Übung zur Vorlesung „Sicherheit“
Übung 5

Thomas Agrikola
Thomas.Agrikola@kit.edu

06.07.2017

Socrative: Signaturen & Schlüsselaustausch

`https://b.socrative.com/login/student/`

Room: `SICHERHEIT`

- App um Quiz durchzuführen
- Zugang durch Browser oder App
- Als Quizteilnehmer kein Account notwendig.

Wiederholung ElGamal-Signaturen

$$a := g^e \quad \text{für zufälliges } e$$

$$b \quad \text{als Lösung von} \quad a \cdot x + e \cdot b = M \bmod |\mathbb{G}|$$

$$\mathrm{Sign}(sk, M) = (a, b)$$

$$\mathrm{Ver}(pk, M, \sigma) = 1 \quad :\Longleftrightarrow \quad (g^x)^a a^b = g^M$$

Möglicher Angriff:

- $a := g^{x+c}$ für zufälliges $c \in \mathbb{Z}_{|\mathbb{G}|}$
- $b := -a \bmod |\mathbb{G}|$
- $\sigma := (a, b)$ ist gültige Signatur für Nachricht

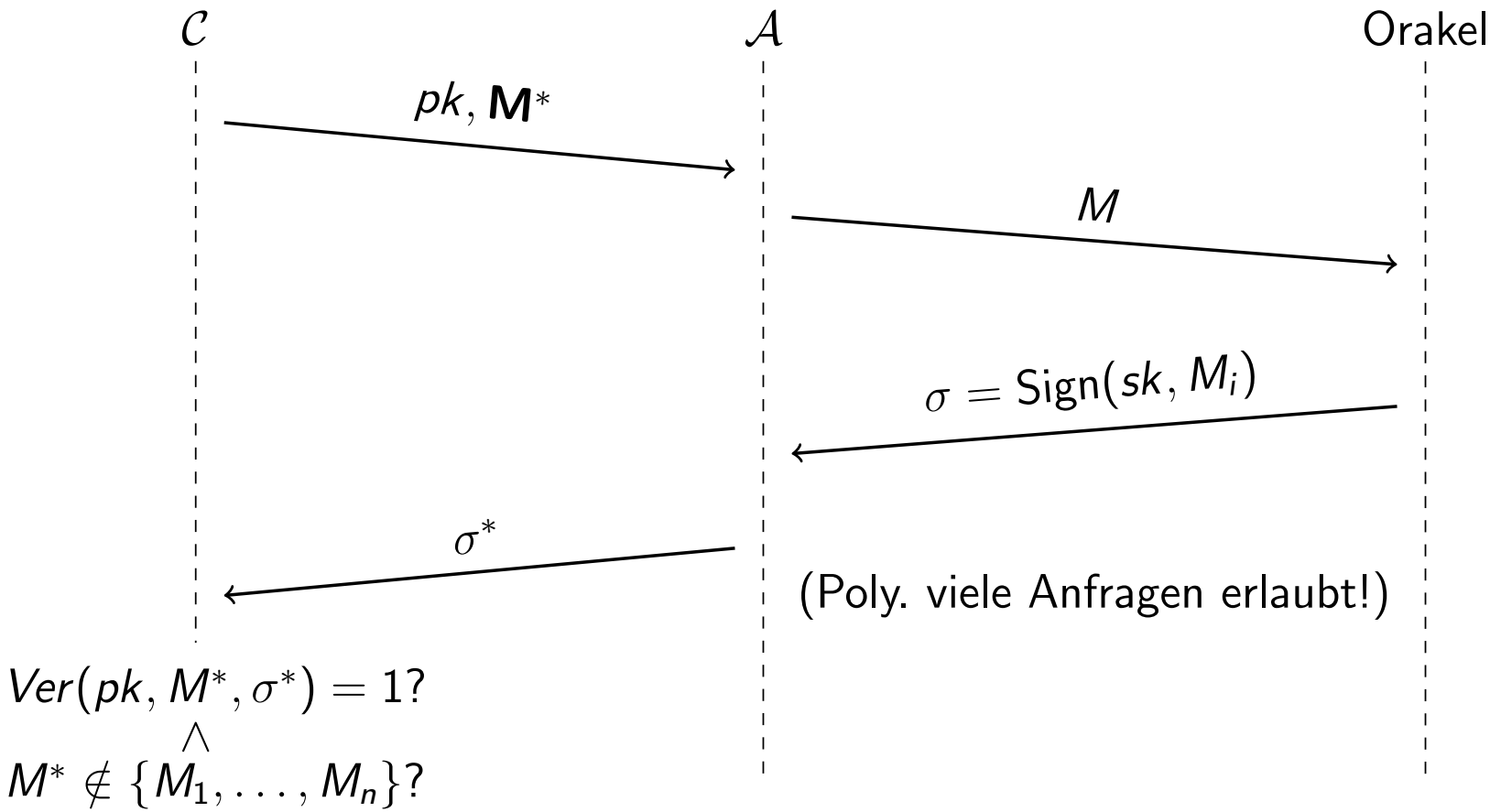
$$M = a \cdot x + e \cdot b = a \cdot x + (x + c) \cdot (-a) = -ac \bmod |\mathbb{G}|$$

Sicherheit – Übungsblatt 5 – Aufgabe 1 (1)

- Lehrbuch-RSA-Signaturen sind nicht EUF-CMA-sicher.
- Betrachte schwächeren Sicherheitsbegriff:
  - Wie EUF-CMA, aber...
  - Angreifer muss zu einer **vorgegebenen** Nachricht m^* eine Fälschung berechnen.
  - Angreifer darf keine Sign-Anfragen für m^* stellen.
- **Frage:** Erfüllen die Lehrbuch-RSA-Signaturen diesen Sicherheitsbegriff?

Sicherheit – Übungsblatt 5 – Neuer Sicherheitsbegriff

- Herausforderer $\mathcal{C}$ führt $(pk, sk) \leftarrow \mathrm{Gen}(1^k)$ aus.
- $\mathcal{C}$ stellt $\mathrm{Sign}(sk, \cdot)$-Orakel für $\mathcal{A}$ bereit.



Sicherheit – Übungsblatt 5 – Aufgabe 1 (1)

Antwort: Lehrbuch-RSA-Signaturen erfüllen neuen Sicherheitsbegriff nicht!

Betrachte folgenden Angreifer $\mathcal{A}$:

- $\mathcal{A}$ erhält den PK $(e, N = P \cdot Q)$ (P, Q prim) und $m^* \in \mathbb{Z}_N$.
- Annahme: m^* ist invertierbar
  - Ist m^* nicht invertierbar, so gilt

$$ggT(m^*, N) = P \vee ggT(m^*, N) = Q$$

    und wir könnten N faktorisieren...
  - .. und damit auch leicht Signaturen fälschen.
- Ziel: berechne σ^* mit $(\sigma^*)^e = m^* \bmod N$
- $\mathcal{A}$ zieht $x \leftarrow \mathbb{Z}_N^\times \setminus \{1\}$ ...
- ... und berechnet $y := x^e \bmod N$.

Sicherheit – Übungsblatt 5 – Aufgabe 1 (1)

- Beobachtung: $y = x^e \neq 1 \bmod N$ (für $x \in \mathbb{Z}_N^\times \setminus \{1\}$)
  - Angenommen $x^e = 1 \bmod N$, dann ist e ein Vielfaches der Ordnung von x.
  - Wegen Lagrange: $\varphi(N) = m \cdot ord(x)$.
  - Also $ggT(e, \varphi(N)) = k \cdot ord(x)$ für ein $k \in \mathbb{N}$.
  - Nach Voraussetzung gilt aber $ggT(e, \varphi(N)) = 1$.
  - Das geht nur, wenn $ord(x) = 1$ also $x = 1$ ist, aber $x \neq 1$. Widerspruch.
- $\mathcal{A}$ setzt $m_1 := m^* \cdot y \bmod N$.
- $m_1 \neq m^* \bmod N$, da $y \neq 1 \bmod N$ und m^* invertierbar.
- $\mathcal{A}$ schickt m_1 an das Sign-Orakel und erhält σ_1.
- Er gibt $\sigma^* = \sigma_1 \cdot x^{-1} \bmod N$ als Fälschung aus.
- (x^{-1} existiert, da $x \in \mathbb{Z}_N^\times$)

Sicherheit – Übungsblatt 5 – Aufgabe 1 (1)

σ^* ist eine gültige Fälschung, denn es gilt:

$$\begin{aligned}(\sigma^*)^e &= (\sigma_1 \cdot x^{-1})^e \bmod N \\ &= \sigma_1^e \cdot (x^e)^{-1} \bmod N \\ &= m_1 \cdot y^{-1} \bmod N \\ &= (m^* \cdot y) \cdot y^{-1} \bmod N \\ &= m^* \bmod N\end{aligned}$$

- Erfolgswkt. $= 1$
- Laufzeit: Polynomiell (simple Berechnungen, nur eine Sign-Anfrage)

Sicherheit – Übungsblatt 5 – Aufgabe 1 (1)

Fazit:

- Lehrbuch-RSA-Signaturen erfüllen auch schwache Sicherheitsbegriffe nicht.
- Sicherheitsbegriff: UUF-CMA (*universally unforgeable...*)
- Problem: Homomorphie

$\Rightarrow$ Lehrbuch-RSA-Signaturen nicht verwenden!

Sicherheit – Übungsblatt 5 – Aufgabe 1 (2)

Digital-Signature-Algorithmus (DSA) über $\mathbb{G} = Q(\mathbb{Z}_p^\times)$, für ungerades primes $p \in \mathbb{N}$.

- $Q(\mathbb{Z}_p^\times) := \{x^2 : x \in \mathbb{Z}_p^\times\}$ ist Menge der Quadrate in $\mathbb{Z}_p^\times$.
- $Q(\mathbb{Z}_p^\times)$ ist eine Untergruppe von $\mathbb{Z}_p^\times$.
- Es sei $p = 2q + 1$ mit $q = 11$ (Erinnerung, diese Primzahlen nennt man *Safe Primes* (oder auch *Strong Primes*).

Erinnerung:

- $\text{Sign}(sk, M) \to \sigma := (a, b)$
  $a = g^e$ für zuf. $e \leftarrow \mathbb{Z}_{|\mathbb{G}|}$
  berechne $b \in \mathbb{Z}_q$, sodass $a \cdot x + e \cdot b = H(M) \bmod |\mathbb{G}|$

Sicherheit – Übungsblatt 5 – Aufgabe 1 (2 (a))

(a) Berechnen Sie

- einen DSA-Public-Key $pk := (\mathbb{G}, g, g^x, (\mathrm{H}, h_1, h_2))$, sowie
- den DSA-Secret-Key $sk := (\mathbb{G}, g, x, (\mathrm{H}, h_1, h_2))$

Wir verwenden die folgende Hashfunktion:

$$\begin{aligned} \mathrm{H}: \quad & \mathbb{Z}_q \times \mathbb{Z}_q \to \mathbb{Z}_q^\times \\ & (x_1, x_2) \mapsto h_1^{x_1} h_2^{x_2} \bmod q \end{aligned}$$

Sicherheit – Übungsblatt 5 – Aufgabe 1 (2 (a))

Für $p = 2q + 1 = 23$ ergibt sich:

$$\mathbb{G} := Q(\mathbb{Z}_{23}^{\times}) = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}.$$
$$|\mathbb{G}| = 11.$$

- Ziehe $x \leftarrow \{0, \ldots, q-1\}$, z.B. $x := 10$.

Vorgegeben waren:

- $g := 8$
- $h_1 := 4$
- $h_2 := 2$

Fehlt noch: g^x

Sicherheit – Übungsblatt 5 – Aufgabe 1 (2 (a))

Wir berechnen

$$
\begin{aligned}
g^x &= 8^{10} \bmod 23 \\
&= (8^2)^4 \cdot 8^2 \bmod 23 \\
&= (64)^4 \cdot 64 \bmod 23 \\
&= (18)^4 \cdot 18 \bmod 23 \\
&= (-5)^4 \cdot 18 \bmod 23 \\
&= (2)^2 \cdot 18 \bmod 23 \\
&= 4 \cdot (-5) \bmod 23 \\
&= -20 \bmod 23 \\
&= 3 \bmod 23
\end{aligned}
$$

Sicherheit – Übungsblatt 5 – Aufgabe 1 (2 (a))

Damit ergibt sich insgesamt:

$$pk = (Q(\mathbb{Z}_{23}^{\times}), 8, 3, (\mathrm{H}, 4, 2))$$
$$sk = (Q(\mathbb{Z}_{23}^{\times}), 8, 10, (\mathrm{H}, 4, 2))$$

Sicherheit – Übungsblatt 5 – Aufgabe 1 (2 (b))

Signieren Sie die Nachricht $M = (7, 3)$ mithilfe des Secret-Keys aus (a).

- Wähle $e \leftarrow \{0, \ldots, q-1\}$, z.B. $e := 5$.
- Berechne

$$
\begin{aligned}
a &:= g^e \bmod p \\
&= 8^5 \bmod 23 \\
&= 8^4 \cdot 8 \bmod 23 \\
&= (64)^2 \cdot 8 \bmod 23 \\
&= (-5)^2 \cdot 8 \bmod 23 \\
&= 2 \cdot 8 \bmod 23 \\
&= 16 \bmod 23
\end{aligned}
$$

Sicherheit – Übungsblatt 5 – Aufgabe 1 (2 (b))

Als Hashwert ergibt sich:

$$\begin{aligned} \mathrm{H}(M) &= \mathrm{H}(7,3) \\ &= h_1^7 h_2^3 \bmod 11 \\ &= 4^7 2^3 \bmod 11 \\ &= \ldots \\ &= 7 \bmod 11. \end{aligned}$$

Löse Gleichung nach b:

$$\begin{aligned} ax + eb &= \mathrm{H}(M) \bmod q \\ 16 \cdot 10 + 5 \cdot b &= 7 \bmod 11 \\ -5 + 5 \cdot b &= 7 \bmod 11 \\ 5 \cdot b &= 1 \bmod 11 \\ b &= 5^{-1} = 9 \bmod 11 \end{aligned}$$

Sicherheit – Übungsblatt 5 – Aufgabe 1 (2 (b))

Die Signatur zur Nachricht $M = (7, 3)$ lautet

$$\sigma := (a, b) = (16, 9).$$

Sicherheit – Übungsblatt 5 – Aufgabe 1 (2 (c))

Verifizieren Sie die Signatur zur Nachricht M aus (b) mittels des Public-Keys aus (a).

Erinnerung:

- $\mathrm{Ver}(pk, M, \sigma)$:
  prüfe, ob

$$(g^x)^a \cdot a^b = g^{H(M)}$$

  gilt.

Sicherheit – Übungsblatt 5 – Aufgabe 1 (2 (c))

Die Signatur ist $\sigma = (16, 9) =: (a, b)$. Überprüfe, ob

$$(g^x)^a \cdot a^b \bmod p = g^{\mathrm{H}(M)} \bmod p.$$

Es ergibt sich

$$\begin{aligned}(g^x)^a \cdot a^b &= 3^{16} \cdot 16^9 \bmod 23 \\ &= 12 \bmod 23,\end{aligned}$$

sowie:

$$\begin{aligned}g^{\mathrm{H}(M)} &= 8^7 \bmod 23 \\ &= 12 \bmod 23.\end{aligned}$$

$\Rightarrow$ Signatur gültig.

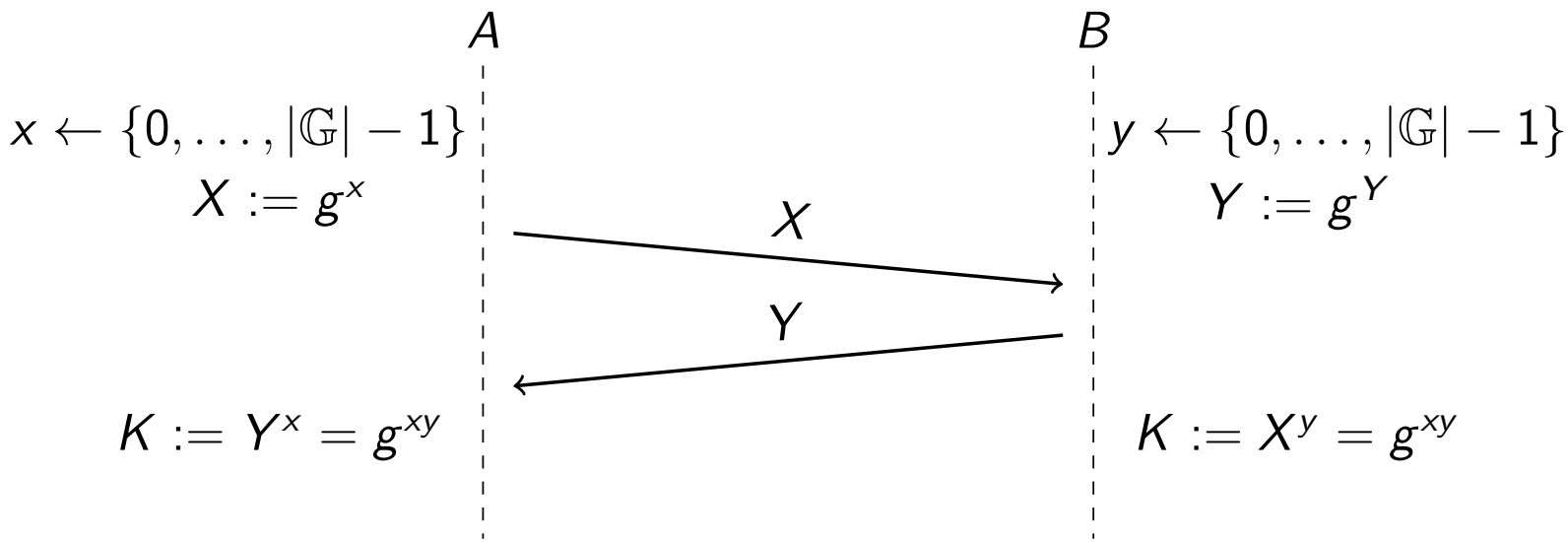
Sicherheit – Übungsblatt 5 – Aufgabe 1 (2)

Fazit:

- DSA Teil des Digital-Signature-Standards, gilt z.B. für US-Behörden.
- Als mögliche Hashfkts. werden dort Algorithmen der SHA-Familie empfohlen.

Sicherheit – Übungsblatt 5 – Aufgabe 2

Betrachten Sie den Diffie-Hellman-Schlüsselaustausch in $\mathbb{G}$:



Sicherheit – Übungsblatt 5 – Aufgabe 2

Es seien

- $\mathbb{G} = Q(\mathbb{Z}_p^\times)$ (also Untergruppe von $\mathbb{Z}_p^\times$),
- $p = 23$,
- $g = 18$,
- $x = 6$,
- $y = 8$.

Zusatzinfo: $|\mathbb{G}| = 11$

Berechnen Sie X, Y, K.

Sicherheit – Übungsblatt 5 – Aufgabe 2

$$
\begin{aligned}
X &= g^x \bmod 23 \\
&= 18^6 \bmod 23 \\
&= ((-5)^2)^3 \bmod 23 \\
&= 25^3 \bmod 23 \\
&= 2^3 \bmod 23 \\
&= 8 \bmod 23
\end{aligned}
$$

Sicherheit – Übungsblatt 5 – Aufgabe 2

$$
\begin{aligned}
Y &= g^y \bmod 23 \\
&= 18^8 \bmod 23 \\
&= ((-5)^2)^4 \bmod 23 \\
&= 2^4 \bmod 23 \\
&= 16 \bmod 23
\end{aligned}
$$

Sicherheit – Übungsblatt 5 – Aufgabe 2

$$
\begin{aligned}
K &= g^{xy} \bmod 23 \\
&= 18^{48} \bmod 23 \\
&= 18^{48 \bmod 11} \bmod 23 \\
&= (-5)^4 \bmod 23 \\
&= 2^2 \bmod 23 \\
&= 4 \bmod 23
\end{aligned}
$$

- Wir verwenden, dass $18 \in \mathbb{G}$ und $|\mathbb{G}| = 11$
- Wir könnten auch mit der Ordnung der Obergruppe ($\mathbb{Z}_{23}^{\times}$, Ordnung 22) arbeiten.

Alice und Bob würden K natürlich als $X^y \bmod 23$ bzw. als $Y^x \bmod 23$ berechnen.

Sicherheit – Übungsblatt 5 – Aufgabe 3

Geg.: 2-Parteien-2-Nachrichten-Schlüsselaustauschverf. KE:

KE.Gen(1^k): Gibt State s und X aus (X ist erste Nachricht im Schlüsselaustausch).

KE.Encap(X): Gibt Y und K aus (Y ist zweite Nachricht im Austausch).

KE.Decap(s, Y): Gibt einen Schlüssel K' aus.

Korrektheit: $\forall k \in \mathbb{N}$, $\forall (s, X) \leftarrow \text{KE.Gen}(1^k)$ gilt für

- $(K, Y) \leftarrow \text{KE.Encap}(X)$, dass
- $\text{KE.Decap}(s, Y) = K$.

Sicherheit – Übungsblatt 5 – Aufgabe 3

Diffie-Hellman so geschrieben:

KE.Gen(1^k): $s := x \leftarrow \mathbb{Z}_p$, $X := g^x$

KE.Encap(X): Zieht $y \leftarrow \mathbb{Z}_p$

- $K = X^y = g^{xy}$
- $Y = g^y$

KE.Decap(s, Y): Berechnet $K' := Y^s = Y^x = g^{xy}$.

Sicherheit – Übungsblatt 5 – Aufgabe 3

Aufgabe: Konstruieren Sie

- ein Public-Key-Verschlüsselungsverfahren $\mathsf{PKE} = (\mathsf{PKE.Gen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ aus dem Schlüsselaustauschverfahren KE.

Hinweis: Denken Sie an die Beziehung zwischen DH-Schlüsselaustausch und ElGamal-Verschlüsselungsverfahren

Sicherheit – Übungsblatt 5 – Aufgabe 3

Schlüsselerzeugung PKE.Gen(1^k) :

- Ziehe $(s, X) \leftarrow$ KE.Gen(1^k)
- Setze $pk := X$
- Setze $sk := s$
- gib (pk, sk) aus

Diffie-Hellman/ElGamal:

- DH: $s = x$, $X = g^x$
- ElGamal: $sk = x$, $pk = g^x$

Sicherheit – Übungsblatt 5 – Aufgabe 3

Verschlüsselung PKE.Enc(pk, M) :

- Berechne $(Y, K) \leftarrow$ KE.Encap(pk).
- $C := (Y, K \oplus M)$.
- gib C aus.

Diffie-Hellman/ElGamal:

- DH: ziehe y, $Y := g^y$, $K = g^{xy}$
- ElGamal: ziehe y, $C := (g^y, g^{xy} \cdot M)$

Sicherheit – Übungsblatt 5 – Aufgabe 3

Entschlüsselung PKE.Dec$(sk, C = (C_1, C_2))$:

- $C_1 = Y$, $C_2 = K \oplus M$, $sk = s$
- $K' :=$ KE.Decap$(sk, C_1) =$ KE.Decap(s, Y)
- $M := C_2 \oplus K'$

- Korrektheit folgt aus Korrektheit von KE $(K = K')$

Diffie-Hellman/ElGamal:

- DH: erhalte Y, $K' = Y^x = g^{xy}$
- ElGamal: $M = C_2 / C_1^x = (g^{xy} \cdot M)/g^{xy}$

Sicherheit – Übungsblatt 5 – Aufgabe 3

Fazit:

- Zusammenhang zwischen Schlüsselaustausch und Verschlüsselung
- Sicherheit noch unklar
  - Sicherheitsdef. für Schlüsselaustausch wurde in VL aber auch nicht besprochen!

Socrative: CRIME

`https://b.socrative.com/login/student/`

Room: `SICHERHEIT`

- App um Quiz durchzuführen
- Zugang durch Browser oder App
- Als Quizteilnehmer kein Account notwendig.

Sicherheit – Übungsblatt 5 – Aufgabe 4

Doktor Meta Aufgabe (Story siehe Blatt)

- Theoretische und praktische Untersuchung von CRIME
- Angriff auf TLS
- Nutzt aus, dass Klartexte vor der Verschlüsselung komprimiert werden

Sicherheit – Übungsblatt 5 – Aufgabe 4

- PKE $= (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ IND-CPA-sicher.
- Zu PKE ist PPT $\mathcal{L}$ bekannt, sodass für alle M

  $$\Pr\left[\mathcal{L}(pk, C) = |M| \;\middle|\; (pk, sk) \leftarrow \mathsf{Gen}(1^k), C \leftarrow \mathsf{Enc}(pk, M)\right]$$

  gleich 1.
- D.h. $\mathcal{L}$ kann die Länge des Klartextes in einem Chiffrat bestimmen.
- $\mathcal{C} = (\mathsf{Comp}, \mathsf{Decomp})$ Kompressionsalgorithmus
  - $|M| = |M'|$ bedeutet nicht $|\mathsf{Comp}(M)| = |\mathsf{Comp}(M')|$!
  - Redundante Nachrichten werden stärker komprimiert.

Sicherheit – Übungsblatt 5 – Aufgabe 4

Es sei nun $\mathrm{PKE}' = (\mathrm{Gen}', \mathrm{Enc}', \mathrm{Dec}')$ gegeben durch:

- $\mathrm{Gen}'(1^k) = \mathrm{Gen}(1^k)$
- $\mathrm{Enc}'(pk, M) = \mathrm{Enc}(pk, \mathrm{Comp}(M))$
- $\mathrm{Dec}'(sk, C) = \mathrm{Decomp}(\mathrm{Dec}(sk, C))$

Zeigen Sie: PKE' ist nicht IND-CPA-sicher.

Sicherheit – Übungsblatt 5 – Aufgabe 4

Betrachte folgenden PPT $\mathcal{A}$:

- $\mathcal{A}$ erhält pk und wählt M_0, M_1 mit
  - $|M_0| = |M_1|$, aber
  - $|\text{Comp}(M_0)| \neq |\text{Comp}(M_1)|$.
- $\mathcal{A}$ schickt M_0, M_1 als Challenge.
- $\mathcal{A}$ erhält C^* und führt $\mathcal{L}(pk, C^*) =: x$ aus.
- Er überprüft, ob $x = |\text{Comp}(M_0)|$, wenn ja, gib 0 aus, sonst...
- ... überprüfe, ob $x = |\text{Comp}(M_1)|$, wenn ja, gib 1 aus, sonst...
- gib ein zufälliges Bit aus.

Sicherheit – Übungsblatt 5 – Aufgabe 4

Sei $\mathcal{E}$ das Ereignis, dass $\mathcal{L}$ die Länge des Klartextes in C^* richtig bestimmt. Dann ist:

$$\begin{aligned}
\Pr[\mathcal{A} \text{ gew.}] &= \Pr[(\mathcal{A} \text{ gew.} \wedge \mathcal{E}) \vee (\mathcal{A} \text{ gew.} \wedge \overline{\mathcal{E}})] \\
&= \Pr[\mathcal{E}] \Pr[\mathcal{A} \text{ gew.} \mid \mathcal{E}] + \Pr[\overline{\mathcal{E}}] \Pr[\mathcal{A} \text{ gew.} \mid \overline{\mathcal{E}}] \\
&= 1 \cdot \Pr[\mathcal{A} \text{ gew.} \mid \mathcal{E}] + 0 \\
&= 1.
\end{aligned}$$

$1 - \frac{1}{2} = \frac{1}{2}$ ist nicht vernachlässigbar, d.h. PKE′ ist nicht IND-CPA-sicher.

Sicherheit – Übungsblatt 5 – Aufgabe 4

Sei nun

$$\Pr[\mathcal{L}(pk, C) = |M| \; |...] = 1 - f(k)$$

mit f vernachlässigbar in k.

$$\begin{aligned}
\Pr[\mathcal{A} \text{ gew.}] &= \Pr[\mathcal{E}] \Pr[\mathcal{A} \text{ gew.} \mid \mathcal{E}] + \Pr[\overline{\mathcal{E}}] \Pr[\mathcal{A} \text{ gew.} \mid \overline{\mathcal{E}}] \\
&\geq \Pr[\mathcal{E}] \cdot \Pr[\mathcal{A} \text{ gew.} \mid \mathcal{E}] \\
&= (1 - f(k)) \cdot 1 \\
&= 1 - f(k)
\end{aligned}$$

Der Vorteil von $\mathcal{A}$ gegenüber Raten ist also mindestens

$$g(k) := 1 - f(k) - \frac{1}{2} = \frac{1}{2} - f(k).$$

Sicherheit – Übungsblatt 5 – Aufgabe 4

Frage: Ist $g(k) := frac12 - f(k)$ nicht vernachlässigbar?
Antwort: Ja!

- Für $k \to \infty$ gehen vernachlässigbare Funktionen gegen 0.
- Aber:

$$\lim_{k\to\infty} g(k) = \lim_{k\to\infty} 1/2 - f(k) = 1/2 \neq 0$$

- Also kann $g(k)$ nicht vernachlässigbar sein.

Achtung:

- Um zu zeigen, dass eine Funktion f vernachlässigbar ist, genügt es nicht zu zeigen, dass sie gegen Null geht!

Sicherheit – Übungsblatt 5 – CRIME

- Szenario: Client hat geheimes HTTP-Cookie, das Browser automatisch an alle Nachrichten an Server anhängt. (Diese Nachrichten sind verschlüsselt.)
- Ziel: Session-Cookie herausfinden.
- Angreifer bringt Browser des Client dazu Nachrichten der Form 'Cookie: ...' an Server zu senden, die er dann abfängt.
  - Eine vom Client an den Server gesendete Nachricht sieht dann so aus (vereinfacht)
    POST / HTTP/1.1\r\n
    Host: host.edu\r\n
    Cookie: cookie_data\r\n
    Cookie: ...

Sicherheit – Übungsblatt 5 – CRIME

- Der Angreifer fängt die Chiffrate ab und kann daraus erkennen, welche Länge die (komprimierte) gesendete Nachricht hat.
- Ist die Länge 'besonders klein', gehen wir davon aus, dass unser gewählter String 'Cookie: ...' zu viel Redundanz geführt hat.

$\Rightarrow$ Auf diese Weise können wir den Cookie Zeichen für Zeichen herausfinden.

Sicherheit – Übungsblatt 5 – Aufgabe 4

Fazit:

- Problem: Chiffrate können Nachrichtenlänge nicht verstecken.
  - Für Angriff/Problem muss nicht unbedingt die exakte Nachrichtenlänge ablesbar sein
  - Es genügt, wenn verschieden lange Nachrichten zu verschieden langen Chiffraten führen.
- Komprimierung & Verschlüsselung verträgt sich nicht
  - Klartext komprimieren $\rightarrow$ Angriff
  - Chiffrat komprimieren führt zu schlechter Kompression, da wenig Redundanz