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.

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.

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?)

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 $V = \{1, \ldots, n\}$ und Kantenmenge $E \subset V^2$, sowie einer Dreifärbung $\phi : V \to \{1, 2, 3\}$.

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

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 **??**.

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 $i \in \mathbb{N}$:

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

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

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.	$(s_1, o_1, \texttt{write})$					

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.		