Einführung in die
Kryptographie
WS 2008/2009

Technische Universität Darmstadt
Fachbereich Informatik
Prof. Johannes Buchmann
Erik Tews
25. Februar 2009

Klausur mit Lösung zum Wintersemester 2008/2009

Name, Vorname: ..... Matrikelnummer: .....

Studiengang: ..... Diplom ☐ Bachelor ☐ Master ☐

Fachbereich: ..... Fachsemester: .....

Prüfungssekretariat in dem Sie angemeldet sind: ..... Keins ☐

Taschenrechnermodell: .....

Wiederholer? ☐ Wievielter Versuch: ..... Jahr des letzten Versuchs: .....

Zulassung: Sie sind zu dieser Klausur nur zugelassen, wenn sie sich gemäß den Regeln Ihrer Studienordnung dafür angemeldet haben.

Unterschrift: .....

Viel Erfolg!

Punktestand

Aufgabe	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	Ferienübung	Σ
Maximale Punktzahl	20	20	20	20	14	20	20	20	20	20	20	
Erreichte Punktzahl												

Hinweise:

Halten Sie Ihren Studienausweis und einen Lichtbildausweis zur Kontrolle bereit. Setzen Sie sich so, dass 2 Plätze rechts und links neben Ihnen, sowie die gesamte Reihe vor Ihnen frei ist.

Notation

- Für jede natürliche Zahl n bezeichnet $(\mathbb{Z}/n\mathbb{Z})$ den Restklassenring der ganzen Zahlen modulo n und $(\mathbb{Z}/n\mathbb{Z})^*$ die multiplikative Gruppe.
- Für einen Körper $\mathbb{K}$ bezeichnet $\mathbb{K}[X]$ den Polynomring über diesem Körper mit Variable X.

Aufgabenblätter

- Füllen Sie das Deckblatt vollständig aus.
- Prüfen Sie, ob die Klausur **10 Aufgaben** und **12 Seiten** enthält.
- Kennzeichnen Sie alle verwendeten Aufgaben- und Zusatzblätter zuerst mit Name und Matrikelnummer.
- Verwenden Sie für jede Aufgabe falls möglich ein neues Blatt.
- Geben Sie die verwendeten Formeln, Sachverhalte und Zwischenergebnisse an.

Bewertung

- Für volle Punktzahl müssen sie bei jeder Aufgabe auch Ihre Lösung begründen bzw. Zwischenschritte mit angeben.
- Unleserlichkeit kann zu Punktabzug führen.
- Sie konnten in der Ferienübung **20 Punkte** erzielen, in der Klausur gibt es maximal **194 Punkte**.
- Die Gesamtnote ergibt sich aus der Summe der in der Klausur und Ferienübung erzielten Punkte.
- Das Ergebnis der Ferienübung bildet keine Zulassungsvoraussetzung zur Klausur.

Dauer der Klausur und zugelassene Hilfsmittel

- Ihnen stehen **120 Minuten** zum Bearbeiten der Aufgaben zur Verfügung.
- Einzige zugelassene Hilfsmittel sind **ein** nicht programmierbarer Taschenrechner und ein beidseitig handschriftlich beschriebenes DIN-A4 Blatt. Tragen Sie die Modellbezeichnung Ihres Taschenrechners in das Deckblatt ein.
- Andere elektronische Geräte (Handys, PDAs, Laptops, programmierbare Taschenrechner) bitte der Klausuraufsicht zur Verwahrung geben.
- Studierende, deren Muttersprache nicht Deutsch ist, können zusätzlich ein zweisprachiges gedrucktes Wörterbuch verwenden.
- Die Klausuraufsicht überprüft vielleicht die Hilfsmittel.

K1 (Polynome). Name: ..... Matrikelnr.: .....
(20 Punkte)

Seien $a(X) = X^3 + X + 1$ und $b(X) = X + 1$ zwei Polynome in $GF(2)[X]$. Berechnen Sie Polynome u, v in $GF(2)[X]$ mit der Eigenschaft $u * a + v * b = 1$.

Lösung. Wir verwenden den EEA um eine solche Lineardarstellung zu berechnen:

$$\begin{array}{ccc} X^3+X+1 & X+1 & 1 \\ & X^2+X & \\ 1 & 0 & 1 = u \\ 0 & 1 & X^2+X = v \end{array}$$

Damit lautet die Lösung $u * a + v * b = (1) * (X^3 + X + 1) + (X^2 + X) * (X + 1) = 1$.

Hinweis: Da wir in $GF(2)[X]$ rechnen, müssen wir beim EEA und anderen Rechnungen Vorzeichen nicht weiter beachten.

K2 (Endlicher Körper). Name: ..... Matrikelnr.: .....
(20 Punkte)

Konstruieren Sie einen endlichen Körper mit 4 Elementen. Geben sie die Additions- und Multiplikationstabelle an. Das Körperpolynom können Sie frei wählen.

Lösung. Wir wählen als Körperpolynom $X^2 + X + 1$, das Polynom ist irreduzibel, und es ist auch das einzist mögliche Polynom. Die Elemente des Körpers sind somit 0, 1, X und $X + 1$. Wir erhalten dann als Addtionstabelle:

	0	1	X	$X+1$
0	0	1	X	$X+1$
1	1	0	$X+1$	X
X	X	$X+1$	0	1
$X+1$	$X+1$	X	1	0

Und als Multiplikationstabelle:

	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	$X+1$	1
$X+1$	0	$X+1$	1	X

K3 (Elementordnung). Name: ..... Matrikelnr.: .....
(20 Punkte)

Bestimmen Sie die Ordnung von 5 in $(\mathbb{Z}/17\mathbb{Z})^*$. Finden sie dann ein Element der Ordnung 4 in dieser Gruppe.

Lösung. Da 17 eine Primzahl und die Gruppenordnung so $17 - 1 = 16$ ist, kommen nur Teiler der 16 als Ordnung für 5 in Frage, also $1, 2, 4, 8$ und 16. Wir prüfen $5^1 = 5 \neq 1 \bmod 17$, $5^2 = 8 \neq 1 \bmod 17$, $5^4 = 13 \neq 1 \bmod 17$, $5^8 = 16 \neq 1 \bmod 17$. Damit muss die Ordnung von 5 zwingend 16 sein.

Damit muss die Ordnung von $5^4 = 13 \bmod 17$ zwingend 4 sein, denn $(5^4)^4 = 5^{16} = 1 \bmod 17$, und für keine kleinere Zahl als 4 gilt $13^x = 1 \bmod 17$, sonst wäre die Ordnung von 5 auch kleiner als 16.

K4 (ElGamal). Name: ..... Matrikelnr.: .....
(20 Punkte)

Sie haben den öffentlichen ElGamal-Schlüssel $(p, g, A) = (17, 3, 8)$. Verschlüsseln Sie den Klartext $m = 5$ mit diesem Schlüssel mit dem ElGamal Verschlüsselungsverfahren. Wählen Sie dabei die Zufallszahl $b = 5$.

Lösung. wir berechen $c = A^b m = 8^5 * 5 = 11 \bmod 17$ und $B = g^b = 5 \bmod 17$. Der Chiffretext ist dann $(c, B) = (11, 5)$.

K5 (Multiple Choice). Name: ..... Matrikelnr.: .....
(14 Punkte)

Für eine korrekte Antwort gibt es zwei Punkte, für eine falsche Antwort werden zwei Punkte abgezogen.

Aussage	Wahr	Falsch
Beim DSA-Signieren sind alle Exponenten ≤ 256 Bit	X	
Hashfunktionen mit Hashlänge 80 Bit können kollisionsresistent sein		X
AES ist eine affin lineare Blockchiffre		X
Bei RSA-Signaturen darf man einen öffentliche Schlüssel mit $e = 3$ verwendet werden	X	
Das Vernam OTP ist perfekt geheim	X	
$(\mathbb{Z}/17\mathbb{Z})^*$ enthält ein Element der Ordnung 3		X
Aus Sicherheitsgründen muss die Primzahl bei Shamirs Secret-Sharing-Verfahren wenigstens 1024 Bit lang sein		X

K6 (RSA Entschlüsselungsexponenten). Name: ..... Matrikelnr.: .....
(20 Punkte)

Es wird bei einer RSA Verschlüsselung das RSA-Modul $n = 35$ verwendet. Welche Zahlen könnten als geheimer Entschlüsselungexponent d gewählt werden?

Lösung. Für den privaten RSA-Schlüssel gilt $e * d = 1 \bmod \varphi(n)$. Zu jedem e gibt es genau dann ein passendes d, wenn e bzw. d teilerfremd sind zu $\varphi(n)$. Zusätzlich ist $e = 1$ verboten, und damit ebenfalls $d = 1^{-1} = 1 \bmod \varphi(n)$. Damit bleiben noch alle zu $\varphi(n) = 4 * 6 = 24 = 2 * 2 * 2 * 3$ teilerfremden Zahlen zwischen 3 und 23 einschließlich übrig. Das sind $3, 5, 7, 9, 11, 13, 17, 19, 23$.

K7 (Babystep-Giantstep). Name: ..... Matrikelnr.: .....
(20 Punkte)

Sie wollen $a^x \equiv b \bmod p$ lösen. Dabei sind a und b ganze Zahlen und p ist eine Primzahl. Angenommen Sie wissen, dass $0 < x < B < p - 1$ ist. Zeigen Sie, wie man x in $O(\sqrt{B})$ vielen Operationen finden kann. Begründen Sie ihre Antwort.

Lösung. Beim Babystep-Giantstep Verfahren wird x aufgeteilt in $x = q * m + r$. Dabei wird $m = \lceil \sqrt{p} \rceil$ gewählt, so dass q und r nicht größer sind als m. Ist bekannt, dass x ein relativ kleiner Wert ist (weil z. B. eine Implementierung aus Performancegründen x immer relativ klein wählt), so kann $m = \lceil \sqrt{B} \rceil$ gewählt werden, x läßt sich so ebenfalls als $q*m+r$ darstellen. Dabei sind nun q und r maximal m. Existiert so eine Darstellung von x, so findet Babystep-Giantstep sie. Bei der Ausführung sind die längsten Operationen das erstellen einer Tabelle mit m Einträgen ($O(\sqrt{B})$) und maximal m Zugriffe auf die Tabelle ($O(\sqrt{B})$). Damit ergibt sich eine Gesamtlaufzeit von $O(\sqrt{B})$.

K8 (Rabin). Name: ..... Matrikelnr.: .....
(20 Punkte)

Ein Ihnen unbekannter Klartext wird mit dem Rabin-Modul $n_1 = 14$ zum Chiffretext $c_1 = 2$ und mit dem Rabin-Modul $n_2 = 15$ zum Chiffretext $c_2 = 1$ verschlüsselt. Berechnen Sie ein mögliches m mit der low exponent attacke.

Lösung. Wir berechnen zuerst mit Hilfe des CRT ein x mod $14*15$ mit $x = 2$ mod 14 und $x = 1$ mod 15. Wir erhalten so $x = 1*14*14+2*1*15 = 16$ mod $14*15$. Durch ziehen der Wurzel aus 16 erhalten wir 4 als einen möglichen Klartext, der diese Eigenschaft hat.

K9 (Affin-lineare Chiffre). Name: ..... Matrikelnr.: .....
(20 Punkte)

Eine affin-lineare Chiffre mit Blocklänge 2 und Modul 2 wird benutzt. Folgende (Klartext, Chiffretext)-Paare werden beobachtet.

$$\left(\begin{array}{c} 1 \\ 0 \end{array}, \begin{array}{c} 0 \\ 1 \end{array}\right), \left(\begin{array}{c} 1 \\ 1 \end{array}, \begin{array}{c} 0 \\ 0 \end{array}\right), \left(\begin{array}{c} 0 \\ 0 \end{array}, \begin{array}{c} 1 \\ 0 \end{array}\right)$$

Wie lautet die Entschlüsselung des Chiffretexts $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$? Wie lautet der Schlüssel?

Lösung. Die Verschlüsselungsfunktion hat die Form $c = Am+b$. Ist $m = (0,0)$, so ist das Ergebnis b. Wir können so einfach $b = (1,0)$ bestimmen. Noch zu bestimmen ist die Matrix A. Aus $A*(1,0)+(1,0) = (0,1)$ können wir erkennen $A*(1,0) = (1,1)$. Damit ist die erste Spalte der Matrix A $(1,1)$. Aus $A*(1,1)+(1,0) = (0,0)$ wissen wir $A*(1,1) = (1,0)$. Also ist die Summe der ersten beiden Matrixspalten damit $(1,0)$ und damit die zweite Spalte der Matrix $(0,1)$.

Damit ist der Schlüssel:

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$$b = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Die Entschlüsselung des Chiffretextes lautet $(0,1)$, da die Abbildung bijektiv ist, es nur 4 Klartexte gibt, und dieser der einzig nicht genannte Klartext in der Aufgabenstellung ist.

K10 (Secret Sharing). Name: ..... Matrikelnr.: .....
(20 Punkte)

Sie haben das Geheimnis $s = 5$ auf 3 Personen verteilt. Gerechnet wird modulo 7. Die erste Person bekommt den Share $(x, f(x)) = (3, 1)$. Zwei Personen sollen das Geheimnis bestimmen können. Weniger nicht. Die Shares der anderen sind $(x, f(x)) = (2, \quad)$ und $(x, f(x)) = (4, \quad)$. Vervollständigen Sie diese Info.

Lösung. Da 2 Personen das Geheimnis rekonstruieren sollen, ist das Polynom von der Form $f(x) = a * x + b$. Aus $s = 5$ können wir $b = 5$ ablesen. Nun müssen wir nur noch die Steigung bestimmen. Da $f(0) = 5$ und $f(3) = 1$ erkennen wir dass die Steigung $3^{-1} * 3 = 1 \bmod 7$ sein muss. Die Funktion ist so $f(x) = 1 * x + 5$. Damit lauten die restlichen Shares $(x, f(x)) = (2, 0)$ und $(x, f(x)) = (4, 2)$.