Übung zur Vorlesung „Sicherheit“
14.07.2014 – Übungsblatt 6

Jessica Koch
jessica.koch@kit.edu

Sicherheit – Übungsblatt 5 – Aufgabe 3

Aufgabe 3 (Zusatz zu letztem Übungsblatt).

- $\text{KE.Gen}(1^k) \to (s, X)$, $pk = X, sk = s$
- 1. Ausführung: $\text{KE.Encap}(X) \to (Y, K)$

  2. Ausführung: $\text{KE.Encap}(X) \to (Y', K')$
- $\text{KE.Decap}(s, Y) = K$

  $\text{KE.Decap}(s, Y') = K'$

$\text{KE.Encap}(X)$ probabilistisch, Y entspricht Zufall, der mitübergeben werden muss.
BSP(DH$\to$ ElGamal): $pk = g^x$, $sk = x$, $Y = g^r$, $K = g^{xr} = (g^x)^r = (g^r)^x = pk^r = Y^{sk}$

Sicherheit – Übungsblatt 6 – Aufgabe 1

Aufgabe 1. Public-Key-Identifikationsprotokoll $(\mathrm{Gen}, \mathrm{P}, \mathrm{V})$

1. $\mathrm{Gen}(1^k)$ wählt $q \in \mathbb{P}$, sodass $p := 2q + 1$ prim.
   $g \in \mathbb{Z}_p^*$, $q := \mathrm{ord}(g)$, ziehe $s \in \mathbb{Z}_q$, setze $h := g^s \bmod p$.
   $pk := (\mathbb{Z}_p^*, g, h)$, $sk := (\mathbb{Z}_p^*, g, s)$
2. $\mathrm{P}(sk) \to X := g^r \bmod p$, r zufällig
3. $\mathrm{V}(pk, X) \to b$, $b \in \{0, 1\}$ zufällig
4. $\mathrm{P}(sk, b) \to y$, $y := r + b \cdot s \bmod q$
5. $\mathrm{V}(pk, y) = \begin{cases} 1, & \text{falls } g^y = h^b X \bmod p \\ 0, & \text{sonst} \end{cases}$

P beweist V, dass er $\log_g h \bmod p$ kennt.

(a) Zeigen Sie die Korrektheit von $(\mathrm{Gen}, \mathrm{P}, \mathrm{V})$.

Sicherheit – Übungsblatt 6 – Aufgabe 1

Aufgabe 1. Public-Key-Identifikationsprotokoll $(\mathrm{Gen}, \mathrm{P}, \mathrm{V})$

1. $\mathrm{Gen}(1^k)$ wählt $q \in \mathbb{P}$, sodass $p := 2q + 1$ prim.
   $g \in \mathbb{Z}_p^*$, $q := \mathrm{ord}(g)$, ziehe $s \in \mathbb{Z}_q$, setze $h := g^s \bmod p$.
   $pk := (\mathbb{Z}_p^*, g, h)$, $sk := (\mathbb{Z}_p^*, g, s)$
2. $\mathrm{P}(sk) \to X := g^r \bmod p$, r zufällig
3. $\mathrm{V}(pk, X) \to b$, $b \in \{0, 1\}$ zufällig
4. $\mathrm{P}(sk, b) \to y$, $y := r + b \cdot s \bmod q$
5. $$\mathrm{V}(pk, y) = \begin{cases} 1, & \text{falls } g^y = h^b X \bmod p \\ 0, & \text{sonst} \end{cases}$$

(b) Wie könnte jemand, der sk nicht kennt V trotzdem überzeugen? Wie groß ist die Erfolgswahrscheinlichkeit?

Sicherheit – Übungsblatt 6 – Aufgabe 1

Aufgabe 1. Public-Key-Identifikationsprotokoll $(\mathrm{Gen}, \mathrm{P}, \mathrm{V})$

1. $\mathrm{Gen}(1^k)$ wählt $q \in \mathbb{P}$, sodass $p := 2q + 1$ prim.
   $g \in \mathbb{Z}_p^*$, $q := \mathrm{ord}(g)$, ziehe $s \in \mathbb{Z}_q$, setze $h := g^s \bmod p$.
   $pk := (\mathbb{Z}_p^*, g, h)$, $sk := (\mathbb{Z}_p^*, g, s)$
2. $\mathrm{P}(sk) \to X := g^r \bmod p$, r zufällig
3. $\mathrm{V}(pk, X) \to b$, $b \in \{0, 1\}$ zufällig
4. $\mathrm{P}(sk, b) \to y$, $y := r + b \cdot s \bmod q$
5. $\mathrm{V}(pk, y) = \begin{cases} 1, & \text{falls } g^y = h^b X \bmod p \\ 0, & \text{sonst} \end{cases}$

(c) Geben Sie einen Simulator $\mathcal{S}$ in der Rolle von P an.

Sicherheit – Übungsblatt 6 – Aufgabe 2

Aufgabe 2. Betrachte Jacobi-Symbol für $a \in \mathbb{N}, p \in \mathbb{P}$:

$$\left(\frac{a}{p}\right) := a^{\frac{p-1}{2}} \bmod p = \begin{cases} 1 & \text{wenn } a \text{ quadratischer Rest} \\ -1 & \text{wenn } a \text{ quadratischer Nichtrest} \\ 0 & \text{wenn } a \text{ ein Vielfaches von } p \end{cases}$$

* $\left(\frac{a}{n}\right) = \left(\frac{a \bmod n}{n}\right), \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$
* $\left(\frac{a_1 a_2}{n}\right) = \left(\frac{a_1}{n}\right)\left(\frac{a_2}{n}\right), \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$

(a) Berechnen Sie die Jacobi-Symbole von $\left(\frac{15}{35}\right)$, $\left(\frac{32}{33}\right)$, $\left(\frac{17}{143}\right)$

(b) Zeigen Sie, dass -1 für $n = pq$ wobei $p \equiv q \equiv 3 \bmod 4$ gilt, kein quadratischer Rest mod n ist, jedoch das Jacobi-Symbol 1 ergibt. (n ist Blum-Integer.)

Sicherheit – Übungsblatt 6 – Aufgabe 2

Aufgabe 2. RSA-Modulus $n = pq$ Blum-Integer. P wählt geheime $s \xleftarrow{\$} \mathbb{Z}_n$, $t_1 \xleftarrow{\$} \{-1, 1\}$, veröffentlicht $v = t_1 \cdot s^2 \bmod n$.

Identifikationsprotokoll:

1. P wählt $r \xleftarrow{\$} \mathbb{Z}_n$, $t_2 \xleftarrow{\$} \{-1, 1\}$, berechnet $x = t_2 \cdot r^2 \bmod n$, sendet x an V.
2. V wählt $b \xleftarrow{\$} \{0, 1\}$, sendet b an P.
3. P berechnet $y = r \cdot s^b \bmod n$, sendet y an V.
4. V überprüft, ob $y^2 = \pm x \cdot v^b \bmod n$ gilt.

(i) Zeigen Sie die Korrektheit des Protokolls für ehrlichen P und V.

(ii) Geben Sie die Erfolgswahrscheinlichkeit für einen unehrlichen P an, falls das Protokoll k mal durchgeführt wird.

Sicherheit – Übungsblatt 6 – Aufgabe 2

Aufgabe 2. RSA-Modulus $n = pq$ Blum-Integer. P wählt geheime $s \xleftarrow{\$} \mathbb{Z}_n$, $t_1 \xleftarrow{\$} \{-1, 1\}$, veröffentlicht $v = t_1 \cdot s^2 \bmod n$.

Identifikationsprotokoll:

1. P wählt $r \xleftarrow{\$} \mathbb{Z}_n$, $t_2 \xleftarrow{\$} \{-1, 1\}$, berechnet $x = t_2 \cdot r^2 \bmod n$, sendet x an V.
2. V wählt $b \xleftarrow{\$} \{0, 1\}$, sendet b an P.
3. P berechnet $y = r \cdot s^b \bmod n$, sendet y an V.
4. V überprüft, ob $y^2 = \pm\, x \cdot v^b \bmod n$ gilt.

(iii) Zeigen Sie durch Angabe eines Simulators, dass die Zero-Knowledge-Eigenschaft gilt.

(iv) Welche Information würde V über v lernen, falls wir das Protokoll ohne die zufälligen Vorzeichen t_1, t_2 durchführen würden?

Sicherheit – Übungsblatt 6 – Aufgabe 3

Aufgabe 3. Gegeben sei das folgende System im Bell-LaPadula-Modell:

- Subjektmenge $\mathcal{S} = \{\text{Alice}, \text{Bob}, \text{Carol}\}$
- Objektmenge $\mathcal{O} = \{D_1, D_2, D_3, D_4\}$
- Menge der Zugriffsoperationen
  $\mathcal{A} = \{\texttt{read}, \texttt{write}, \texttt{append}, \texttt{execute}\}$
- Zugriffskontrollmatrix M gegeben durch

	D_1	D_2	D_3	D_4
Alice	r,w,a	r	r,w,a	r,x
Bob	r,w,a	r,w,a	r,w,a	r,x
Carol	r	r	r,w,a	r,w,a,x

Sicherheit – Übungsblatt 6 – Aufgabe 3

Aufgabe 3.
Zuordnung der Sicherheitsstufen $F = (f_S, f_C, f_O)$ gegeben durch

	f_S	f_C
Alice	*Verwaltung*	*Verwaltung*
Bob	*Forschung*	*Lehre*
Carol	*Präsidium*	*Forschung*

	f_O
D_1	*Verwaltung*
D_2	*Lehre*
D_3	*Forschung*
D_4	*Präsidium*

Lehre $<$ Verwaltung $<$ Präsidium und Lehre $<$ Forschung $<$ Präsidium

Sicherheit – Übungsblatt 6 – Aufgabe 3

Aufgabe 3.

	Anforderung	Zugriff erteilt/verweigert
1.	$(Alice, D_1, \mathtt{a})$	
2.	$(Bob, D_2, \mathtt{w})$	
3.	$(set(f_C(Bob) = Forschung))$	alte Vorlesung/Übung
4.	$(Bob, D_3, \mathtt{r})$	
5.	$(Carol, D_3, \mathtt{r})$	
6.	$(set(f_C(Carol) = Praesidium))$	alte Vorlesung/Übung
7.	$(Carol, D_2, \mathtt{w})$	
8.	$(Alice, D_2, \mathtt{r})$	
9.	$(Bob, D_4, \mathtt{r})$	
10.	$(set(f_C(Alice) = Lehre))$	alte Vorlesung/Übung
11.	$(Bob, D_2, \mathtt{a})$	zusätzlich

Organisatorisches

- **Hinweis:** Keine alten Klausuren oder Übungsblätter zu Bell-laPadula oder Chinese-Wall Aufgaben. Nur Klausuren und Übungen ab 2013!!
- Hauptklausur, 22.07.14
- An- und Abmeldung zur Hauptklausur bis **heute** Mo, 14.07.14
- Raumverteilung online spätestens Ende der Woche