



Klausur im WS 2005/06 zur Vorlesung Einführung in die Kryptographie

21. Februar 2006

Matrikelnummer:

Name, Vorname:

Verwendeter Taschenrechner:

Fachbereich: Fachsemester:

Studiengang: Diplom Bachelor Master

Angemeldet im Prüfungssekretariat:Nein

Krypto-Klausur bereits abgelegt? Jahr(e): Note:

Zulassung: Sie sind zur Prüfung zur „Einführung in die Kryptographie“ nur dann zugelassen, wenn sie alle der folgenden Voraussetzungen erfüllen:

- Sie haben sich ordnungsgemäß zur vorlesungsbegleitenden Prüfung zur Einführung in die Kryptographie angemeldet.
- Sie haben bisher höchstens einmal die Prüfung zur Einführung in die Kryptographie mitgeschrieben.

Unterschrift:

VIEL ERFOLG!

Hausübung

Aufgabe	1	2
Maximale Punktzahl	5	5
Erreichte Punktzahl		

Klausur

Aufgabe	1	2	3	4	5	Σ
Maximale Punktzahl	15	18	15	20	22	100
Erreichte Punktzahl						

Hinweise:

Aufgabenblätter

- Füllen Sie das Deckblatt vollständig aus.
- Prüfen Sie, ob die Klausur **5 Aufgaben** und **6 Seiten** (Deck- und Hinweisblatt und 5 Aufgabenblätter) enthält.
- Kennzeichnen Sie alle verwendeten Blätter zuerst mit Name und Matrikelnummer.
- Verwenden Sie für jede Aufgabe ein neues Blatt.
- Geben Sie die verwendeten Formeln, Sachverhalte und Zwischenergebnisse an.

Bewertung

- Ein nicht vorhandener Lösungsweg führt zu Punktabzug.
- Unleserlichkeit führt zu Punktabzug.
- Sie konnten in der Hausübung 10 Punkte erzielen.
- In der Klausur gibt es 90 Punkte.
- Die Gesamtnote ergibt sich aus der Summe der in der Klausur und Hausübung erzielten Punkte.
- Das Ergebnis der Hausübung bildet keine Zulassungsvoraussetzung zur Klausur.

Dauer der Klausur und zugelassene Hilfsmittel

- Ihnen stehen **100 Minuten** zum Bearbeiten der Aufgaben zur Verfügung.
- Einzige zugelassene Hilfsmittel sind **ein** nicht programmierbarer Taschenrechner ohne Formelspeicher und ein beidseitig handschriftlich beschriebenes DIN-A4 Blatt. Tragen Sie die genaue 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 Wörterbuch verwenden.
- Die Klausuraufsicht überprüft die Hilfsmittel.

Prüfungstyp

- Diese Klausur ist Teil der vorlesungsbegleitenden Prüfung zur „Einführung in die Kryptographie“, die aus den Teilprüfungen Hausübung und Klausur besteht.
- Sie sind in einem Diplomstudiengang und haben sich in keinem Prüfungssekretariat zur Prüfung angemeldet \implies Dies ist eine vorlesungsbegleitende Prüfung für Sie, die Sie in einer Diplomprüfung einbringen können.
- Sie sind in einem Diplomstudiengang, haben das Vordiplom abgeschlossen und haben sich in dem zuständigen Prüfungssekretariat zur Prüfung angemeldet \implies Diese vorlesungsbegleitende Prüfung ist eine Diplomprüfung für Sie.
- Sie sind in einem Ba/Ma-Studiengang und haben sich in dem zuständigen Prüfungssekretariat angemeldet \implies Dies ist eine Fachprüfung für Sie.
- Sie sind in einem Ba/Ma-Studiengang und haben sich in Ihrem zuständigen Prüfungssekretariat nicht zur Prüfung angemeldet \implies STOP: Sie dürfen an dieser Prüfung nicht teilnehmen!

Name: Matrikelnummer:

Aufgabe 1 (RSA – 15 Punkte)

Ihr öffentlicher RSA-Schlüssel ist $(n, e) = (44969, 31351)$. Ihr privater RSA-Schlüssel ist $d = 4423$. Der öffentliche RSA-Modulus n wurde von Ihnen als das Produkt von $p = 193$ und $q = 233$ berechnet. Ihnen wurde der Schlüsseltext $c = 9488$ gesendet. Berechnen Sie den zugehörigen Klartext mit CRT und schneller Exponentiation.

Name: Matrikelnummer:

Aufgabe 2 (Diskrete Logarithmen – 18 Punkte)

Sie wollen den diskreten Logarithmus von 55 zur Basis 5 in \mathbb{Z}_{157}^\times berechnen.

Hinweis: 157 ist prim.

- (a) Bei der Berechnung des diskreten Logarithmus mit dem speicherplatzeffizienten Pollard-Rho-Algorithmus aus der Vorlesung entsteht die Folge $\beta_1, \beta_2, \dots \in \mathbb{Z}_{157}^\times$. Die erste Kollision ist $\beta_5 = \beta_{14}$. Welche Kollision entdeckt der Pollard-Rho-Algorithmus?

Hinweis: Ihnen sind die Initialisierungswerte des Pollard-Rho-Algorithmus, insbesondere x_0 unbekannt.

- (b) Die von Ihnen mit dem Pollard-Rho-Algorithmus ermittelte Kollision ergibt folgendes:

$$5^4 55^{64} \equiv 5^{28} 55^4 \pmod{157}$$

Bestimmen Sie mit dieser Erkenntnis den diskreten Logarithmus von 55 zur Basis 5 in \mathbb{Z}_{157}^\times .

- (c) Hätten Sie den Babystep-Giantstep-Algorithmus verwendet, welcher Babystep wäre mit welchem Giantstep zusammengefallen?

Name: Matrikelnummer:

Aufgabe 3 (DSA – 15 Punkte)

Wir betrachten DSA in der Untergruppe der Ordnung 17 von \mathbb{Z}_{103}^\times . Alice will für sich ein Schlüssel-paar erzeugen, wobei Ihr zufällig gewählter geheimer Exponent $a = 7$ sein soll. Um ein Element g zu konstruieren, das die Untergruppe der Ordnung 17 erzeugt, wählt sie eine Primitivwurzel $x \in \mathbb{Z}_{103}^\times$ nach den folgenden Kriterien: $x \in \{1, \dots, 102\}$ soll ungerade und möglichst klein sein. Danach bestimmt sie $g = x^i \pmod{103}$, wobei $i \in \mathbb{N}$ möglichst klein sein soll.

- (a) Zeigen Sie zunächst, daß Alice $g = 72$ erhält. Geben Sie dann den öffentlichen Schlüssel von Alice an.
- (b) Alice signiert das Dokument m . Der Hashwert von m ist $h(m) = 15$. Sie wählt als zufälligen Parameter $k = 5$. Berechnen Sie die Signatur.
- (c) Sie haben eine Signatur zum Dokument m vorliegen: $(r, s) = (15, 5)$. Der Hashwert von m ist $h(m) = 15$. Können Sie die Signatur als Alices verifizieren?

Name: Matrikelnummer:

Aufgabe 4 (Quadratisches Sieb – 20 Punkte)

Faktorisieren Sie $n = 10123$ mit dem Quadratischen Sieb, indem Sie die Aufgabenteile (a) – (c) bearbeiten.

(a) Finden Sie die Nullstellen des Polynoms

$$f(x) = (x + m)^2 - n$$

zu allen Moduli aus der Faktorbasis $F(7) = \{2, 3, 5, 7\}$, wobei $m = \lfloor \sqrt{n} \rfloor$.

(b) Wieviele Zahlen x gibt es im Intervall $[0, 83]$, für die $f(x)$ durch 2, 3 und 7 teilbar ist?

(c) Wir bezeichnen mit „Rest(x)“ die natürliche Zahl $k = f(x) / (2^{e_2} \cdot 3^{e_3} \cdot 5^{e_5} \cdot 7^{e_7})$, so daß e_i für $i = 2, 3, 5, 7$ maximal ist. Vervollständigen Sie die unten stehende Tabelle und faktorisieren Sie dann n mit dem Quadratischen Sieb.

x	1	3	5	7	9	11	13	15
$2 f(x)$								
$3 f(x)$		ja					ja	
$5 f(x)$								
$7 f(x)$						ja		
Rest(x)	13	1	451	221		157		

Aufgabe 5 (Endliche Körper – 22 Punkte)

Wir betrachten den endlichen Körper

$$\mathbb{F}_{2^m} = \mathbb{F}_2[X]/p(X)\mathbb{F}_2[X],$$

wobei $p(X)$ ein irreduzibles Polynom vom Grad m ist. Wir betrachten die folgende Abbildungen für $b \in \mathbb{F}_{2^m}$:

$$\pi : \mathbb{F}_2^m \rightarrow \mathbb{F}_{2^m}, \quad (a_{m-1}, a_{m-2}, \dots, a_0) \mapsto \sum_{i=0}^{m-1} a_i X^i \quad \text{und} \quad \phi_b : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m, \quad a \mapsto \pi^{-1}(b \cdot \pi(a))$$

(a) Für alle $b \in \mathbb{F}_{2^m}$ läßt sich die Abbildung ϕ_b mit einer Matrix $G_b \in \mathbb{F}_2^{m \times m}$ wie folgt beschreiben:

$$\phi_b : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m, \quad a \mapsto aG_b.$$

Beweisen Sie diese Aussage. Hinweis: Sie müssen dazu G_b nicht explizit angeben.

(b) Sei g ein Erzeuger von $\mathbb{F}_{2^m}^\times$ und G_g die Matrix, die die Abbildung ϕ_g beschreibt. Zeigen Sie, daß die Abbildung

$$\psi : \mathbb{F}_{2^m}^\times \rightarrow \mathcal{G} = \langle G_g \rangle, \quad g^i \mapsto G_g^i$$

ein Isomorphismus von Gruppen ist, d.h. die Abbildung ψ ist multiplikativ, bijektiv und das Bild der 1 ist die Einheitsmatrix.

(c) Verwenden Sie die von Ihnen im vorigen Aufgabenteil gezeigte Aussage, um die Ordnung von \mathcal{G} zu bestimmen und zu zeigen, daß das Problem, diskrete Logarithmen zu bestimmen, in \mathcal{G} und $\mathbb{F}_{2^m}^\times$ gleich schwer ist. D.h. das Problem, diskrete Logarithmen in \mathcal{G} zu berechnen, kann auf das Problem, diskrete Logarithmen in $\mathbb{F}_{2^m}^\times$ zu berechnen, reduziert werden und umgekehrt.

(d) Formulieren Sie die ElGamal-Verschlüsselung für die Gruppe \mathcal{G} .

(e) Zeigen Sie, daß für $m = 5$, $p(X) = X^5 + X^4 + X^3 + X + 1$ und $\pi^{-1}(g) = (0, 0, 0, 1, 0)$ das Polynom g ein Erzeuger von $\mathbb{F}_{2^m}^\times$ ist. Geben Sie die Matrix G_g an:

$$G_g = \begin{pmatrix} | & | & | & | & | \\ \hline | & | & | & | & | \\ \hline | & | & | & | & | \\ \hline | & | & | & | & | \\ \hline | & | & | & | & | \end{pmatrix}$$

Name: Matrikelnummer:

Name: Matrikelnummer:

Name: Matrikelnummer: