Einführung in die
Kryptographie
WS 2008/2009

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

Klausur 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 $u * a + v * b = 1$.

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.

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.

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 $b = 5$.

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

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?

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.

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.

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?

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.