Karlsruher Institut für Technologie

Institut für Theoretische Informatik
Prof. Dr. D. Hofheinz

Stammvorlesung Sicherheit im Sommersemester 2017

Klausur

02.08.2017

Vorname: _____

Nachname: _____

Matrikelnummer: _____

Klausur-ID: _____

Hinweise

- Schreiben Sie auf **alle Blätter** der Klausur und Zusatzblätter Ihre Klausur-ID und Ihren Namen.
- Für die Bearbeitung stehen Ihnen 60 Minuten zur Verfügung.
- Es sind keine Hilfsmittel zugelassen.
- Schreiben Sie Ihre Lösungen auf die Aufgabenblätter sowie auf deren Rückseiten.
- Bitte kennzeichnen Sie deutlich, welche Lösung gewertet werden soll. Bei mehreren angegebenen Möglichkeiten wird jeweils die schlechteste Alternative gewertet.
- Zusätzliches Papier erhalten Sie bei Bedarf von der Aufsicht.
- Die Klausur umfasst 12 Seiten.

Aufgabe	mögliche Punkte					erreichte Punkte				
	a	b	c	d	Σ	a	b	c	d	Σ
1	8	1	5	-	14				-	
2	5	11	-	-	16			-	-	
3	3	2	2	2	9					
4	10	5	-	-	15			-	-	
5	6	-	-	-	6		-	-	-	
Σ					60					

Aufgabe 1. $(8(= 4 + 4) + 1 + 5$ Punkte)

Wir betrachten das RSA-Verschlüsselungsverfahren aus der Vorlesung (ohne Padding).

(a) Bei RSA muss modulo einer großen Zahl N potenziert werden. Dieser Vorgang kann beim Entschlüsseln beschleunigt werden, wenn die Faktoren von N bekannt sind. Seien $P = 19$ und $Q = 11$ und damit $N = P \cdot Q = 209$. Berechnen Sie $5^{42} \bmod N$ auf diese optimierte Weise.

(i) Berechnen Sie dazu $5^{42} \bmod P$ und $5^{42} \bmod Q$.

(ii) Berechnen Sie aus den Ergebnissen aus Aufgabenteil (a)(i) $5^{42} \bmod N$. Geben Sie dazu zunächst die allgemeine Formel an um aus $a_P :\equiv a \bmod P$ und $a_Q :\equiv a \bmod Q$ den Wert $a \bmod N$ zu berechnen.

Hinweis: Nutzen Sie den Chinesischen Restsatz. Es gilt $19^{-1} = 7 \bmod 11$ und $11^{-1} = 7 \bmod 19$.

(b) Seien $P \neq Q$ Primzahlen und sei $N := P \cdot Q$. Welche Bedingungen muss der öffentliche Schlüssel (N, e) beim RSA-Verschlüsselungsverfahren erfüllen?

(c) Sei $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ das RSA-Verschlüsselungsverfahren aus der Vorlesung (ohne Padding). Sei $pk = (N, e)$, $sk = (N, d)$ ein von $\mathsf{Gen}(1^k)$ erzeugtes Schlüsselpaar. Die Primfaktoren von N seien P und Q mit $P \neq Q$.

Geben Sie einen Beweis für die Korrektheit des RSA-Verschlüsselungsverfahrens an. Betrachten Sie dabei Nachrichten aus $\mathbb{Z}_N$ (also auch nicht-invertierbare Nachrichten). (Ein Beweis, der nur für den Nachrichtenraum $\mathbb{Z}_N^\times$ gültig ist, führt zu höchstens einem Punkt.)

Hinweis: Nutzen Sie den Chinesischen Restsatz (d.h. $\mathbb{Z}_N$ und $\mathbb{Z}_P \times \mathbb{Z}_Q$ sind als Ringe isomorph).

Aufgabe 2. $(5(= 3 + 2) + 11(= 2 + 6 + 3)$ Punkte)

(a) Für das ElGamal-Signaturverfahren aus der Vorlesung wurde eine hinreichend große Primzahl $p > 2$ erzeugt. Die Gruppe $\mathbb{G} := Q(\mathbb{Z}_p^\times) := \{x^2 \mid x \in \mathbb{Z}_p^\times\}$ hat Ordnung $q := |\mathbb{G}| := \frac{p-1}{2}$. Ferner sei g ein Erzeuger von $\mathbb{G}$.

(i) Geben Sie die Algorithmen (Sig, Ver) für das ElGamal-Signaturverfahren über der Gruppe $\mathbb{G}$ an. Nehmen Sie dazu an, dass die Schlüssel pk und sk die Form $pk = (p,\ g,\ g^x \bmod p)$ beziehungsweise $sk = (p,\ g,\ x)$ haben, wobei x zufällig aus $\mathbb{Z}_{|\mathbb{G}|}$ gewählt ist.

(ii) Kann das ElGamal-Signaturverfahren unter geeigneten zahlentheoretischen Annahmen EUF-CMA-sicher sein? Begründen Sie Ihre Antwort.

(b) Betrachten wir nun das ElGamal-Verschlüsselungsverfahren (Gen, Enc, Dec) über der Gruppe $\mathbb{G}$ (wobei $\mathbb{G}$ wie in Aufgabenteil (a) definiert ist).

(i) Geben Sie die Algorithmen (Enc, Dec) für das ElGamal-Verschlüsselungsverfahren über der Gruppe $\mathbb{G}$ an. Nehmen Sie dazu an, dass die Schlüssel pk und sk die Form $pk = (p,\ g,\ g^x \bmod p)$ beziehungsweise $sk = (p,\ g,\ x)$ haben, wobei x zufällig aus $\mathbb{Z}_{|\mathbb{G}|}$ gewählt ist.

(ii) Aus der Vorlesung ist bekannt, dass dieses Verschlüsselungsverfahren unter naheliegenden Annahmen IND-CPA-sicher ist, wenn es in $\mathbb{G} = Q(\mathbb{Z}_p^\times)$ verwendet wird.

Im Folgenden betrachten wir welches Problem auftritt, wenn das ElGamal-Verschlüsselungsverfahren über der ganzen Gruppe $\mathbb{Z}_p^\times$ verwendet wird. Dazu sei $\mathbb{G} := \mathbb{Z}_p^\times$ und g ein Erzeuger von $\mathbb{Z}_p^\times$.

(1) Nehmen Sie zunächst an, dass das im öffentlichen Schlüssel enthaltene Gruppenelement $g^x \bmod p$ immer ein Quadrat in $\mathbb{Z}_p^\times$ ist.
Geben Sie einen PPT-Angreifer an, der das IND-CPA-Spiel mit nicht-vernachlässigbarer Wahrscheinlichkeit gewinnt. (Für die Erfolgswahrscheinlichkeit und die Laufzeit reicht eine kurze Begründung aus.)
Sie dürfen die folgenden Hinweise ohne Beweis verwenden:
Hinweis 1: Es kann effizient (in polynomieller Zeit) überprüft werden, ob eine Zahl ein Quadrat in $\mathbb{Z}_p^\times$ ist oder nicht. Sie können annehmen, dass eine in Polynomialzeit berechenbare Funktion `isSquare`$(\cdot)$ gegeben ist, die ausgibt, ob die Eingabe ein Quadrat in $\mathbb{Z}_p^\times$ ist oder nicht.
Hinweis 2: Produkte von Quadraten sind Quadrate. Das Produkt von einem Quadrat mit einem Nicht-Quadrat ist ein Nicht-Quadrat.
Hinweis 3: Erzeuger von $\mathbb{Z}_p^\times$ sind keine Quadrate. Genau die Hälfte der Elemente in $\mathbb{Z}_p^\times$ sind Quadrate.

(2) Betrachten wir nun den Fall, dass das im öffentlichen Schlüssel enthaltene Gruppenelement $g^x \bmod p$ immer als Nicht-Quadrat erzeugt wird. Funktioniert der obige Angriff auch in diesem Fall noch? Begründen Sie Ihre Antwort. Geben Sie insbesondere genau an, was Ihr Angreifer in welchen Fällen ausgibt.
Sie dürfen die Hinweise aus dem vorigen Aufgabenteil (b)(ii)(1) wieder ohne Beweis verwenden.

Aufgabe 3. $(3 + 2 + 2 + 2$ Punkte)

(a) Sei (Gen, Sig, Ver) ein Signaturverfahren. Geben Sie die Definition von EUF-CMA-Sicherheit an. Geben Sie dazu insbesondere an, wann ein Signaturverfahren (Gen, Sig, Ver) EUF-CMA-sicher ist. Definieren Sie dazu auch das EUF-CMA-Spiel.

(b) Sei $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ eine Blockchiffre mit Schlüsselraum $\{0,1\}^k$ und Nachrichten- und Chiffratraum $\{0,1\}^n$. Die Blockchiffre soll im CBC-Modus betrieben werden. Skizzieren Sie die Verschlüsselung und die Entschlüsselung im CBC-Modus.

(c) Sei $H\colon \{0,1\}^* \to \{0,1\}^k$ eine kryptographische Hashfunktion. Geben Sie die Definition von Kollisionsresistenz für kryptographische Hashfunktionen an. Geben Sie dazu insbesondere an, wann eine kryptographische Hashfunktion H kollisionsresistent ist.

(d) Sei $H\colon \{0,1\}^* \to \{0,1\}^k$ eine kryptographische Hashfunktion. Nennen Sie 2 Möglichkeiten für H Key-Strengthening durchzuführen, d.h. die Auswertung von H zu erschweren.

Aufgabe 4. $(10(= 2 + 8) + 5(= 1 + 4)$ Punkte)

In der gesamten Aufgabe sei (Gen, Enc, Dec) ein IND-CPA-sicheres asymmetrisches Verschlüsselungsverfahren. Wir konstruieren daraus zwei neue asymmetrische Verschlüsselungsverfahren.

(a) (Gen′, Enc′, Dec′) sei wie folgt definiert:

$\mathsf{Gen}'(1^k)$	$\mathsf{Enc}'(pk, m)$	$\mathsf{Dec}'(sk, C = (C_1, C_2))$
$(pk, sk) \leftarrow \mathsf{Gen}(1^k)$	wähle R zuf. aus $\{0,1\}^k$	$R \leftarrow \mathsf{Dec}(sk, C_2)$
return (pk, sk)	$C_1 := m \oplus R$	$m := C_1 \oplus R$
	$C_2 \leftarrow \mathsf{Enc}(pk, R)$	**return** m
	return $C := (C_1, C_2)$	

Das so definierte Verschlüsselungsverfahren (Gen′, Enc′, Dec′) ist nur für die Verschlüsselung von Nachrichten in $\{0,1\}^k$ geeignet.

(i) Zeigen Sie die Korrektheit von $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$.

(ii) (Gen', Enc', Dec') ist IND-CPA-sicher, wenn (Gen, Enc, Dec) IND-CPA-sicher ist. Abb. 1 zeigt eine Beweisskizze für den IND-CPA-Beweis. Für den Beweis wird ein PPT Angreifer $\mathcal{A}$ auf die IND-CPA-Sicherheit von (Gen', Enc', Dec') mit nicht-vernachlässigbarer Erfolgswahrscheinlichkeit angenommen. Daraus soll ein PPT Angreifer $\mathcal{B}$ auf die IND-CPA-Sicherheit von (Gen, Enc, Dec) konstruiert werden, dessen Erfolgswahrscheinlichkeit nicht-vernachlässigbar ist.

Vervollständigen Sie die Beweisskizze indem Sie die Stellen (1), (2), (3), (4) und (5) in der unten stehenden Tabelle ergänzen. Zur Erinnerung: Gegeben (Gen, Enc, Dec) ist (Gen', Enc', Dec') wie folgt definiert:

$\mathsf{Gen}'(1^k)$	$\mathsf{Enc}'(pk, m)$	$\mathsf{Dec}'(sk, C = (C_1, C_2))$
$(pk, sk) \leftarrow \mathsf{Gen}(1^k)$	wähle R zuf. aus $\{0,1\}^k$	$R \leftarrow \mathsf{Dec}(sk, C_2)$
return (pk, sk)	$C_1 := m \oplus R$	$m := C_1 \oplus R$
	$C_2 \leftarrow \mathsf{Enc}(pk, R)$	**return** m
	return $C := (C_1, C_2)$	

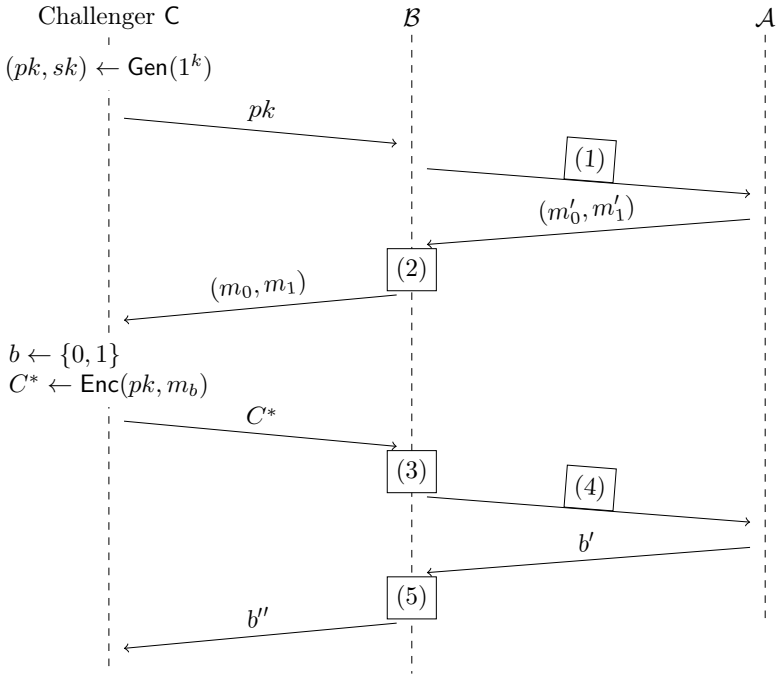

Abbildung 1: IND-CPA-Reduktion.

(1)	
(2)	
(3)	
(4)	
(5)	

(b) Sei $H\colon \{0,1\}^* \to \{0,1\}^k$ eine kollisionsresistente kryptographische Hashfunktion. Das asymmetrische Verschlüsselungsverfahren (Gen^*, Enc^*, Dec^*) sei wie folgt definiert.

$\mathsf{Gen}^*(1^k)$	$\mathsf{Enc}^*(pk, m)$	$\mathsf{Dec}^*(sk, C = (C_1, C_2))$
$(pk, sk) \leftarrow \mathsf{Gen}(1^k)$	$C_1 := H(m)$	$m \leftarrow \mathsf{Dec}(sk, C_2)$
return (pk, sk)	$C_2 \leftarrow \mathsf{Enc}(pk, m)$	**return** m
	return $C := (C_1, C_2)$	

(i) Zeigen Sie die Korrektheit von (Gen^*, Enc^*, Dec^*).

(ii) Beweisen Sie, dass (Gen^*, Enc^*, Dec^*) nicht IND-CPA-sicher ist. Geben Sie dazu einen entsprechenden IND-CPA-Angreifer für (Gen^*, Enc^*, Dec^*) an. Geben Sie außerdem an, wie genau Ihr Angreifer die Nachrichten m_0 und m_1, die er an den Challenger sendet, wählt. Achten Sie darauf, dass Ihr Angreifer polynomielle Laufzeit und einen nicht-vernachlässigbaren Vorteil gegenüber Raten hat.

Aufgabe 5. (6 Punkte)

Im Bell-LaPadula-Modell aus der Vorlesung seien

- die Subjektmenge $\mathcal{S} = \{\texttt{alice}, \texttt{admin}, \texttt{bob}\}$,
- die Objektmenge $\mathcal{O} = \{\texttt{diary}, \texttt{exam}, \texttt{shared}, \texttt{passwd}\}$,
- die Menge der Zugriffsoperationen $\mathcal{A} = \{\texttt{read}, \texttt{write}, \texttt{append}, \texttt{execute}\}$ und
- die Menge der Sicherheitslevel $\mathcal{L} = \{\texttt{topsecret}, \texttt{alice's secrets}, \texttt{bob's secrets}, \texttt{unclassified}\}$ mit der $\mathcal{L}$-Halbordnung

$$\begin{array}{ccccc} \texttt{topsecret} & \geq & \texttt{alice's secrets} & \geq & \texttt{unclassified} \\ \texttt{topsecret} & \geq & \texttt{bob's secrets} & \geq & \texttt{unclassified} \end{array}$$

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

	diary	exam	shared	passwd
alice	{read, write, append}	$\emptyset$	$\mathcal{A}$	{read}
bob	{read, append}	{read, write, append}	$\mathcal{A}$	{read}
admin	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$

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

	$f_s(\cdot)$	$f_c(\cdot)$
alice	alice's secrets	unclassified
bob	bob's secrets	unclassified
admin	topsecret	unclassified

	$f_o(\cdot)$
diary	alice's secrets
exam	bob's secrets
shared	unclassified
passwd	topsecret

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

1. (bob, diary, read)
2. (alice, diary, read)
3. (alice, shared, append)
4. (bob, shared, read)
5. (admin, exam, read)
6. (admin, passwd, append)
7. (admin, diary, execute)
8. (admin, exam, append)
9. (admin, shared, append)

Geben Sie für die einzelnen Zugriffe jeweils an, ob die ds-, ss- oder $\star$-Eigenschaft erfüllt oder verletzt ist. Nutzen Sie dafür die Spalten „ds“, „ss“ und „$\star$“ der unten stehenden Tabelle. Benutzen Sie dabei ✓ für „erfüllt“ und × für „verletzt“. Geben Sie für alle verletzten Eigenschaften in der Spalte „Bemerkung“ an, **warum** sie jeweils verletzt sind. Ändert sich durch einen Zugriff der aktuelle Sicherheitslevel des Subjekts, so geben Sie in der Spalte „Bemerkung“ an, wie er sich ändert. Gehen Sie davon aus, dass zu Beginn noch kein Zugriff stattgefunden hat.

Zur Erinnerung:

Die Zugriffskontrollmatrix M:

	diary	exam	shared	passwd
alice	{read, write, append}	$\emptyset$	$\mathcal{A}$	{read}
bob	{read, append}	{read, write, append}	$\mathcal{A}$	{read}
admin	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$

Die Sicherheitslevel $f_s(\cdot)$, $f_c(\cdot)$ und $f_o(\cdot)$:

	$f_s(\cdot)$	$f_c(\cdot)$
alice	alice's secrets	unclassified
bob	bob's secrets	unclassified
admin	topsecret	unclassified

	$f_o(\cdot)$
diary	alice's secrets
exam	bob's secrets
shared	unclassified
passwd	topsecret

	Zugriff	ds	ss	$\star$	Bemerkung
1.	(bob, diary, read)				
2.	(alice, diary, read)				
3.	(alice, shared, append)				
4.	(bob, shared, read)				
5.	(admin, exam, read)				
6.	(admin, passwd, append)				
7.	(admin, diary, execute)				
8.	(admin, exam, append)				
9.	(admin, shared, append)				