Karlsruhe Institute of Technology

Institut für Theoretische Informatik
Jun.-Prof. Dr. D. Hofheinz

Stammvorlesung Sicherheit im Sommersemester 2014

Nachklausur

29.09.2014

Vorname: _____

Nachname: _____

Matrikelnummer: _____

Hinweise

- Für die Bearbeitung stehen Ihnen 60 Minuten zur Verfügung.
- Zum Bestehen der Klausur sind 20 der 60 möglichen Punkte hinreichend.
- Es sind keine Hilfsmittel zugelassen.
- Schreiben Sie Ihre Lösungen auf die Aufgabenblätter sowie auf deren Rückseiten.
- Zusätzliches Papier erhalten Sie bei Bedarf von der Aufsicht.

Aufgabe	mögliche Punkte					erreichte Punkte				
	a	b	c	d	Σ	a	b	c	d	Σ
1	2	4	3	1	10					
2	4	4	-	-	8			-	-	
3	3	3	-	-	6			-	-	
4	2	2	6	-	10				-	
5	6	3	-	-	9			-	-	
6	1	6	-	-	7			-	-	
7	10x1				10					
Σ					60					

Aufgabe 1. (2+4+3+1 Punkte) Betrachten Sie das ElGamal-Verschlüsselungsverfahren aus der Vorlesung. Es sei eine zyklische (Unter-)Gruppe $\mathbb{G} \subset \mathbb{Z}_{11}^*$ mit $\mathbb{G}$-Erzeuger $g = 3$ der Ordnung 5 gegeben.

(a) Berechnen Sie zu dem geheimen Schlüssel $sk = (\mathbb{G}, g = 3, x = 7)$ den öffentlichen Schlüssel pk.

(b) (i) Geben Sie an, wie ein Chiffrat C zu einer Nachricht $M \in \mathbb{G}$ berechnet wird.

(ii) Sei $C = (5, 3)$ ein Chiffrat. Verwenden Sie den geheimen Schlüssel aus (a), um den Klartext $M \in \mathbb{G}$ zu berechnen.

(c) Ein Angreifer sieht bei einer Auktion, bei der voriges ElGamal-Verschlüsselungsverfahren mit den Schlüsseln aus (a) verwendet wird, das Chiffrat $C = (9, 1)$ von einem Bieter B und möchte das gleiche Gebot M wie B abgeben. Damit dies nicht auffällt soll für sein Chiffrat $C^* \neq C$ gelten. Geben Sie einen erfolgreichen Angriff und ein neues Chiffrat C^* an.

(d) Nennen Sie einen sicherheitsrelevanten Unterschied zwischen dem ElGamal-Verschlüsselungsverfahren und dem Lehrbuch-RSA-Verfahren aus der Vorlesung.

Lösungsvorschlag zu Aufgabe 1.

(a) $pk := (\mathbb{G}, g, h) = (\mathbb{G}, 3, 9)$ da:

$$\begin{aligned} g^x &:= 3^7 \bmod 11 = 3^4 \cdot 3^3 \bmod 11 = 81 \cdot 27 \bmod 11 = 4 \cdot 5 \bmod 11 \\ &= 20 \bmod 11 = 9 \bmod 11 \end{aligned}$$

(kürzer: $3^7 \bmod 11 = 3^{7 \bmod 5} \bmod 11 = 3^2 \bmod 11 = 9 \bmod 11$)

(b) (i) Es wird ein zufälliges $y \in \mathbb{Z}_{11}$ gezogen und $C = \mathsf{Enc}(pk, M) = (g^y, g^{xy} \cdot M) = (3^y, 9^y \cdot M)$ berechnet.

(ii) Für $C =: (Y, Z)$ berechnen wir

$$\begin{aligned} M &:= Z/Y^x \bmod 11 \\ &= 3 \cdot (5^{-7 \bmod 10}) \bmod 11 = 3 \cdot 5^3 \bmod 11 = \ 3 \cdot 5 \cdot 25 \bmod 11 \\ &= 15 \cdot 25 \bmod 11 = 4 \cdot 3 \bmod 11 = 12 \bmod 11 = 1 \bmod 11 \end{aligned}$$

(c) Der Angriff nutzt die Homomorphie des Verfahrens:

- Der Angreifer wählt ein zufälliges $y \in \mathbb{Z}_{11}$, z.B. $y = 1$
- Er berechnet das Chiffrat C' von 1: $C' = (g^y, g^{xy} \cdot 1) = (3, 9 \cdot 1) = (3, 9)$
- Nun multipliziert er die beiden Chiffrate C, C' und erhält somit dank der Homomorphie des Verfahrens ein Chiffrat $C^* = C \cdot C' = (5, 9)$ von $1 \cdot M$.

(d) Unterschied Sicherheit: ElGamal unter naheliegender Annahme semantisch sicher (IND-CPA-sicher)

Aufgabe 2. (4+4 Punkte) Wir betrachten das einfache RSA-Signaturschema (ohne Paddingfunktion) aus der Vorlesung.

(a) Geben Sie einen effizienten Angriff an, falls ein Angreifer zu einem vom Challenger vorgegebenen m^* eine gültige Signatur σ^* erstellen soll. Ein Angreifer darf sich dabei vom Challenger beliebige Nachrichten $m \neq m^*$ signieren lassen.

(b) Gegeben seien die Primzahlen $P = 3$ und $Q = 5$. Berechnen Sie den RSA-Modulus N und $\varphi(N)$ sowie einen möglichen nichttrivialen öffentlichen Schlüssel pk mit zugehörigem geheimen Schlüssel sk.

Lösungsvorschlag zu Aufgabe 2.

(a) Ein Angreifer erhält als Eingabe vom Challenger eine Nachricht m^*. Sein Ziel ist die Berechnung einer Signatur σ^* mit $(\sigma^*)^e \equiv m^* \bmod N$.

- Der Angreifer wählt zufälliges $x \leftarrow \mathbb{Z}_N$, wobei $x \in \mathbb{Z}_N^* \setminus \{1\}$ mit großer Wahrscheinlichkeit und berechnet $y \equiv x^e \bmod N$.
- Angreifer berechnet $m_1 := m^* \cdot y \bmod N$, und lässt m_1 vom Challenger signieren. (Weil $x \neq 1 \bmod N$ gewählt wurde, ist auch $y \neq 1 \bmod N$. Daher ist $m_1 \neq m^*$.) Er erhält σ_1 mit $\sigma_1^e \equiv m_1 \bmod N$.
- Angreifer berechnet $\sigma^* \equiv \sigma_1 \cdot x^{-1} \bmod N$, und gibt σ^* aus. Dies ist möglich, da $x \in \mathbb{Z}_N^*$ invertierbar ist. Ausserdem ist dies eine gültige Signatur für m^*, denn

$$(\sigma^*)^e \equiv (\sigma_1 \cdot x^{-1})^e \equiv \sigma_1^e \cdot (x^e)^{-1} \equiv m_1 \cdot y^{-1} \equiv m^* \cdot y \cdot y^{-1} \equiv m^* \bmod N.$$

Die Tatsache, dass Lehrbuch-RSA Signaturen multiplikativ homomorph sind, erlaubt also diesen Angriff.

(b) $N = P \cdot Q = 3 \cdot 5 = 15$

$\varphi(N) = (P-1)(Q-1) = 2 \cdot 4 = 8$

$pk = (N, e)$, wobei $e \in \{3, \ldots, \varphi(N)\}$ zufällig und gleichverteilt mit $\mathtt{ggt}(e, \varphi(N)) = 1$ gilt. Wähle z.B $e = 7$. Somit ist $pk = (15, 7)$.

$sk = (N, d)$, wobei $d = e^{-1} \bmod \varphi(N)$. Zu $e = 7$ ist $d = 7$ das Inverse modulo $\varphi(N)$, da $7 \cdot 7 = 49 = 1 \bmod 8$.

Aufgabe 3. (3+3 Punkte)

(a) Geben Sie zu einer Blockchiffre mit $E, D : \{0,1\}^k \times \{0,1\}^l \to \{0,1\}^l$ für jeden der drei Betriebsmodi ECB, CBC und CTR an, wie sich der Chiffratblock C_i und dessen Entschlüsselung M_i berechnet.

(b) Beschreiben Sie jeweils für den ECB- und CBC-Mode, wie sich ein gekipptes Bit im Block C_i bei der Entschlüsselung auf M_i und M_{i+1} auswirkt. (Ist bspw. nur ein einzelnes Bit betroffen oder der ganze Block?)

Lösungsvorschlag zu Aufgabe 3.

(a) Die Berechnungen von C_i und M_i sind in den einzelnen Betriebsmodi folgendermaßen:

ECB: $C_i := E(K, M_i)$, $M_i = D(K, C_i)$

CBC: $C_i := E(K, M_i \oplus C_{i-1})$, $M_i = D(K, C_i) \oplus C_{i-1}$, wobei $IV =: C_0$ zufälliger Initialisierungsvektor

CTR: $C_i := E(K, IV + i) \oplus M_i$, $M_i = C_i \oplus E(K, IV + i)$

(b) ECB: Bei der Entschlüsselung von C_i ist durch das gekippte Bit der ganze Block M_i zerstört. Es gibt keine Fehlerfortpflanzung, d.h. M_{i+1} wird wieder korrekt entschlüsselt, da dafür nur C_{i+1} und nicht C_i benötigt wird.

CBC: Bei der Entschlüsselung von C_i ist durch das gekippte Bit der ganze Block M_i zerstört. Fehlerfortpflanzung: Um M_{i+1} zu berechnen benötigen wir $D(K, C_{i+1}) \oplus C_i$, so dass durch ein gekipptes Bit in C_i nur das entsprechende Bit in M_{i+1} gekippt ist.

Aufgabe 4. (2+2+6 Punkte)

(a) Wann besitzt ein Public-Key-Identifikationsprotokoll $(\mathsf{Gen}, \mathrm{P}, \mathrm{V})$ gemäß der Definition aus der Vorlesung die Zero-Knowledge-Eigenschaft?

(b) Nennen und erklären Sie die zwei Eigenschaften, die ein Commitment-Verfahren Com besitzt.

(c) Füllen Sie beim folgenden, aus der Vorlesung bekannten, **noch nicht vollständigen** Graph-Dreifärbarkeits-ZK-Protokoll $(\mathsf{Gen}, \mathrm{P}, \mathrm{V})$ die Stellen mit den doppelten Fragezeichen (**??**) korrekt aus:

Gen erzeugt einen Graph $G = (V, E)$ mit Knotenmenge $K = \{1, \ldots, n\}$ und Kantenmenge $E \subset V^2$, sowie einer Dreifärbung $\phi : V \to \{1, 2, 3\}$.

$$pk = G, \quad sk = (G, \phi)$$

P kennt (pk, sk), V kennt nur pk.

Protokoll zwischen P und V:

1. P wählt Bijektion $\pi : \{1, 2, 3\} \to \{1, 2, 3\}$ der Farben
2. P berechnet die Commitments $com_i = Com(??; ??)$ für **??** und $i = 1 \ldots n$.
3. P sendet alle Commitments $com_1, \ldots, com_n$ an V
4. V wählt **??** und sendet dies an P
5. P öffnet **??** und sendet dies an V
6. V akzeptiert gdw. alle Openings gültig sind und **??**

Das Protokoll wird **??**.

Lösungsvorschlag zu Aufgabe 4.

(a) Ein Public-Key-Identifikationsprotokoll $(\mathsf{Gen}, \mathsf{P}, \mathsf{V})$ ist Zero-Knowledge (ZK), falls für jeden PPT-Algorithmus $\mathcal{A}$ (Angreifer) ein PPT-Algorithmus $\mathcal{S}$ (Simulator) existiert, sodass die folgenden Verteilungen ununterscheidbar sind (wobei $(pk, sk) \leftarrow \mathsf{Gen}(1^k)$): $\langle \mathsf{P}(sk), \mathcal{A}(1^k) \rangle$ und (Ausgabe von) $\mathcal{S}(1^k, pk)$.

(b) Hiding-Eigenschaft: Für beliebige $M, M' \in \{0,1\}^*$ sind die Verteilungen $Com(M; R)$ und $Com(M'; R)$ für zufälliges R ununterscheidbar.

Binding-Eigenschaft: Für jeden PPT-Angreifer $\mathcal{A}$ ist

$$\Pr[Com(M; R) = Com(M'; R') \text{ und } M \neq M']$$

vernachlässigbar in k, wobei die Wahrscheinlichkeit über $(M, R, M', R') \leftarrow \mathcal{A}(1^k)$ gemeint ist.

(c) Korrektes Protokoll:

1. P wählt Bijektion $\pi : \{1, 2, 3\} \to \{1, 2, 3\}$ der Farben
2. P berechnet die Commitments $com_i = Com(\pi(\phi(i)); R_i)$, für zufälliges R_i und $i = 1 \ldots n$.
3. P sendet alle Commitments $com_1, \ldots, com_n$ an V
4. V wählt zufällige Kante $(i, j) \in E$ und sendet dies an P
5. P öffnet com_i, com_j und sendet dies an V
6. V akzeptiert gdw. alle Openings gültig sind und $\pi(\phi(i)) \neq \pi(\phi(j))$

Das Protokoll wird k-mal wiederholt für $k \in \mathbb{N}$.

Aufgabe 5. (6+3 Punkte)

(a) Es sei $H : \{0,1\}^* \to \{0,1\}^k$ eine kollisionsresistente Hashfunktion. Sind die folgenden Konstruktionen ebenfalls kollisionsresistent? Falls **ja**, begründen Sie ihre Antwort, falls **nein**, geben Sie eine Kollision an.

(i) $H'(M) := H(|M|)$, wobei $|M|$ die Länge von M in Bits angibt.

(ii) $H'(M) := H(M) \oplus H(M \oplus X)$, für ein festes, bekanntes $X \in \{0,1\}^{|M|}$.

(iii) $H'(M) := H(f(M))$, für eine beliebige und effizient berechenbare injektive Funktion $f : \{0,1\}^* \to \{0,1\}^*$.

(b) Es sei eine Funktion $h : \{0,1\}^* \to \{0,1\}^n$ gegeben. Wir definieren induktiv für alle $i \in \mathbb{N}$:

$$h^1(x) := h(x) \quad \text{und} \quad h^i(x) := h^{i-1}(h(x)) \quad \text{für} \quad i > 1$$

Zeigen Sie: Falls h kollisionsresistent ist, ist auch h^i kollisionsresistent für alle $i \in \mathbb{N}$.

Lösungsvorschlag zu Aufgabe 5.

(a) (i) Nicht kollisionsresistent. Jedes Nachrichtenpaar M_0, M_1 mit $M_0 \neq M_1$ und $|M_0| = |M_1|$ führt zu einer Kollision. Solche M_0, M_1 können effizient gefunden werden.

(ii) Nicht kollisionsresistent. Für jede Nachricht M führt das Paar M, $M \oplus X$ zu einer Kollision: $H'(M) = H(M) \oplus H(M \oplus X) = H(M \oplus X) \oplus H(M) = H(M \oplus X) \oplus H(M \oplus X \oplus X) = H'(M \oplus X)$.

(iii) Kollisionsresistent. Sei $H'(M_0) = H'(M_1)$ (für $M_0 \neq M_1$) und damit $H(f(M_0)) = H(f(M_1))$. Da f injektiv ist, gilt $f(M_0) \neq f(M_1)$ und wir haben eine Kollision für H gefunden.

(b) Wenn h^i nicht kollisionsresistent ist, finden wir mit praktikablem Aufwand x_1 und x_2, sodass $h^i(x_1) = h^i(x_2)$ und $x_1 \neq x_2$. Sei j der größte Wert, für den noch $h^j(x_1) \neq h^j(x_2)$ gilt. Dieser Wert j lässt sich durch vollständige Suche in maximal i Schritten finden. Nach Konstruktion bilden $h^j(x_1)$ und $h^j(x_2)$ eine Kollsion für h, da $h^{j+1}(x_1) = h^{j+1}(x_2) \Leftrightarrow h(h^j(x_1)) = h(h^j(x_2))$ und somit kann h nicht kollisionsresistent sein.

Aufgabe 6. (1+6 Punkte) Im Bell-LaPadula-Modell aus der Vorlesung seien

- die Subjektmenge $\mathcal{S} = \{s_1, s_2, s_3, s_4\}$,
- die Objektmenge $\mathcal{O} = \{o_1, o_2, o_3\}$,
- die Menge der Zugriffsoperationen $\mathcal{A} = \{\texttt{read}, \texttt{write}, \texttt{append}, \texttt{execute}\}$ und
- die Menge der Sicherheitslevel $\mathcal{L} = \{\texttt{topsecret}, \texttt{secret}, \texttt{unclassified}\}$ mit der $\mathcal{L}$-Halbordnung $\texttt{topsecret} \geq \texttt{secret} \geq \texttt{unclassified}$

gegeben. Die Zugriffskontrollmatrix $M = (M_{s,o})_{s \in \mathcal{S}, o \in \mathcal{O}}$ ist durch die Tabelle

	o_1	o_2	o_3
s_1	{read, write}	{read, write, append}	$\emptyset$
s_2	{read, execute}	{read, write, execute}	{read}
s_3	{execute}	{read, write}	{append}
s_4	$\emptyset$	$\mathcal{A}$	{append}

definiert und die maximalen und aktuellen Sicherheitslevel $F = (f_s, f_c, f_o)$ sind durch die Tabellen

	$f_s(\cdot)$	$f_c(\cdot)$
s_1	secret	unclassified
s_2	topsecret	unclassified
s_3	secret	unclassified
s_4	unclassified	unclassified

	$f_o(\cdot)$
o_1	unclassified
o_2	secret
o_3	topsecret

beschrieben. Betrachten Sie die folgende Abfolge von Zugriffen $b \in \mathcal{S} \times \mathcal{O} \times \mathcal{A}$ in Reihenfolge:

1. $(s_2, o_2, \texttt{write})$
2. $(s_3, o_3, \texttt{read})$
3. $(s_2, o_3, \texttt{read})$
4. $(s_4, o_1, \texttt{read})$
5. $(s_2, o_2, \texttt{append})$
6. $(s_1, o_1, \texttt{write})$

(a) Wann ist ein Bell-LaPadula-Systemzustand sicher?

(b) Beschreiben Sie in der Spalte "Gültigkeit" in der unter stehenden Tabelle, ob die einzelnen Zugriffe gültig oder ungültig sind, und ob der aktuelle Sicherheitslevel nach gültigem Zugriff geändert wird. (Die Spalten "ds", "ss" und "$\star$" können Sie als Hilfsspalten benutzen.) Falls Sie ungültig gewählt haben, zeigen Sie auf, welche Eigenschaft(en) – im Sinne der ds-, ss- oder $\star$-Eigenschaft – verletzt wurde(n). Begründen Sie Ihre Entscheidung in der Spalte "Bemerkungen". Sie können davon ausgehen, dass noch kein Zugriff stattfand.

	Zugriff	ds	ss	$\star$	Gültigkeit	Bemerkungen
1.	$(s_2, o_2, \texttt{write})$					
2.	$(s_3, o_3, \texttt{read})$					
3.	$(s_2, o_3, \texttt{read})$					
4.	$(s_4, o_1, \texttt{read})$					
5.	$(s_2, o_2, \texttt{append})$					
6.	$(s_1, o_1, \texttt{write})$					

Lösungsvorschlag zu Aufgabe 6.

(a) Ein Bell-LaPadula-Systemzustand ist sicher, falls alle Zugriffe die ds-, ss- und $\star$-Eigenschaft erfüllen.

(b)

	Zugriff	ds	ss	$\star$	Gültigkeit	Bemerkungen
1.	$(s_2, o_2, \texttt{write})$	✓	✓	✓	gültig	(keine Änderung an $f_c(s_2)$)
2.	$(s_3, o_3, \texttt{read})$	×	×	✓	ungültig	$\texttt{read} \notin M_{s_3,o_3}$ und $f_o(o_3) > f_s(s_3)$
3.	$(s_2, o_3, \texttt{read})$	✓	✓	✓	gültig	$f_c(s_2) = \texttt{topsecret}$
4.	$(s_4, o_1, \texttt{read})$	×	✓	✓	ungültig	$\texttt{read} \notin M_{s_4,o_1}$
5.	$(s_2, o_2, \texttt{append})$	×	✓	×	ungültig	$\texttt{append} \notin M_{s_2,o_2}$ und $f_c(s_2) > f_o(o_2)$
6.	$(s_1, o_1, \texttt{write})$	✓	✓	✓	gültig	(keine Änderung an $f_c(s_1)$)

Aufgabe 7. (10 Punkte) Bei dieser Multiple-Choice-Aufgabe gibt jede richtige Antwort 1 Punkt; für jede falsche Antwort wird 1 Punkt abgezogen, die Gesamtpunktzahl der Aufgabe kann jedoch nicht negativ werden. Für nicht beantwortete Fragen (kein Kreuz) werden keine Punkte abgezogen.

	wahr	falsch
Laut Kerckhoffs' Prinzip muss ein Verschlüsselungsverfahren öffentlich sein.		
Die Blockchiffre AES verwendet eine Feistel-Struktur.		
Bei der differentiellen Kryptoanalyse werden Ausgabedifferenzen in Abhängigkeit von Eingabedifferenzen betrachtet.		
Für jede Hashfunktion $H : \{0,1\}^{2k} \to \{0,1\}^k$ existieren zwangsläufig Kollisionen.		
Für alle $N \in \mathbb{N}, M \in \mathbb{Z}_N$ gilt immer: $M^{N-1} = 1 \mod N$.		
Der DSA verwendet eine kollisionsresistente Hashfunktion H in seinem Signaturalgorithmus.		
Semantische Sicherheit impliziert IND-CPA-Sicherheit.		
Kerberos ist ein symmetrisches Verfahren, mit dem man Schlüssel austauschen kann.		
Das signaturbasierte PK-ID-Protokoll aus der Vorlesung besitzt die Zero-Knowledge-Eigenschaft.		
Das Bell-LaPadula-Modell sieht eine dynamische Anpassung der Zugriffskontrollmatrix vor.		

Lösungsvorschlag zu Aufgabe 7.

	wahr	falsch
Laut Kerckhoffs' Prinzip muss ein Verschlüsselungsverfahren öffentlich sein.[1]	×	×
Die Blockchiffre AES verwendet eine Feistel-Struktur.		×
Bei der differentiellen Kryptoanalyse werden Ausgabedifferenzen in Abhängigkeit von Eingabedifferenzen betrachtet.	×	
Für jede Hashfunktion $H : \{0,1\}^{2k} \to \{0,1\}^k$ existieren zwangsläufig Kollisionen.	×	
Für alle $N \in \mathbb{N}, M \in \mathbb{Z}_N$ gilt immer: $M^{N-1} = 1 \mod N$.		×
Der DSA verwendet eine kollisionsresistente Hashfunktion H in seinem Signaturalgorithmus.	×	
Semantische Sicherheit impliziert IND-CPA-Sicherheit.	×	
Kerberos ist ein symmetrisches Verfahren, mit dem man Schlüssel austauschen kann.	×	
Das signaturbasierte PK-ID-Protokoll aus der Vorlesung besitzt die Zero-Knowledge-Eigenschaft.		×
Das Bell-LaPadula-Modell sieht eine dynamische Anpassung der Zugriffskontrollmatrix vor.		×

[1] Die Aussage wurde in der Vorlesung und auf den Folien unterschiedlich formuliert