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

Stammvorlesung Sicherheit im Sommersemester 2014

Klausur

22.07.2014

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	3	3	3	11					
2	4	6	-	-	10			-	-	
3	3	4	4	-	11				-	
4	3	4	4	-	11				-	
5	7				7					
6	10x1				10					
Σ					60					

Aufgabe 1. (2+3+3+3 Punkte) Betrachten Sie das einfache Lehrbuch-RSA-Verschlüsselungsverfahren aus der Vorlesung.

(a) Seien die Primzahlen $P = 7$ und $Q = 17$ gegeben. Berechnen Sie den geheimen Exponenten d zum öffentlichen Exponenten $e = 5$ und geben Sie den öffentlichen Schlüssel an.

(b) (i) Verschlüsseln Sie die Nachricht $M = 97$ mit den Schlüsseln aus (a).

(ii) Entschlüsseln Sie das Chiffrat $C = 32$ mit den Schlüsseln aus (a).

Hinweis: Rechnen Sie vorteilhaft! Zerlegen Sie die Zahlen geschickt in einzelne Faktoren und verwenden Sie bei Bedarf negative Repräsentanten modulo N.

(c) Das betrachtete Lehrbuch-RSA-Verfahren ist IND-CPA-unsicher.

(i) Geben Sie einen effizienten Angreifer an, der das IND-CPA-Experiment mit Wahrscheinlichkeit 1 gewinnt.

(ii) Nennen Sie eine Möglichkeit, wie man diesen Angriff verhindern könnte.

(d) Wir betrachten folgendes Sicherheitsspiel für das Lehrbuch-RSA-Verfahren: Sei $pk = (N, e)$ mit $N = PQ$ bekannt. Ein Angreifer bekommt vom Challenger ein Chiffrat C^* zur Nachricht M^* und soll M^* zurückgeben. Er darf sich zusätzlich Chiffrate $C \neq C^*$ vom Challenger entschlüsseln lassen. Geben Sie einen effizienten Angreifer mit Erfolgswahrscheinlichkeit 1 an.

Aufgabe 2. (4+6 Punkte)

(a) Gegeben sei ein MAC für zwei Parteien A und B:

(i) Beschreiben Sie allgemein die Algorithmen eines MAC-Verfahrens und eventuelle Annahmen an die Parteien bzw. Anforderungen an die Algorithmen.

(ii) Nennen Sie 2 Ziele, die durch ein MAC-Verfahren sichergestellt werden sollen.

(iii) Was ist der Unterschied zu einer digitalen Signatur?

(b) Betrachten wir nun das ElGamal-Signaturverfahren $(\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ über der zyklischen Gruppe $\mathbb{G} = \langle g \rangle$.

(i) Sei $h \in \mathbb{G}$. Geben Sie den Secret Key sk zum Public Key $pk = (\mathbb{G}, g, h)$ an.

(ii) Geben Sie einen Angriff an, der zeigt, dass das Verfahren aus der Vorlesung nicht EUF-CMA-sicher ist.

(iii) Wie kann man Ihren Angriff aus (ii) verhindern?

(iv) Wir verändern den Signaturalgorithmus zu $\mathsf{Sig}(sk, M) = \sigma$, wobei $\sigma \cdot x = M \bmod |\mathbb{G}|$ für das geheime x aus dem Secret Key gilt. Wie sieht die entsprechende Verifikation aus und wieso ist diese Änderung problematisch?

Aufgabe 3. (3+4+4 Punkte)

(a) Beschreiben Sie für eine Blockchiffre $E(K, X) : \{0,1\}^k \times \{0,1\}^{2k} \to \{0,1\}^{2k}$, wie sie eine Nachricht $M \in \{0,1\}^*$ im CBC-Mode ver- und entschlüsselt und nennen Sie einen Vorteil gegenüber dem ECB-Mode.

(b) Aus der Vorlesung ist die Blockchiffre DES bekannt. Hierbei handelt es sich um eine Feistel-Chiffre mit einer Blocklänge von 64 Bit und einer effektiven Schlüssellänge von 56 Bit. Wir betrachten eine Variante von DES, bei der die Rundenschlüssel nicht aus dem Gesamtvorrat von 56 Bit berechnet werden, sondern in den Feistel-Runden 1-8 mittels einer beliebigen Funktion aus der ersten 28-Bit-Schlüsselhälfte erzeugt werden und in den Feistel-Runden 9-16 mittels derselben Funktion aus der zweiten 28-Bit-Schlüsselhälfte erzeugt werden.

Konstruieren Sie einen Angriff, mit dem sich der zur Verschlüsselung benutzte geheime Schlüssel K bestimmen lässt, und der höchstens 2^{40} Operationen benötigt. Ihr Angriffsalgorithmus ist in Besitz von einigen Klartext-Chiffrat-Paaren. Erläutern Sie kurz, warum Ihr Angriff tatsächlich mit hoher Wahrscheinlichkeit den richtigen Schlüssel findet und zeigen Sie kurz, dass Ihr Angriff tatsächlich höchstens 2^{40} Operationen benötigt.

Hinweis: Angriffe, die weniger als 2^{40} Operationen benötigen sind ebenfalls als Lösung zulässig. Nehmen Sie an, dass ein Algorithmus zur Sortierung von n Elementen exakt $n \cdot \log n$ Operationen benötigt.

(c) Sei $n \in \mathbb{N}, n \geq 2$. Wir betrachten eine symmetrische Chiffre

$$\begin{aligned} \text{Enc} : \{0,1\}^{2n} \times \{0,1\}^{2n} &\to \{0,1\}^{2n}, \\ \text{Enc}(K, M) &= C = C_1 \dots C_{2n}, \end{aligned}$$

die Nachrichten $M = M_1 \dots M_{2n} \in \{0,1\}^{2n}$ mit einem $2n$-Bit-Schlüssel $K = K_1 \dots K_{2n}$ folgendermaßen verschlüsselt:

M_1	M_2	$\dots$	M_n	M_{n+1}	M_{n+2}	$\dots$	M_{2n}
$\oplus$	$\oplus$	$\dots$	$\oplus$	$\oplus$	$\oplus$	$\dots$	$\oplus$
K_1	K_3	$\dots$	K_{2n-1}	K_{2n}	K_{2n-1}		K_{n+1}
$\oplus$	$\oplus$	$\dots$	$\oplus$	$\oplus$	$\oplus$	$\dots$	$\oplus$
K_2	K_4	$\dots$	K_{2n}	K_1	K_2		K_n
C_1	C_2	$\dots$	C_n	C_{n+1}	C_{n+2}	$\dots$	C_{2n}

Wie kann ein Angreifer geschickt zwei Nachrichten $M^{(1)} \neq M^{(2)}$ gleicher Länge wählen und **nur** mithilfe des Chiffrats und der gewählten Nachrichten entscheiden, welche der beiden verschlüsselt wurde?

Aufgabe 4. (3+4+4 Punkte) Eine vertrauenswürdige Instanz veröffentlicht einen RSA-Modulus $N = PQ$. Sie zieht zufällig gleichverteilt geheime Zahlen $s_1, \ldots, s_k \leftarrow \mathbb{Z}_n$ und veröffentlicht $v_i = s_i^2 \bmod N$ für alle $i \in \{1, \ldots, k\}$. Ein Prover P erhält die geheimen Zahlen s_i für alle $i \in \{1, \ldots, k\}$ und will einen Verifier V überzeugen, dass er die Quadratwurzeln von v_i kennt. Dazu wird folgendes Protokoll ausgeführt:

1. P wählt $r \xleftarrow{\$} \mathbb{Z}_N$, berechnet $x = r^2 \bmod N$, sendet x an V.
2. V wählt zufällig gleichverteilt $b_1, \ldots, b_k \leftarrow \{0, 1\}$, sendet b_i, für alle $i \in \{1, \ldots, k\}$ an P.
3. P berechnet $y = r \prod_{i=1}^{k} s_i^{b_i} \bmod N$, sendet y an V.
4. V überprüft, ob $y^2 = x \prod_{i=1}^{k} v_i^{b_i} \bmod N$ gilt.

Dies wird t Mal wiederholt.

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

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

(c) Betrachten wir für $k = 1, t = 2$ den Spezialfall, dass jedes Mal der gleiche Zufall r verwendet wird. Wie muss V dabei vorgehen um geheime Informationen zu bekommen und welche sind dies?

Aufgabe 5. (7 Punkte) Im Bell-LaPadula-Modell aus der Vorlesung seien

- die Subjektmenge $\mathcal{S} = \{s_1, s_2, s_3\}$,
- die Objektmenge $\mathcal{O} = \{o_1, o_2, o_3, o_4\}$,
- 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	o_4
s_1	{read, append, execute}	{read, write, append}	{read, append}	$\mathcal{A}$
s_2	{read}	{read, execute}	{read, append}	$\mathcal{A}$
s_3	$\emptyset$	{read}	{read, append}	{read, write, append}

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

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

	$f_o(\cdot)$
o_1	topsecret
o_2	topsecret
o_3	secret
o_4	unclassified

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

1. $(s_1, o_2, \texttt{read})$
2. $(s_2, o_2, \texttt{read})$
3. $(s_3, o_4, \texttt{execute})$
4. $(s_3, o_3, \texttt{append})$
5. $(s_2, o_3, \texttt{write})$
6. $(s_1, o_3, \texttt{write})$

Beschreiben Sie – beispielsweise in der Spalte "Bemerkungen" in der unter stehenden Tabelle, die Sie für Ihre Lösung benutzen können –, ob die einzelnen Zugriffe gültig (✓) oder ungültig (×) sind, und ob der aktuelle Sicherheitslevel nach gültigem Zugriff geändert wird. Falls der Zugriff nicht gültig ist, zeigen Sie auf, welche Eigenschaft(en) – im Sinne der ds-, ss- oder $\star$-Eigenschaft – verletzt wurde(n). Begründen Sie Ihre Entscheidung (ebenfalls beispielsweise in der Spalte "Bemerkungen" unten). Gehen Sie davon aus, dass zu Beginn noch kein Zugriff stattgefunden hat.

	Zugriff	ds	ss	$\star$	Bemerkungen
1.	$(s_1, o_2, \texttt{read})$				
2.	$(s_2, o_2, \texttt{read})$				
3.	$(s_3, o_4, \texttt{execute})$				
4.	$(s_3, o_3, \texttt{append})$				
5.	$(s_2, o_3, \texttt{write})$				
6.	$(s_1, o_3, \texttt{write})$				

Aufgabe 6. (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
Ein Public-Key-Verfahren mit deterministischem Enc-Algorithmus erfüllt den IND-CPA-Sicherheitsbegriff.		
Der One-Time-Pad ist sicher gegen Veränderungen der verschlüsselten Nachricht.		
Im CBC-Mode sind Ver- und Entschlüsselung parallelisierbar.		
$H'(x) = H(f(x))$ ist kollisionsresistent, falls H kollisionsresistent und f effizient berechenbar und injektiv ist.		
$f(k) = \frac{1}{k^c}$, für c konstant, ist vernachlässigbar in k.		
Für den erweiterten euklidischen Algorithmus $EE(a, b) = (\alpha, \beta)$ gilt $\alpha \cdot a + \beta \cdot b = 1$ für alle $a, b \in \mathbb{N}$.		
Im Kerberos-Protokoll werden keine Man-in-the-middle-Angriffe berücksichtigt.		
Für $M := \sigma^d \bmod N$ im RSA-Signaturverfahren mit $pk = (N, e), sk = (N, d)$ ist M eine Signatur für σ.		
Das Commitment $\mathsf{Com}(M; R) = \mathsf{H}(M, R)$ ist binding, falls H eine kollisionsresistente Hashfunktion ist.		
Das Chinese Wall Modell sichert eine konfliktfreie Zuordnung von Beratern zu Objekten zu.		