Einführung i. d. Kryptographie - Übung 7

2025-01-22

Aufgabe 1

Ver- und Entschlüsseln Sie mithilfe eines Feistelnetzwerkes mit Rundenfunktion $F(R_i, K_i)$ und 4 Runden den Klartext P, bestehend aus den beiden Hälften L_0 und R_0 . Verwenden Sie dafür die Rundenschlüssel $K_1, \ldots, K_4$.

- Wie viele Runden benötigen Sie mindestens, um jede Hälfte von P verarbeitet zu haben?
- Wie müssen die Hälften vertauscht werden, damit die Entschlüsselung mit demselben Netzwerk funktioniert?

Verschlüsselung

Nach der 1. Runde:

$$
\begin{aligned}
L_1 &= R_0 && (1)\\
R_1 &= L_0 \oplus F(R_0, K_1) && (2)
\end{aligned}
$$

Die rechte Seite ist noch im Klartext, die linke ist XORed mit der verschlüsselten Hälfte.

2. Runde:

$$
\begin{aligned}
L_2 &= R_1 && (3)\\
&= L_0 \oplus F(R_0, K_1) && (4)\\
R_2 &= L_1 \oplus F(R_1, K_2) && (5)\\
&= R_0 \oplus F(L_0 \oplus F(R_0, K_1), K_2) && (6)
\end{aligned}
$$

Jetzt wurden beide Hälften bereits verschlüsselt.

3. Runde:

$$
\begin{aligned}
L_3 &= R_2 && (7)\\
R_3 &= L_2 \oplus F(R_2, K_3) && (8)
\end{aligned}
$$

4. Runde:

$$
\begin{aligned}
L_4 &= R_3 && (9)\\
R_4 &= L_3 \oplus F(R_3, K_4) && (10)
\end{aligned}
$$

Entschlüsselung

Zum Entschlüsseln von $C = (L_4, R_4)$ wenden wir das Feistelnetzwerk mit den Schlüsseln $K_4, \dots, K_1$ in umgekehrter Reihenfolge und den Text $(L'_0 = R_4, R'_0 = L_4)$ an:

1. Runde:

$$\begin{aligned}
L'_1 &= R'_0 = L_4 \overset{(9)}{=} R_3 \\
R'_1 &= L'_0 \oplus F(R'_0, K_4) \\
&= R_4 \oplus F(L_4, K_4) \\
&= R_4 \oplus F(R_3, K_4) \\
&\overset{(10)}{=} \big(L_3 \oplus F(R_3, K_4)\big) \oplus F(R_3, K_4) \\
&= L_3
\end{aligned}$$

Die rechte Seite ist noch im Klartext, die linke ist XORed mit der verschlüsselten Hälfte.

2. Runde:

$$\begin{aligned}
L'_2 &= R'_1 = L_3 \overset{(7)}{=} R_2 \\
R'_2 &= L'_1 \oplus F(R'_1, K_3) \\
&= R_3 \oplus F(R_2, K_3) \\
&\overset{(8)}{=} \big(L_2 \oplus F(R_2, K_3)\big) \oplus F(R_2, K_3) \\
&= L_2
\end{aligned}$$

3. Runde:

$$\begin{aligned}
L'_3 &= R'_2 = L_2 \overset{(3)}{=} R_1 \\
R'_3 &= L'_2 \oplus F(R'_2, K_2) \\
&= R_2 \oplus F(R_1, K_2) \\
&\overset{(5)}{=} \big(L_1 \oplus F(R_1, K_2)\big) \oplus F(R_1, K_2) \\
&= L_1
\end{aligned}$$

4. Runde:

$$\begin{aligned}
L'_4 &= R'_3 = L_1 \overset{(1)}{=} R_0 \\
R'_4 &= L'_3 \oplus F(R'_3, K_1) \\
&= R_1 \oplus F(R_0, K_1) \\
&\overset{(2)}{=} \big(L_0 \oplus F(R_0, K_1)\big) \oplus F(R_0, K_1) \\
&= L_0
\end{aligned}$$

Der Plaintext ergibt sich nach vertauschen $P = (R'_4, L'_4) = (L_0, P_0)$.

Aufgabe 2

Gegeben sei

$$2^x \mod 1155 = 338. \tag{11}$$

Bestimmen Sie x ohne Taschenrechner. Verwenden Sie die Primfaktorzerlegung des Modulus.

Wir wissen, $1155 = 3 \cdot 5 \cdot 7 \cdot 11$. Wenn $a \equiv b \mod (p \cdot q)$, dann gilt auch $a \equiv b \mod p$ und $a \equiv b \mod q$. Aus (11) können wir also folgende Bedingungen folgern:

$$2^x \mod 3 = 338 \mod 3 \equiv 2 \qquad \Rightarrow x \equiv 1 \mod 3 \tag{12}$$
$$2^x \mod 5 = 338 \mod 5 \equiv 3 \qquad \Rightarrow x \equiv 3 \mod 5 \tag{13}$$
$$2^x \mod 7 = 338 \mod 7 \equiv 2 \qquad \Rightarrow x \equiv 1 \mod 7 \tag{14}$$
$$2^x \mod 11 = 338 \mod 11 \equiv 8 \qquad \Rightarrow x \equiv 3 \mod 11 \tag{15}$$

So erhalten wir ein System Simultaner Kongruenzen (der Chinesische Restsatz garantiert uns, dass es eine Eindeutige Lösung gibt) und wir berechnen für jeden Primfaktor m_i die Werte $M_i = m/m_i$ und $y_i = M_i^{-1} \mod m_i$:

1. Kongruenz:
$$x \equiv 1 \mod 3$$
   a. $a_1 = 1$
   b. $M_1 = 1155/3 = 385$ und $385 \equiv 1 \mod 3$
   c. Weil $M_1 \equiv 1 \mod 3$, gilt $y_1 = 1$
2. Kongruenz:
$$x \equiv 3 \mod 5$$
   a. $a_2 = 3$
   b. $M_2 = 1155/5 = 231$ und $231 \equiv 1 \mod 5$
   c. Weil $M_2 \equiv 1 \mod 5$, gilt $y_2 = 1$
3. Kongruenz:
$$x \equiv 1 \mod 7$$
   a. $a_3 = 1$
   b. $M_3 = 1155/7 = 165$ und $165 \equiv 4 \mod 7$
   c. Weil $M_3 \equiv 4 \mod 7$, berechnen wir den erweiterten Euklid für 4 und 7 und erhalten $y_3 = 2$
4. Kongruenz:
$$x \equiv 3 \mod 11$$
   a. $a_4 = 3$
   b. $M_4 = 1155/11 = 105$ und $105 \equiv 6 \mod 11$
   c. Weil $M_4 \equiv 6 \mod 11$, berechnen wir den erweiterten Euklid für 6 und 11 und erhalten $y_4 = 2$

Wir berechnen $\sum_i (a_i \cdot y_i \cdot M_i) \mod 1155$, das ist

$$1 \cdot 1 \cdot 385 + 3 \cdot 1 \cdot 231 + 1 \cdot 2 \cdot 165 + 3 \cdot 2 \cdot 105 = 2038 \mod 1155 = 883$$

Es gilt $2^{883} \equiv 338 \mod 1155$.

Zusatz: weil $\varphi(1155) = 1155 \cdot \frac{2}{3}\frac{4}{5}\frac{6}{7}\frac{10}{11} = 2 \cdot 4 \cdot 6 \cdot 10 = 480$ finden wir sogar einen kleineren Exponenten, der die Gleichung erfüllt: $x = 403 \equiv 883 \mod \varphi(1155)$.

Aufgabe 3

Zeigen Sie (mittels Satz von Euler Fermat): Für jede natüliche Zahl a gilt $a^{13} \mod 10 = a \mod 10$

Fall 1: $\text{ggT}(a, 10) = 1$

Sei a teilerfemd zu 10, d.h. $\text{ggT}(a, 10) = 1$, dann können wir den Satz von Euler-Fermat anwenden, wir wissen $\varphi(10) = (5-1) \cdot (2-1) = 4$ und $13 = 3 \cdot \varphi(10) + 1$. Daher gilt

$$a^{13} \mod 10 = a^{3\cdot\varphi(10)+1} \mod 10 = \tag{16}$$

$$= \left(a^{\varphi(10)}\right)^3 \cdot a \mod 10 \equiv 1 \cdot a \mod 10 \tag{17}$$

Fall 2: $\text{ggT}(a, 10) = 10$

Weil $a \equiv 0 \mod 10$ das neutrale Element bzgl. der Multiplikation ist, gilt für diesen Fall sogar $a^k \equiv a \equiv 0 \mod 10$.

Fall 3: $\text{ggT}(a, 5) = 5$

Sei $a = 5k$ für ein $k \in \mathbb{Z}$. Wir betrachten

$$a^{13} \mod 10 = (5k)^{13} \mod 15 = 5^{13}k^{13} \mod 10. \tag{18}$$

Weil $\text{ggt}(a, 10) = \text{ggT}(5k, 10) = 5$ wissen wir, dass $\text{ggT}(k, 10) = 1$. Indem wir Euler-Fermat anwenden, vereinfachen wir (18) wie in Fall 1 und haben

$$a^{13} \mod 10 \equiv 5^{13} \mod 10 = 1220703125 \mod 10 \equiv 5, \tag{19}$$

wie behauptet.

Fall 4: $\text{ggT}(a, 10) = 2$

Analog zu Fall 3 vereinfachen wir

$$a^{13} \mod 10 \equiv 2^13 \mod 10 = 8192 \mod 10 \equiv 2 \tag{20}$$

Aufgabe 4

Alice und Bob vereinbaren mittels Diffie-Hellman einen symmetrischen Schlüssel. Bestimmen Sie für die folgende Primzahlen jeweils ein geeignetes g_i, a_i sowie b_i, und berechnen Sie jeweils k_i.

Sehen Sie Unterschiede zwischen den durch die Primzahlen jeweils aufgespannten multiplikativen Gruppen?

1. $p_1 = 47$
2. $p_2 = 31$

Für den Algorithmus brauchen wir $a, b < p - 1$ und ein $g < p$ und berechnen

1. $\alpha = g^a \mod p$ bzw. $\beta = g^b \mod p$
2. $k = \beta^a \mod p = \alpha^b \mod p$

Wir können die gleichen a, b, g für p_1 und p_2 wählen, wenn $a, b < p_2 - 1$ und $g < p_2$.

Sei $a = 7$, $b = 8$ und $g = 15$, dann haben wir

p	g	a	b	α	β	$\beta^a \mod p$	$\alpha^b \mod p$
47	15	7	10	40	36	16	16
31	15	7	10	23	4	16	16

Mir fällt kein Unterschied zwischen den Gruppen auf, außer, dass $(\mathbb{Z}/31\mathbb{Z})^*$ 30 Elemente und $(\mathbb{Z}/47\mathbb{Z})^*$ 46 Elemente haben.