



11. Juli 2001

Lösungsvorschlag zur Semestralklausur zu
Einführung in die Kryptographie
SS 2001

Name, Vorname:

Fachbereich: Matrikelnummer: Fachsemester:

Aufbaustudium: Wiederholer(in):

Unterschrift:

Hinweise:

1. Prüfen Sie, ob die Klausur alle 10 Aufgaben enthält.
2. Füllen Sie das Deckblatt vollständig aus.
3. Halten Sie ihren Studenausweis und einen Lichtbildausweis bereit.
4. Kennzeichnen Sie alle verwendeten Blätter zuerst mit Name und Matrikelnr.
5. Es sind die verwendeten Formeln und die Zwischenergebnisse anzugeben.
6. Markieren Sie auf dem Deckblatt die bearbeiteten Aufgaben.
7. Zum Bestehen der Prüfung ist es hinreichend 50 Punkte zu erreichen.
8. Ihnen stehen 90 min zum Bearbeiten der Aufgaben zur Verfügung.
9. Zugelassene Hilfsmittel sind ein DIN A4 Blatt (beidseitig) handgeschriebene Formelsammlung und ein nicht programmierbarer Taschenrechner.

Aufgabe	1	2	3	4	5	6	7	8	9	10
Punkte maximal	10	10	10	10	10	10	10	10	10	10
bearbeitet										
Punkte erreicht										

1. Aufgabe: Erweiterter Euklidischer Algorithmus (10 Punkte)

- (a) Berechnen Sie $\gcd(235, 147)$ samt seiner Darstellung der Form $x * 235 + y * 147$ mit dem erweiterten Euklidischen Algorithmus. (7 Punkte)
- (b) Wie lautet das multiplikative Inverse von 147 modulo 235? (3 Punkte)

-
- (a) Wir wenden den erweiterten euklidischen Algorithmus an und erhalten folgende Tabelle:

k	0	1	2	3	4	5
r_k	235	147	88	59	29	1
q_k		1	1	1	2	29
x_k	1	0	1	1	2	5
y_k	0	1	1	2	3	8

Damit gilt: $\gcd(235, 147) = -5 * 235 + 8 * 147 = 1$.

- (b) An der gefunden Darstellung sieht man: $147^{-1} \equiv 8 \pmod{235}$.

2. Aufgabe: Blockchiffren (10 Punkte)

Zeigen Sie, daß alle Verschlüsselungsfunktionen von Blockchiffren der Blocklänge 2 mit Alphabet \mathbb{Z}_2 affin linear sind.

Hinweis: Vergleichen Sie die Anzahl aller möglichen Permutationen mit der Anzahl der affin linearen Verschlüsselungsfunktionen.

Wir zählen zunächst alle Permutationen $\mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^2$. Davon existieren offensichtlich $4! = 24$ verschiedene. Nun betrachten wir die affin linearen Verschlüsselungsfunktionen $Ax + b$. Es existieren die 6 folgenden nicht singulären 2×2 Matrizen über \mathbb{Z}_2 :

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

Für den Vektor b ergeben sich die folgenden 4 Möglichkeiten:

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

Dies ergibt $6 * 4 = 24$ Kombinationen. Bleibt zu zeigen, daß diese tatsächlich verschieden sind. Sei also $Ax + b = A'x + b'$. Betrachte $x = 0$. Dann folgt sofort $b = b'$. Bleibt zu betrachten $Ax = A'x$. Betrachte nun die Fälle

$$x = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ und } x = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Damit folgt $A = A'$. Insgesamt folgt also, daß die Anzahl der Permutationen gleich der Anzahl der affin linearen Funktionen ist, und die Permutationen deshalb affin linear sind.

3. Aufgabe: Kryptoanalyse affin linearer Chiffren (10 Punkte)

Bei einer Kommunikation haben Sie die folgenden Chiffretextblöcke mitgelesen: “QK”, “X!”, und “MY”. Sie haben herausgefunden, daß die zugehörigen Klartextblöcke “AT”, “HE”, und “NE” lauten. Sie gehen davon aus, daß diese Verschlüsselung durch einfache wiederholte Anwendung (ECB Mode) einer affin linearen Chiffre der Blocklänge 2 stattgefunden hat. Ausserdem wissen Sie, daß das zugrundeliegende Alphabet die Menge $\{A - Z, ., !, ?\}$ ist, wobei die Zuordnung von Buchstaben und Zahlen anhand der angegebenen Tabelle erfolgt. Bestimmen Sie die Verschlüsselungsfunktion mittels der in der Vorlesung vorgestellten Known-Plaintext-Attacke auf affin lineare Chiffren.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
P	Q	R	S	T	U	V	W	X	Y	Z	.	!	?	
15	16	17	18	19	20	21	22	23	24	25	26	27	28	

w_0		w_1		w_2	
A	T	H	E	N	E
0	19	7	4	13	4
c_0		c_1		c_2	
Q	K	X	!	M	Y
16	10	23	27	12	24

Das Alphabet hat 29 Elemente. Also rechnen wir modulo 29. Da die Blocklänge 2 ist, werden 2×2 Matrizen verwendet.

$$W \equiv (w_1 - w_0, \dots, w_n - w_0) \equiv \begin{pmatrix} 7 & 13 \\ 14 & 14 \end{pmatrix} \pmod{29}$$

$$\text{adj}(W) \equiv \begin{pmatrix} 14 & 16 \\ 15 & 7 \end{pmatrix} \pmod{29}$$

$$\det(W) \equiv 3 \pmod{29}$$

$$\det(W)^{-1} \equiv 10 \pmod{29}$$

$$W^{-1} \equiv \det(W)^{-1} * \text{adj}(W) \equiv \begin{pmatrix} 24 & 15 \\ 5 & 12 \end{pmatrix} \pmod{29}$$

$$C \equiv (c_1 - c_0, \dots, c_n - c_0) \equiv \begin{pmatrix} 7 & 25 \\ 17 & 14 \end{pmatrix} \pmod{29}$$

$$A \equiv C \cdot W^{-1} \equiv \begin{pmatrix} 3 & 28 \\ 14 & 17 \end{pmatrix} \pmod{29}$$

$$b \equiv c_0 - Aw_0 \equiv \begin{pmatrix} 6 \\ 6 \end{pmatrix}$$

Die Verschlüsselungsfunktion ist also

$$\begin{pmatrix} 3 & 28 \\ 14 & 17 \end{pmatrix} x + \begin{pmatrix} 6 \\ 6 \end{pmatrix} \pmod{29}.$$

4. Aufgabe: Gruppen und Ordnungen (10 Punkte)

- (a) Bestimmen Sie die Elemente von $(\mathbb{Z}/10\mathbb{Z})^*$. (2 Punkte)
- (b) Bestimmen Sie die Ordnung von $(\mathbb{Z}/10\mathbb{Z})^*$. (1 Punkt)
- (c) Berechnen Sie die von $(3 + 10\mathbb{Z})$ in $(\mathbb{Z}/10\mathbb{Z})^*$ erzeugte Untergruppe $\langle 3 + 10\mathbb{Z} \rangle$. (3 Punkte)
- (d) Bestimmen Sie die Ordnung von $\langle 3 + 10\mathbb{Z} \rangle$. (1 Punkt)
- (e) Bestimmen Sie die Ordnung aller in $\langle 3 + 10\mathbb{Z} \rangle$ enthaltenen Elemente. (3 Punkte)

-
- (a) $(\mathbb{Z}/10\mathbb{Z})^* = \{(1 + 10\mathbb{Z}), (3 + 10\mathbb{Z}), (7 + 10\mathbb{Z}), (9 + 10\mathbb{Z})\}$
 - (b) $order((\mathbb{Z}/10\mathbb{Z})^*) = 4$
 - (c) $\langle 3 + 10\mathbb{Z} \rangle = \{(1 + 10\mathbb{Z}), (3 + 10\mathbb{Z}), (7 + 10\mathbb{Z}), (9 + 10\mathbb{Z})\}$
 - (d) $order(\langle 3 + 10\mathbb{Z} \rangle) = 4$
 - (e) $order((1 + 10\mathbb{Z})) = 1$
 $order((3 + 10\mathbb{Z})) = 4$
 $order((7 + 10\mathbb{Z})) = 4$
 $order((9 + 10\mathbb{Z})) = 2$

5. Aufgabe: Schnelle Exponentiation (10 Punkte)

Berechnen Sie mit Hilfe der schnellen Exponentiation $6^{(7^8)} \pmod{53}$.

$gcd(53, 6) = 1$ also kann der Exponent modulo $\varphi(53) = 52$ reduziert werden.

$$7^2 \equiv 49 \pmod{52}$$

$$7^4 \equiv 9 \pmod{52}$$

$$7^8 \equiv 29 \pmod{52}$$

$$6^2 \equiv 36 \pmod{53}$$

$$6^4 \equiv 24 \pmod{53}$$

$$6^8 \equiv 46 \pmod{53}$$

$$6^{16} \equiv 49 \pmod{53}$$

$$6^{29} \equiv 6^{16} * 6^8 * 6^4 * 6 \equiv 4 \pmod{53}$$

6. Aufgabe: RSA-Verschlüsselung (10 Punkte)

- (a) Bestimmen Sie alle RSA-Moduln n mit $\varphi(n) = 24$. Bestimmen Sie auch die entsprechenden Primfaktoren. (6 Punkte)
- (b) Bestimmen Sie für alle RSA-Moduln aus (a) und für den öffentlichen RSA-Exponenten $e = 5$ den Klartext m zum Chiffretext $c = 3$. (4 Punkte)

-
- (a) Die Zerlegungen von 24 sind $24 = 1 * 24 = 2 * 12 = 3 * 8 = 4 * 6$. Wenn also $\varphi(n) = (p - 1) * (q - 1) = 24$ gelten soll, dann kann nur

$$p = 3, q = 13, n = 39$$

oder

$$p = 5, q = 7, n = 35$$

sein.

- (b) Mit $5 * 5 \equiv 25 \equiv 1 \pmod{24}$ folgt $d = 5$, also:

$$m \equiv 3^5 \equiv 33 \pmod{35}$$
$$m \equiv 3^5 \equiv 9 \pmod{39}$$

7. Aufgabe: Chinesischer Restsatz (10 Punkte)

Bestimmen Sie die kleinste nicht negative Lösung der gegebenen simultanen Kongruenz mit dem chinesischen Restsatz.

$$x \equiv 6 \pmod{8}$$
$$x \equiv 10 \pmod{15}$$
$$x \equiv 8 \pmod{17}.$$

$$a_1 = 6, m_1 = 8, M_1 = 255$$
$$a_2 = 10, m_2 = 15, M_2 = 136$$
$$a_3 = 8, m_3 = 17, M_3 = 120$$

$$M = 2040$$

$$y_1 * 255 \equiv 1 \pmod{8}$$
$$y_1 * 7 \equiv 1 \pmod{8}$$
$$y_1 \equiv 7 \pmod{8}$$

$$y_2 * 136 \equiv 1 \pmod{15}$$
$$y_2 * 1 \equiv 1 \pmod{15}$$
$$y_2 \equiv 1 \pmod{15}$$

$$y_3 * 120 \equiv 1 \pmod{17}$$
$$y_3 * 1 \equiv 1 \pmod{17}$$

$$y_3 \equiv 1 \pmod{17}$$

$$x \equiv 510 + 1360 + 960 \equiv 790 \pmod{2040}$$

8. Aufgabe: ElGamal Signatur (10 Punkte)

Alice wählt den Modul $p = 31$, die Basis $g = 7$ und den geheimen Exponenten $a = 3$.

- (a) Bestimmen Sie den öffentlichen Schlüssel von Alice. (2 Punkte)
- (b) Bestimmen Sie die Signatur zum Hashwert $h(m) = 12$ mit $k = 11$. (5 Punkte)
- (c) Verifizieren Sie die in (b) erzeugte Signatur. (3 Punkte)

(a) $A \equiv g^a \pmod{p}$
 $A \equiv 7^3 \equiv 2 \pmod{31}$
 $(p, g, A) = (31, 7, 2)$

(b) $r \equiv g^k \pmod{p}$
 $r \equiv 7^{11} \equiv 20 \pmod{31}$

$$k^{-1} * k \equiv 1 \pmod{p-1}$$
$$k^{-1} * 11 \equiv 1 \pmod{30}$$
$$k^{-1} \equiv 11 \pmod{30}$$

$$s \equiv k^{-1}(h(x) - ar) \pmod{p-1}$$
$$s \equiv 11(12 - 3 * 20) \equiv 12 \pmod{30}$$

$$(r, s) = (20, 12)$$

(c) $1 \leq r \leq (p-1)$
 $1 \leq 20 \leq 30$

$$A^r * r^s \equiv g^{h(x)} \pmod{p}$$
$$2^{20} * 20^{12} \equiv 7^{12} \pmod{31}$$
$$16 \equiv 16 \pmod{31}$$

9. Aufgabe: Babystep-Giantstep Algorithmus (10 Punkte)

Lösen Sie $15^x \equiv 4 \pmod{13}$ mit dem Babystep-Giantstep Algorithmus.

$$15^x \equiv 2^x \equiv 4 \pmod{13}$$
$$m = \lceil \sqrt{\varphi(13)} \rceil = \lceil \sqrt{12} \rceil = 4$$

r	$\gamma^{-r} * \alpha \pmod p$
0	$2^{-0} * 4 \equiv 4 \pmod{13}$
1	$2^{-1} * 4 \equiv 7 * 4 \equiv 2 \pmod{13}$
2	$2^{-2} * 4 \equiv (7 * 7) * 4 \equiv 1 \pmod{13}$

Da der Babystep zu $r = 2$ gleich 1 ist, gilt $x = 2$.

10. Aufgabe: Zero-Knowledge-Beweis (10 Punkte)

Sei p eine Primzahl, g eine Primitivwurzel $\pmod p$ und $A \in \{1, \dots, p-1\}$. Alice kann Bob mit folgendem Zero-Knowledge-Beweis davon überzeugen, daß sie den diskreten Logarithmus a von $A \pmod p$ zur Basis g kennt. Ergänzen Sie das Protokoll.

