FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2023/24
17.01.2024

Musterlösung zum 12. Übungsblatt zur Vorlesung Kryptologie

Übung 1

a) Alices öffentlicher Schlüssel ist (p, g, A) mit:

$$A \;=\; g^{\alpha} \bmod p \;=\; 5^{23} \bmod 37 \;=\; 20.$$

b) Bob berechnet:

$$\begin{aligned} B &= g^{\beta} \bmod p = 5^{7} \bmod 37 = 18, \\ c &= A^{\beta} \cdot m \bmod p = 20^{7} \cdot 15 \bmod 37 = 34. \end{aligned}$$

$(B, c) = (18, 34)$ ist der Geheimtext.

c) Zum Entschlüsseln berechnet Alice K und K^{-1} in $\mathbb{Z}_p$:

$$\begin{aligned} K &= B^{\alpha} \bmod p = 18^{23} \bmod 37 = 22, \\ K^{-1} &= 32. \end{aligned}$$

Der Klartext ergibt sich als:

$$m \;=\; K^{-1} \cdot c \bmod p \;=\; 32 \cdot 34 \bmod 37 \;=\; 15.$$

Übung 2

Zu zeigen ist $B^x = \left(A^{\beta}\right)^{-1} \bmod p$. Modulo p gilt:

$$\begin{aligned} A^{\beta} \cdot B^{x} &= A^{\beta} \cdot B^{p-1-\alpha} = \left(g^{\alpha}\right)^{\beta} \cdot \left(g^{\beta}\right)^{p-1-\alpha} \\ &= g^{\alpha\beta+\beta p-\beta-\beta\alpha} = g^{\beta(p-1)} \\ &= \left(g^{(p-1)}\right)^{\beta} = 1 \bmod p. \end{aligned}$$

Übung 3

a) Die Signatur ist das Tupel (r, s) mit $r = g^k \bmod p$ und $s = k^{-1}(m - \alpha r) \bmod (p-1)$, wobei $k^{-1} \cdot k = 1 \bmod (p-1)$ ist.

$$\begin{aligned} k^{-1} &= 25, \\ r &= 5^{13} \bmod 37 = 13, \\ s &= 25 \cdot (20 - 23 \cdot 13) \bmod 36 = 9. \end{aligned}$$

b) Überprüfe ob $A^r r^s = g^m \bmod p$:

$$20^{13} \cdot 13^9 \bmod 37 = 12 = 5^{20} \bmod 37.$$

Übung 4

Wählt man das gleiche k zur Signatur von m_1 und m_2, so erhält man das gleiche $r = g^k \bmod p$ und nur unterschiedliche s_1 und s_2 durch $s_i = k^{-1}(m_i - \alpha r) \bmod (p-1)$. Damit gilt

$$\begin{aligned} s_1 - s_2 &= k^{-1}(m_1 - \alpha r) - k^{-1}(m_2 - \alpha r) \bmod (p-1) \\ &= k^{-1}(m_1 - m_2) \bmod (p-1). \end{aligned}$$

Falls $\gcd(s_1 - s_2, p-1) = 1$ ist, kann man diese Gleichung eindeutig nach k auflösen:

$$k = (s_1 - s_2)^{-1}(m_1 - m_2) \bmod (p-1).$$

Damit ist beispielsweise in der Formel $s_1 = k^{-1}(m_1 - \alpha r) \bmod (p-1)$ alles außer α bekannt, und man kann, falls $\gcd(r, p-1) = 1$ ist, α berechnen.

Ist $\gcd(s_1 - s_2, p-1) \neq 1$, kann man zwar nicht eindeutig nach k auflösen, aber es gibt nur wenig mögliche k, die man dann ausprobieren kann. Ist $\gcd(r, p-1) \neq 1$, so ist α tatsächlich nicht eindeutig berechenbar. Zur Erzeugung von Signaturen reicht aber offensichtlich die Kenntnis von k und $\alpha r \bmod (p-1)$, so dass ein Angreifer Signaturen fälschen kann.

Übung 5

a) Einsetzen ergibt:

$$A^r r^s = A^r \left(g^u A^v\right)^s = A^r g^{su} A^{sv} = A^r g^{su} A^{-rv^{-1}v} = A^r g^m A^{-r} = g^m \bmod (p-1).$$

b) Wähle beispielsweise $u = 10$ und $v = 11$. Dann ist

$$\begin{aligned} r &= 5^{10} \cdot 20^{11} \bmod 37 = 2, \\ s &= -2 \cdot 11^{-1} \bmod 36 = 34 \cdot 23 \bmod 36 = 26, \\ m &= 26 \cdot 10 \bmod 36 = 8. \end{aligned}$$

Tatsächlich ist dann $20^2 \cdot 2^{26} \bmod 37 = 16 = 5^8 \bmod 37$.