Institut für Informatik
Prof. Dr. J. Rothe

Sommersemester 2024
Übungsblatt 6

Lösungsvorschläge

Kryptokomplexität II

Bearbeitungszeit: 14. Mai bis 24. Mai
Verantwortlich: Roman Zorn

Aufgabe 1: ElGamal – Known-Message-Angriff I

Betrachten Sie den in der Vorlesung beschriebenen Known-Message-Angriff auf das ElGamal-Protokoll für digitale Signaturen. Zeigen Sie, dass die dabei definierten Werte σ, ρ und m die Verifikationsbedingung

$$\gamma^m \equiv \beta^\sigma \cdot \sigma^\rho \mod p$$

tatsächlich erfüllen.

Lösungsvorschlag: Nur die öffentlichen Zahlen, also p, γ und β sowie die Signatur $(\hat{\sigma}, \hat{\rho})$ für $\hat{m}$ sind bekannt. Wir wissen, dass b, s existieren, sodass

$$\beta = \gamma^b \mod p, \tag{1}$$
$$\hat{\sigma} = \gamma^s \mod p, \tag{2}$$
$$\hat{\rho} = (\hat{m} - b\hat{\sigma})s^{-1} \mod p-1. \tag{3}$$

Nun soll eine Signatur gefälscht werden.
Dazu wählen wir $x, y, z \in \mathbb{Z}_{p-1}$ sodass $\text{ggT}\,(x\hat{\sigma} - z\hat{\rho}, p-1) = 1$. Des weiteren sind σ, ρ und m definiert durch

$$\sigma = \hat{\sigma}^x \gamma^y \beta^z \mod p, \tag{4}$$
$$\rho = \hat{\rho}\sigma(x\hat{\sigma} - z\hat{\rho})^{-1} \mod (p-1), \tag{5}$$
$$m = \sigma(x\hat{m} + y\hat{\rho})(x\hat{\sigma} - z\hat{\rho})^{-1} \mod (p-1). \tag{6}$$

Wir wollen nun zeigen, dass

$$\gamma^m \equiv \beta^\sigma \cdot \sigma^\rho \mod p. \tag{7}$$

Es gilt nach (1), (2) und (4)

$$\begin{aligned}\beta^\sigma \sigma^\rho &= \gamma^{b\sigma} \cdot (\hat{\sigma}^x \gamma^y \beta^z)^\rho \\ &= \gamma^{b\sigma} \gamma^{sx\rho} \gamma^{y\rho} \gamma^{bz\rho} \\ &= \gamma^{b\sigma + (sx+y+bz)\rho}.\end{aligned}$$

Um nun (7) zu zeigen, müssen wir zeigen, dass $\gamma^{b\sigma+(sx+y+bz)\rho} \equiv \gamma^m \mod p$ gilt. Unter Zuhilfenahme von Fermats kleinem Theorem, gilt für die Primzahl p für alle k, ℓ, dass $[\ell \equiv k \mod p-1] \Rightarrow [\gamma^k \equiv \gamma^\ell \mod p]$. Also genügt es zu zeigen, dass

$$b\sigma + (sx + y + bz)\rho \equiv m \mod p-1.$$

Es gilt

$$\begin{aligned}
& m = b\sigma + (sx + y + bz)\rho \\
\iff\ & 0 = b\sigma + (sx + y + bz)\rho - m \\
\overset{(6)}{\iff}\ & 0 = b\sigma + (sx + y + bz)\rho - \sigma(x\hat{m} + y\hat{\rho})(x\hat{\sigma} - z\hat{\rho})^{-1} \\
\overset{(5)}{\iff}\ & 0 = b\sigma + (sx + y + bz)(\hat{\rho}\sigma(x\hat{\sigma} - z\hat{\rho})^{-1}) - \sigma(x\hat{m} + y\hat{\rho})(x\hat{\sigma} - z\hat{\rho})^{-1} \\
\iff\ & 0 = b\sigma + \sigma(sx\hat{\rho} + y\hat{\rho} + bz\hat{\rho} - x\hat{m} - y\hat{\rho})(x\hat{\sigma} - z\hat{\rho})^{-1} \\
\overset{(3)}{\iff}\ & 0 = b\sigma + \sigma(sx(\hat{m} - b\hat{\sigma})s^{-1} + bz\hat{\rho} - x\hat{m})(x\hat{\sigma} - z\hat{\rho})^{-1} \\
\iff\ & 0 = b\sigma + \sigma(x\hat{m} - xb\hat{\sigma} + bz\hat{\rho} - x\hat{m})(x\hat{\sigma} - z\hat{\rho})^{-1} \\
\iff\ & 0 = b\sigma + \sigma(-xb\hat{\sigma} + bz\hat{\rho})(x\hat{\sigma} - z\hat{\rho})^{-1} \\
\iff\ & 0 = b\sigma + \sigma(-b(x\hat{\sigma} - z\hat{\rho}))(x\hat{\sigma} - z\hat{\rho})^{-1} \\
\iff\ & 0 = b\sigma - \sigma b \cdot 1 = 0.
\end{aligned}$$

Aufgabe 2: ElGamal – Known-Message-Angriff II

Betrachten Sie erneut den in der Vorlesung beschriebenen Known-Message-Angriff auf das ElGamal-Protokoll für digitale Signaturen. Seien $p = 401$ und $\gamma = 13$ bekannt. Angenommen, Erich kennt die Werte $\langle \hat{m}, \beta, (\hat{\sigma}, \hat{\rho}) \rangle = \langle 197,\ 37,\ (75, 344) \rangle$. Führen Sie einen Known-Message-Angriff auf das ElGamal Protokoll für digitale Signaturen mit den Werten $x = 221,\ y = 80$ und $z = 23$ aus.

(a) ► Zeigen Sie dazu zunächst, dass die Werte $x,\ y$ und z gültig sind.

Lösungsvorschlag: Wir zeigen, dass für x, y und z gilt $gcd(x\hat{\sigma} - z\hat{\rho}, p-1) = 1$.

$$gcd(221 \cdot 75 - 23 \cdot 344, 400) = gcd(8663, 400) = 1,$$

also sind x, y, z gültig.

(b) ► Führen Sie anschließend Erichs Angriff durch und geben Sie die gefälschte Signatur an.

Lösungsvorschlag: Bekannt sind $p = 401, \gamma = 13, \hat{m} = 197, \beta = 37, \hat{\sigma} = 75, \hat{\rho} = 344$ sowie die gewählten $x = 221, y = 80, z = 23$.

Zunächst berechnet Erich $(x\hat{\sigma} - z\hat{\rho})^{-1} \equiv 8663^{-1} \equiv 263^{-1} \equiv 327 \mod 400$. Nun

berechnet er

$$\begin{aligned}\sigma &= \hat{\sigma}^x \gamma^y \beta^z \mod p,\\ \rho &= \hat{\rho}\sigma(x\hat{\sigma} - z\hat{\rho})^{-1} \mod (p-1),\\ m &= \sigma(x\hat{m} + y\hat{\rho})(x\hat{\sigma} - z\hat{\rho})^{-1} \mod (p-1).\end{aligned}$$

Also:

$$\begin{aligned}\sigma &= \hat{\sigma}^x \gamma^y \beta^z\\ &= 75^{221} \cdot 13^{80} \cdot 37^{23} \equiv 190 \cdot 39 \cdot 124 \equiv 149 \mod 401,\\ \rho &= \hat{\rho}\sigma(x\hat{\sigma} - z\hat{\rho})^{-1}\\ &= 344 \cdot 149 \cdot 327 \equiv 312 \mod 400,\\ m &= \sigma(x\hat{m} + y\hat{\rho})(x\hat{\sigma} - z\hat{\rho})^{-1}\\ &= 149 \cdot (221 \cdot 197 + 80 \cdot 344) \cdot 327 \mod 400\\ &\equiv 149 \cdot 257 \cdot 327 \mod 400\\ &\equiv 211 \mod 400\end{aligned}$$

Also ist $(\sigma, \rho) = (149, 312)$ die gefälschte Signatur für $m = 211$.

Anmerkung: Um zu zeigen, dass diese Signatur gültig ist, prüfen wir

$$\begin{aligned}\gamma^m &\equiv \beta^\sigma \cdot \sigma^\rho && \mod 401\\ 13^{211} &\equiv 37^{149} \cdot 149^{312} && \mod 401\\ 279 &\equiv 46 \cdot 224 && \mod 401\\ 279 &\equiv 279 && \mod 401 \ \checkmark\end{aligned}$$

Aufgabe 3: Kryptographische Hash-Funktionen

Kryptographische Hash-Funktionen finden viele Anwendungen. Unter anderem wurden sie in der Vorlesung als mögliche Gegenmaßnahmen zum Fälschen einer Signatur vorgestellt.

(a) Betrachten Sie die folgende Hash-Funktion: $h(x) = x \mod 33$.

► Wie in Blatt 5 Aufgabe 3 seien die Parameter $p = 383, \gamma = 5, s = 29, b = 15$ für ElGamals Signatur-Schema gegeben. Signieren Sie $m = 54$ unter Verwendung der Hash-Funktion h.

► Geben Sie eine andere Nachricht m' an, für die diese Signatur ebenfalls gültig ist.

► Bewerten Sie, ob h eine geeignete Hash-Funktion für die Anwendung ist.

Lösungsvorschlag: Anstelle von $m = 54$ signieren wir $h(m) = 21$.

- $\beta = \gamma^b = 5^{15} \equiv 245 \mod 383$.
- $\sigma = \gamma^s \equiv 5^{29} \equiv 132 \mod 383$.
- $\rho \equiv (h(m) - b \cdot \sigma) \cdot s^{-1} \equiv (21 - 15 \cdot 132) \cdot 303 \equiv 51 \mod 382$

Die Signatur ist $\langle m, \beta, (\sigma, \rho)\rangle = \langle 54, 245, (132, 51)\rangle$. Zum Verifizieren prüft man die Kongruenz

$$\begin{aligned} \gamma^{h(m)} &\equiv \beta^\sigma \cdot \sigma^\rho \mod p \\ 5^{21} &\equiv 245^{132} \cdot 132^{51} \mod 383 \\ 40 &\equiv 110 \cdot 70 \mod 383 \\ 40 &\equiv 40 \mod 383 \quad \checkmark \end{aligned}$$

Die Signatur ist offensichtlich für alle m' gültig mit $m' \equiv 21 \mod 33$, also z.B. für $m' = 21$. Es ist also einfach ein m' zu finden mit $h(m) = h(m')$. Damit ist h keine geeignete Hash-Funktion.

(b) Heutzutage verwendet man oft den *secure hash algorithm (SHA)*. Je nach Version bildet er Daten auf eine Zahl fester Länge von $160, 224, 256$ bis hin zu 512 Bit ab. [1]

► Angenommen Sie verwenden zur Absicherung von Signaturen den *SHA-1* mit 160 Bit. Erich kann 10000 Nachrichten inklusive Hash pro Sekunde erzeugen. Wie lange wird Erich (näherungsweise) brauchen, bis er mit 50% Sicherheit eine zweite Nachricht m' mit gleichem Hash wie m gefunden hat? Gehen Sie davon aus, dass alle Hashes etwa gleich oft vorkommen.

Lösungsvorschlag: Wenn Erich zufällig eine Nachricht m' wählt, so hat er eine Chance von 2^{-160}, dass $SHA(m) = SHA(m')$.

Wir modellieren Erichs Suche als mehrfaches unabhängiges Raten einer Nachricht m' und lösen dazu $(1 - 2^{-160})^x = 0.5$ nach x auf. Näherungsweise wird die Gleichung für $x = 1.01 \cdot 10^{48}$ erfüllt. So viele Versuche braucht Erich also um mit 50% Sicherheit ein m' mit $SHA(m) = SHA(m')$ zu finden.

Da Erich 10000 Versuche pro Sekunde hat, ergibt sich ein Zeitaufwand von $1.01 \cdot 10^{44}$ Sekunden, also etwa $1.17 \cdot 10^{39}$ Tage oder $3.2 \cdot 10^{30}$ Jahrmillionen.

Aufgabe 4: Rabins Public-Key-Kryptosystem

Betrachten Sie das Kryptosystem von Rabin mit $p = 83$ und $q = 103$.

(a) ► Verschlüsseln Sie die Nachricht $m = 177$. Was sind der öffentliche und private Schlüssel?

[1] SHA-1 (mit 160 Bit) wird nicht mehr als Sicher eingestuft. SHA-256 ist heutzutage ein Mindeststandard.

Lösungsvorschlag: Wir bestimmen zunächst den öffentlichen Schlüssel n mit $n = p \cdot q = 83 \cdot 103 = 8549$. Den privaten Schlüssel bilden p und q.

Wir bestimmen $c \equiv m^2 \equiv 177^2 \equiv 5682 \mod 8549$. Die verschlüsselte Nachricht lautet also 5682.

(b) ► Berechnen Sie für den in Aufgabenteil (a) erhaltenen Ciphertext alle möglichen Klartexte.

Lösungsvorschlag: Gesucht sind alle m' mit $m' \equiv \sqrt{5682} \mod 8549$.

Nach der Vorlesung gilt für die Primzahlen p und q mit $p \equiv q \equiv 3 \mod 4$, dass $\sqrt{5682} \equiv +/- \ 5682^{(p+1)/4} \mod p$ und $\sqrt{5682} \equiv +/- \ 5682^{(q+1)/4} \mod q$. Wir berechnen die beiden positiven Wurzeln m_p und m_q.

$$\begin{aligned} m_p &:= 5682^{(p+1)/4} \mod p \\ &\equiv 5682^{(84)/4} \mod 83 \\ &\equiv 5682^{21} \mod 83 \\ &\equiv 11 \mod 83 \end{aligned}$$

$$\begin{aligned} m_q &:= 5682^{(q+1)/4} \mod q \\ &\equiv 5682^{(104)/4} \mod 103 \\ &\equiv 5682^{26} \mod 103 \\ &\equiv 29 \mod 103 \end{aligned}$$

Wir suchen nun Lösungen z_p, z_q für $z_p p + z_q q = 1$. Mit Hilfe des erweiterten Euklidischen Algorithmus erhält man $z_p = 36$ und $z_q = -29$.

Nun berechnen wir

$$\begin{aligned} s &= (z_p p m_q + z_q q m_p) \mod n \\ &= (36 \cdot 83 \cdot 29 + (-29) \cdot 103 \cdot 11)) \mod 8549 \\ &\equiv 53795 \mod 8549 \\ &\equiv 2501 \mod 8549 \\ t &= (z_p p m_q - z_q q m_p) \mod n \\ &= (36 \cdot 83 \cdot 29 + 29 \cdot 103 \cdot 11)) \mod 8549 \\ &\equiv 119509 \mod 8549 \\ &\equiv 8372 \mod 8549 \end{aligned}$$

Die Lösungen für $\sqrt{5682} \mod 8549$ sind nun $+/- \ s \mod 8549$ und $+/- \ t \mod 8549$, also $\{s, -s, t, -t\} = \{2501, 6048, 8372, 177\}$.

Es gilt tatsächlich:

$$c = 5682 \equiv 2501^2 \equiv 6048^2 \equiv 8372^2 \equiv 177^2 \mod 8549.$$

Anmerkung: Wir wissen natürlich, dass 177 *der Klartext war. Generell sind aber alle 4 Zahlen mögliche Klartexte.*