

Klausur „Kryptographie“ Juli 2006

Name:
Vorname:
Matrikel-Nr.:
Studienfach:

Wichtige Hinweise:

1. Prüfen Sie Ihr Klausurexemplar auf Vollständigkeit (ein Deckblatt und Aufgabenblätter mit den Seitennummern 2–13).
2. Die Klausur dauert 100 Minuten.
3. Alle Aufgaben sind auf dem jeweils zugehörigen Aufgabenblatt zu bearbeiten.

	Punkte	erreicht
Aufgabe 1	16	
Aufgabe 2	16	
Aufgabe 3	16	
Aufgabe 4	16	
Aufgabe 5	16	
Aufgabe 6	20	
Gesamt	100	

4. **Vermerken Sie Ihren Namen und Ihre Matrikelnummer auf jedem Aufgabenblatt!**
5. Die Klausur ist komplett (mit Deckblatt und allen Aufgabenblättern) abzugeben.
6. Die Fragen sollen knapp und präzise in Stichpunkten beantwortet werden. Alle in Formeln vorkommenden Bezeichner müssen erklärt werden – soweit die Aufgabenstellung nicht ausdrücklich etwas anderes aussagt.
7. Formale mathematische Beweise werden nicht verlangt.
8. **Unterschreiben Sie die letzte Seite der Klausur!**

Klausur „Kryptographie“ Juli 2006

Name: Matrikelnummer:

Aufgabe 1 (Informationstheorie)

(16 Punkte)

- (a) Man gebe die Formel für die Entropie an.
(Bitte alle vorkommenden Bezeichner erklären!)
- (b) Grob vereinfacht kann man das Verfahren, mit dem typische Benutzer ihr Passwort wählen, wie folgt beschreiben:
- Wähle zufällig $i \in \{1, \dots, 4\}$.
 - Wähle das Passwort zufällig aus einem Wörterbuch D_i .

Wörterbuch D_i enthalte $2^{20 * i}$ Passwörter. Die Wörterbücher sind disjunkt, d.h., es gibt kein Wort, das in mehr als einem Wörterbuch enthalten ist.

Wie groß ist die Entropie dieser Passwortquelle?

Klausur „Kryptographie“ Juli 2006

Name: Matrikelnummer:

Zusätzlicher Platz zur Bearbeitung von **Aufgabe 1**.

Klausur „Kryptographie“ Juli 2006

Name: Matrikelnummer:

Aufgabe 2 (Flusschiffren)

(16 Punkte)

- (a) Wie groß kann die Periode eines LFSR der Größe n höchstens sein?
(Kurze Begründung!)
- (b) Man gebe ein LFSR der Größe 2 an, das maximale Periode hat.
(Beschreibung oder Skizze!)
- (c) Welche der folgenden Bit-Sequenzen können von LFSR der Größe 3 erzeugt worden sein? (Das zuerst ausgegebene Bit steht ganz links, das letzte ganz rechts. Man beachte, dass die jeweiligen Feedback-Polynome unbekannt sind bzw. passend gewählt werden können.)

- 1. 001001
- 2. 011001
- 3. 000111

Man beschreibe ein LFSR und die zugehörige Startbelegung, um die jeweilige Bit-Sequenz zu erzeugen.

Oder, man begründe warum kein LFSR der Größe 3 diese Sequenz erzeugen kann.

Klausur „Kryptographie“ Juli 2006

Name: Matrikelnummer:

Zusätzlicher Platz zur Bearbeitung von **Aufgabe 2**.

Name: Matrikelnummer:

Aufgabe 3 (Blockchiffren)

(16 Punkte)

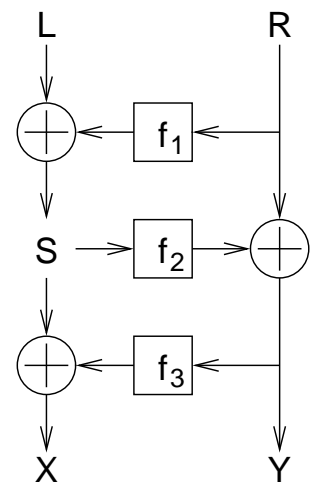
- (a) Was ist ein Chosen-Plaintext Angriff auf eine Blockchiffre?
(Kurze Beschreibung!)

Rechts abgebildet ist eine **3-Runden Feistelchiffre**, d.h. eine Permutation $P : \{0, 1\}^{2n} \rightarrow \{0, 1\}^{2n}$. $(X, Y) = P(L, R)$ ist definiert durch

$$S := L \oplus f_1(R), Y := R \oplus f_2(S) \text{ und } X := S \oplus f_3(Y).$$

Das Ziel eines Angreifers besteht stets darin, P von einer Zufallspermutation zu unterscheiden. Wir setzen zunächst voraus, dass f_1, f_2 und f_3 unabhängige zufällige Funktionen $\{0, 1\}^n \rightarrow \{0, 1\}^n$ sind. Aus der Vorlesung ist bekannt, dass in diesem Fall keine effizienten Chosen Plaintext Unterscheidungsangriffe möglich sind.

Wir betrachten modifizierte Angriffsszenarien, in denen derartige Angriffe doch möglich sind.



- (b) Angenommen, der Angreifer kennt zu zwei Werten $R_1 \neq R_2$ die Funktionswerte $f_1(R_1)$ und $f_1(R_2)$.
- (c) Angenommen, f_1 und f_3 sind unabhängige Zufallspermutationen, aber für f_2 gilt schlicht und einfach $f_2(S) = S$.

In beiden Fällen gebe man jeweils einen **Chosen Plaintext Unterscheidungsangriff** an, der mit zwei gewählten Klartexten (also zwei Paaren (L, R) und (L', R')) auskommt und mit großem Vorteil zwischen P und einer Zufallspermutation unterscheidet.

Klausur „Kryptographie“ Juli 2006

Name: Matrikelnummer:

Zusätzlicher Platz zur Bearbeitung von **Aufgabe 3**.

Klausur „Kryptographie“ Juli 2006

Name: Matrikelnummer:

Aufgabe 4 (Konkrete Blockchiffren)

(16 Punkte)

- (a) Eine der vier internen Grundoperationen des AES ist die Shift-Row Operation. Was leistet die Shift-Row Operation?
- (b) Man stelle sich eine Variante des AES vor, bei der die Shift-Row Operation nicht durchgeführt wird. Die anderen Operationen und ihre Reihenfolge sind unverändert. Ein Angreifer soll die Variante von einer korrekten Implementation unterscheiden. Er hat Zugriff auf die Blockchiffre unter einem ihm unbekanntem Schlüssel.

Der Angreifer stellt zwei Chosen Plaintext Orakelfragen, deren Klartexte sich nur an drei Bytes unterscheiden – siehe die Abbildung unten. Man gebe ein Kriterium an, um Chiffretexte der Variante von Chiffretexten des echten AES mit großem Vorteil zu unterscheiden!

1	1	1	1	1	1	1	1
1	1	1	1	1	2	1	4
1	1	1	1	1	1	1	1
1	1	1	1	1	8	1	1

Klausur „Kryptographie“ Juli 2006

Name: Matrikelnummer:

Zusätzlicher Platz zur Bearbeitung von **Aufgabe 4**.

Klausur „Kryptographie“ Juli 2006

Name: Matrikelnummer:

Aufgabe 5 (Public-Key Kryptographie mit KLEINEN Zahlen) (16 Punkte)

- (a) Wie wird beim RSA Kryptosystem der Schlüssel erzeugt? Welcher Teil des Schlüssels ist öffentlich, welcher Teil ist geheim?
(Die Bezeichner n , e , d , p , q und $\varphi(n)$ können ohne zusätzliche Erklärungen wie in der Vorlesung benutzt werden.)

Sei nun ein RSA-Modulus $n = 91$ gegeben. Aus irgendwelchen Quellen haben wir erfahren, dass $\varphi(n) = 72$ gilt.

- (b) Man faktorisiere n . Dabei ist auch der Rechenweg anzugeben.
Die Beschreibung des Rechenweges soll erkennen lassen, wie man *große* RSA-Moduli n effizient faktorisieren kann, wenn man $\varphi(n)$ kennt.
- (c) Welche der Zahlen aus $\{2, \dots, 12\}$ sind ein geeigneter öffentlicher Exponent e ?

Klausur „Kryptographie“ Juli 2006

Name: Matrikelnummer:

Zusätzlicher Platz zur Bearbeitung von **Aufgabe 5**.

Klausur „Kryptographie“ Juli 2006

Name: Matrikelnummer:

Aufgabe 6 (Public-Key Kryptographie) (20 Punkte)

Zum Schutz vor Rate-Verifikationsangriffen hat sich jemand ein *randomisiertes RSA-Schema* ausgedacht. Bei der Schlüsselerzeugung werden ein Modulus n und zwei verschiedenen öffentlichen Exponenten e_1 und e_2 generiert, und natürlich zwei geheime Exponenten d_1 und d_2 mit $e_1 * d_1 \equiv 1 \pmod{\varphi(n)}$ und $e_2 * d_2 \equiv 1 \pmod{\varphi(n)}$. Die Verschlüsselung eines Klartextes $M \in \mathbb{Z}_n^*$ erfolgt so:

- Wähle zufällig $r \in \mathbb{Z}_n^*$.
 - Berechne $b = r^{e_1} \pmod{n}$ und $c = r^{e_2} * M \pmod{n}$.
 - Chiffretext: $(b, c) \in \mathbb{Z}_n^* \times \mathbb{Z}_n^*$.
- (a) Der Empfänger eines Chiffrextes (b, c) kennt d_1 und d_2 – und natürlich den öffentlichen Schlüssel (n, e_1, e_2) . Wie kann er (b, c) **entschlüsseln**?
- (b) Dieses Schema ist unsicher! Man gebe einen **Chosen Plaintext Angriff** an, der mit Vorteil ≈ 1 entscheiden kann, ob ein Chiffretext (b, c) die Verschlüsselung eines zufälligen Klartextes aus \mathbb{Z}_n^* darstellt, oder die Verschlüsselung eines vom Angreifer gewählten Klartextes $M \in \mathbb{Z}_n^*$. Der Angreifer kennt d_1 und d_2 *nicht*, und er kann *keine* RSA-Wurzeln mod n berechnen.

Zur Klarstellung: Weder der Empfänger noch der Angreifer kennen den Zufallswert r – auch wenn sie ihn *vielleicht* berechnen können.

Klausur „Kryptographie“ Juli 2006

Name: Matrikelnummer:

Zusätzlicher Platz zur Bearbeitung von **Aufgabe 6**.