ist. Nachfolgend verifizieren wir die Nichtlinearität der S-Box S_1 für einige Eingangswerte.

Zeigen Sie, dass $S_1(x_1) \oplus S_1(x_2) \neq S_1(x_1 \oplus x_2)$ gilt, wobei "$\oplus$" eine bitweise XOR-Verknüpfung ist.

1. $x_1 = 000000, x_2 = 000001$
2. $x_1 = 111111, x_2 = 100000$
3. $x_1 = 101010, x_2 = 010101$

3.2. Wir möchten verifizieren, dass $IP(\cdot)$ und $IP^{-1}(\cdot)$ tatsächlich inverse Operationen darstellen. Wir betrachten den 64-Bit-Vektor $x = (x_1, x_2, \ldots, x_{64})$. Zeigen Sie, dass $IP^{-1}(IP(x)) = x$ für die ersten fünf Bit von x gilt, d. h. für x_i, $i = 1,2,3,4,5$.

3.3. Wie lautet der 64-Bit-Ausgangswert der ersten DES-Runde, wenn die Klartext- und die Schlüsselbits alle null sind?

3.4. Was ist der Ausgangswert der ersten DES-Runde, wenn die Klartext- und die Schlüsselbits alle den Wert eins haben?

3.5. Eine wichtige Eigenschaft von Blockchiffren ist die Diffusion, d. h. die Änderung eines Eingangsbits soll die Änderung vieler Ausgangsbits zur Folge haben. In dieser Aufgabe untersuchen wir diese auch Avalanche-Effekt (Lawineneffekt) genannte Eigenschaft.

Der DES-Eingang sei ein 64-Bit-Wort, dass nur aus Nullen besteht, bis auf Bit Nummer 57, welches den Wert "1" hat. (Man beachte, dass das Eingangswort zunächst die Anfangspermutation durchläuft.)

1. Für welche S-Boxen der ersten Runde ändert sich der Eingangswert verglichen mit dem Fall, bei dem alle 64 Klartextbits den Wert 0 haben?
2. Was ist die minimale Anzahl der S-Box-Ausgangsbits, die sich ändern werden, wenn man nur die Entwurfskriterien der S-Boxen in Betracht zieht (und nicht die tatsächlichen Eingangswerte)?
3. Wie lautet der Ausgang nach der ersten Runde?
4. Wie viele Ausgangsbits nach der ersten Runde haben sich tatsächlich verändert verglichen mit dem Fall, bei dem alle Klartextbits den Wert 0 hatten? (Wir betrachten hier nur die Veränderung nach einer Runde. Der wirkliche Lawineneffekt kommt zustande, wenn man die nachfolgenden Runden betrachtet.)

3.6. Ein weitere wichtige Eigenschaft von Blockchiffren ist, dass eine minimale Änderung im Schlüssel den Ausgang, d. h. das Chiffrat, stark beeinflusst.

1. Gegeben sei eine DES-Verschlüsselung mit einem gegebenen Schlüssel. Nun ändert das Schlüsselbit an Position 1 (noch vor $PC-1$) seinen Wert. Welche S-Boxen in welchen Runden werden bei der DES-Verschlüsselung hierdurch beeinflusst?

2. Welche S-Boxen in welchen Runden werden bei der DES-Dechiffrierung beeinflusst?

3.7. Ein DES-Schlüssel K_w ist ein sogenannter *schwacher Schlüssel* (*weak key*), wenn Ver- und Entschlüsselung die gleiche Operation sind:

$$\mathrm{DES}_{K_w}(x) = \mathrm{DES}^{-1}_{K_w}(x), \text{ für alle } x \tag{3.1}$$

1. Welche Beziehung müssen die Unterschlüssel der Ver- und Entschlüsselung aufweisen, damit Bedingung (3.1) erfüllt ist?
2. Es gibt vier schwache DES-Schlüssel. Wie lauten diese?
3. Wie wahrscheinlich ist es, dass ein zufällig gewählter Schlüssel ein schwacher Schlüssel ist?

3.8. DES hat eine ungewöhnliche Eigenschaft, wenn man die bitweisen Komplemente der Ein- und Ausgänge betrachtet. Wir untersuchen die Komplementeigenschaft in dieser Aufgabe.

Das bitweise Komplement (d. h. Einsen werden Nullen und umgekehrt) eines Wortes A wird mit A' bezeichnet. Wie üblich, steht das Symbol $\oplus$ für die bitweise XOR-Verknüpfung. Ziel ist es, zu zeigen, dass für das Tripel (x, y, k) mit

$$y = \mathrm{DES}_k(x)$$

das Folgende auch gilt:

$$y' = \mathrm{DES}_{k'}(x'). \tag{3.2}$$

In Worten ausgedrückt: Gegeben sei DES mit einem Paar Klar-/Geheimtext sowie dem Schlüssel. Wenn man nun das Komplement des Klartextes und des Schlüssels bildet, so ist das resultierende Chiffrat ebenfalls das Komplement des ursprünglichen Chiffrats. Um die Komplementeigenschaft zu beweisen, zeigen Sie, dass die folgenden Schritte gelten:

1. Zeigen Sie, dass für Wörter (A, B) mit gleicher Bitlänge das Folgende gilt:

   $$A' \oplus B' = A \oplus B$$

   und

   $$A' \oplus B = (A \oplus B)'$$

2. Zeigen Sie, dass gilt: $PC-1(k') = (PC-1(k))'$.
3. Zeigen Sie, dass gilt: $LS_i(C'_{i-1}) = (LS_i(C_{i-1}))'$.
4. Zeigen Sie unter Verwendung der beiden obigen Resultate, dass, wenn k_i die Unterschlüssel von k sind, die Unterschlüssel von k' die Werte k'_i sind, wobei $i = 1, 2, \ldots, 16$.
5. Zeigen Sie, dass gilt: $IP(x') = (IP(x))'$.
6. Zeigen Sie, dass gilt: $E(R'_i) = (E(R_i))'$.
7. Zeigen Sie unter Verwendung der vorherigen Schritte, dass, wenn (R_{i-1}, L_{i-1}, k_i) den Wert R_i erzeugen, dann erzeugen $(R'_{i-1}, L'_{i-1}, k'_i)$ den Wert R'_i.

8. Zeigen Sie die Korrektheit von Gleichung (3.2).

3.9. Wir betrachten einen DES-Angriff per vollständiger Schlüsselsuche. Geben sei ein Paar Klartext/Chiffrat. Wie viele Schlüssel muss man (i) maximal testen und (ii) im Durchschnitt testen, bis man den Schlüssel gefunden hat?

3.10. In dieser Aufgabe untersuchen wir Taktraten, mit der DES in Hardware getaktet werden muss, um hohe Durchsatzraten zu erzielen. Der Durchsatz wird im Wesentlichen von der Geschwindigkeit einer DES-Runde bestimmt. Das Hardware-Modul für eine DES-Runde wird 16-mal iteriert, um die vollständige Verschlüsselung durchzuführen. (Alternativ können auch alle 16 Runden hintereinander in Hardware in einer sogenannten Pipeline realisiert werden. Dies führt zu einem sehr hohen Durchsatz, aber auch zu hohen Hardware-Kosten.)

1. Wir nehmen an, dass eine Runde in einem Taktzyklus ausgeführt werden kann. Wie lautet die Formel für die Taktfrequenz, um einn Verschlüsselungsrate von r [Bit/s] zu erzielen? Wir ignorieren hierbei die Eingangs- und Endpermutation.
2. Welche Taktrate ist für eine Verschlüsselungsgeschwindigkeit von 1 Gbit/s erforderlich? Und welche Taktrate für eine Verschlüsselungsgeschwindigkeit von 8 Gbit/s?

3.11. Wie in Abschnitt 3.5.1 beschrieben, kann man mit dem COPACABANA-Spezialrechner kostengünstig Brute-Force-Angriffe durchführen. Nachfolgend betrachten wir Angriffe auf DES.

1. Berechnen Sie die durchschnittliche Laufzeit für eine vollständige Schlüsselsuche unter den folgenden Annahmen:
   - COPACOBANA besteht aus 20 Einsteckmodulen
   - jedes Modul ist mit 6 FPGAs (dies sind programmierbare Hardware-Bausteine) bestückt
   - in jedem FPGA sind 4 DES-Kerne implementiert
   - jeder DES-Kern besteht aus einer sog. Pipeline-Architektur, so dass in jedem Taktzyklus eine vollständige Ver- bzw. Entschlüsselung stattfindet
   - die Taktfrequenz beträgt 100 MHz
2. Wie viele COPACOBANA-Maschinen werden benötigt, wenn eine durchschnittliche DES-Schlüsselsuche eine Stunde betragen soll?
3. Warum ist der COPACOBANA-Angriff nur eine obere Schranke für die Angriffszeit auf DES?

3.12. In diese Aufgabe betrachten wir eine Software zur Datei-Verschlüsselung, die in den 1990er Jahren verbreitet war. Zur Verschlüsselung wurde der normale DES mit 56-Bit-Schlüsseln verwendet. Zu der damaligen Zeit waren Computer und Hardware-Chips noch bedeutend langsamer, so dass eine vollständige Schlüsselsuche erheblicher schwerer war und DES für viele Anwendungen ausreichend Schutz bot. Unglücklicherweise gab es allerdings eine Schwachstelle in der Schlüsselableitung, die im Folgenden analysiert wird. Wir nehmen an, dass man mit einen konventionellen PC 10^6 Schlüssel pro Sekunde testen kann.

Der Schlüssel wird durch ein Passwort gebildet, welches aus 8 Zeichen besteht. Der Schlüssel ist einfach die Aneinanderreihung von 8 ASCII-Zeichen, so dass sich insgesamt $64 = 8 \cdot 8$ Schlüsselbits ergeben. Wie bekannt ignoriert die Permutation $PC-1$ das LSB (least significant bit) jedes ASCII-Zeichens, so dass sich effektiv 56 Schlüsselbits ergeben.

1. Wie groß ist der Schlüsselraum, wenn alle 8 Passwortzeichen zufällig gewählte 8-Bit-ASCII-Zeichen sind? Wie lange dauert eine vollständige Schlüsselsuche im Durchschnitt mit einem einzelnen PC?
2. Wie viele Schlüsselbits gibt es, wenn alle 8 Passwortzeichen zufällig gewählte 7-Bit-ASCII-Zeichen sind, d. h. die MSBs haben alle den Wert null. Wie lange dauert durchschnittlich eine vollständige Schlüsselsuche mit einem PC?
3. Wie groß ist der Schlüsselraum, wenn neben der Einschränkung aus dem Aufgabenteil 2 nur Buchstaben für das Passwort verwendet werden? Ein Besonderheit der Software war, dass alle Buchstaben zunächst in Großbuchstaben konvertiert wurden, bevor der DES-Schlüssel gebildet wurde. Wie lange dauert eine vollständige Schlüsselsuche im Durchschnitt mit einem einzelnen PC?

3.13. In dieser Aufgaben betrachten wir die Lightweight-Chiffre PRESENT.

1. Berechnen Sie den Zustand von PRESENT-80 nach der ersten Runde. Es werden die folgenden Eingangswerte benutzt (Angaben in Hexadezimal-Notation):
   Klartext = `0000 0000 0000 0000`,
   Schlüssel = `BBBB 5555 5555 EEEE FFFF`.
   Benutzen Sie die folgende Tabelle, um das Problem mit Papier und Bleistift zu lösen.

Klartext	`0000 0000 0000 0000`
Rundenschlüssel	
Zustand nach addRoundKey	
Zustand nach sBoxLayer	
Zustand nach pLayer	

2. Berechnen Sie nun den Rundenschlüssel für die zweite Runde unter Benutzung der nachfolgenden Tabelle.

Schlüssel	`BBBB 5555 5555 EEEE FFFF`
Schlüssel nach Rotation	
Schlüssel nach S-Box	
Schlüssel nach Round Counter	
2. Rundenschlüssel	