



## Lösungsvorschlag für die Klausur zur „Einführung in die Kryptographie“ im WS 05/06

### Aufgabe 1 (RSA)

Wir entschlüsseln mit *CRT* und berechnen zunächst

$$\begin{aligned}c_p &:= c \pmod p &= 31, \\d_p &:= d \pmod{p-1} &= 7, \\c_q &:= c \pmod q &= 168 \text{ und} \\d_q &:= d \pmod{q-1} &= 15.\end{aligned}$$

Es ergibt sich

$$\begin{aligned}m_p &= c_p^{d_p} \pmod p &= 31^{2^2} \cdot 31^2 \cdot 31 &= 139 \text{ und} \\m_q &= c_q^{d_q} \pmod q &= 168^{2^3} \cdot 168^{2^2} \cdot 168^2 \cdot 168 &= 59.\end{aligned}$$

Da  $p \cdot 99 - 82 \cdot q = 193 \cdot 99 - 82 \cdot 233 = 1$ , berechnet sich der Klartext als

$$m = m_q * 99 * p + m_p * 111 * q \pmod n = 525.$$

### Aufgabe 2 (Diskrete Logarithmen)

- (a) Der Pollard-Rho-Algorithmus ist so konstruiert, daß wenn man eine Kollision vom  $i$ -ten Schritt mit dem  $j$ -ten Schritt hat, dann auch eine vom  $i + 1$ -ten und  $j + 1$ -ten Schritt hat. Bei der Speicherplatzeffizienten Variante wird bis zum  $2^{i+1}$ -ten Schritt der  $2^i$ -te gespeichert. Wir erhalten somit eine Kollision vom 16-ten und 16 + 9-ten Schritt, da  $14 - 5 = 9$ .

- (b) Wir erhalten die Kongruenz

$$28 - 4 \equiv (64 - 4)x \pmod{156}$$

für den diskreten Logarithmus  $x$  von 55 zur Basis 5. Daraus ergibt sich, wenn man die gesamte Gleichung durch 12 teilt:

$$5x \equiv 2 \pmod{13} \iff x \equiv 3 \pmod{13}.$$

Jetzt bleibt uns nichts weiter übrig, als den diskreten Logarithmus als einen der Werte  $x = 3 + k13$  mit  $k \in \mathbb{N}$  zu bestimmen. Dazu berechnen wir erst

$$\begin{aligned}5^3 &\equiv 125 \pmod{157} \\5^{13} &\equiv 22 \pmod{157}.\end{aligned}$$

Es gilt mit  $x = 3 + 2 \cdot 13 = 29$ :  $5^x \equiv 55 \pmod{157}$  ( $X^{16} \equiv 81 \pmod{157}$ ).

- (c) Beim Babystep-Giantstep-Algorithmus wird zunächst  $m = \lceil \sqrt{156} \rceil = 13$  und dann  $55 \cdot 5^{-r} \pmod{157}$  für  $r = 1, 2, \dots, m$  berechnet (Babysteps). Dann werden die Giantsteps als  $5^{mi}$  für  $i = 1, \dots, m - 1$  berechnet. Es wird daher eine Korrespondenz zwischen dem

3-ten Babystep und dem 2-ten Giantstep

gefunden. Das 3-te Element der Babystepmenge ist (13, 3), da  $55 \cdot 125^{-1} \equiv 13 \pmod{157}$ .

### Aufgabe 3 (DSA)

(a) Wir stellen zunächst fest:

$$\begin{aligned} 3^{(2*17)} &\equiv 1 \pmod{103}, \\ 5^{(2*17)} &\equiv 56 \not\equiv 1 \pmod{103}, \\ 5^{(3*17)} &\equiv 102 \not\equiv 1 \pmod{103}, \\ 5^{(2*3)} &\equiv 72 \not\equiv 1 \pmod{103} \end{aligned}$$

und wählen daher  $g = 5^6 \pmod{p}$  als Generator der Untergruppe, in der Alice DSA verwenden will. Der öffentliche Schlüssel von Alice lautet:

$$(p, q, g, A) = (103, 17, 72, 66).$$

(b) Sei  $k = 5$  unser zufällig gewählter Exponent. Dann ist

$$g^k \equiv 8 \pmod{p} \quad \text{und} \quad r = (g^k \pmod{p}) \pmod{q} = 8$$

der erste Teil der Signatur. Der zweite berechnet sich mit  $k^{-1} \equiv 7 \pmod{q}$  zu

$$s \equiv k^{-1}(h(m) + ar) \equiv 4 \pmod{q}.$$

(c) Es gilt  $1 \leq r \leq p - 1$ . Wir verifizieren die Signatur mit  $s^{-1} \equiv 7 \pmod{q}$ .

$$\begin{aligned} s^{-1}h(m) &\equiv 3 \pmod{q} \quad \text{und} \quad rs^{-1} \equiv 3 \pmod{q} \\ g^{s^{-1}h(m)} A^{rs^{-1}} &\equiv 66 \pmod{p} \\ 66 &\equiv 15 \equiv r \pmod{q}. \end{aligned}$$

Die Signatur ist also gültig.

#### Aufgabe 4 (Quadratisches Sieb)

(a) Es gilt:  $m = 100$ . Wir erhalten die Nullstellen durch quadratische Ergänzung

$$\begin{aligned}
 (x+m)^2 - n &\equiv x^2 + 1 \pmod{2} &\Rightarrow x &\equiv 1 \pmod{2}, \\
 &\equiv (x+1)^2 + 2 \pmod{3} &\Rightarrow x &\equiv 0, 1 \pmod{3}, \\
 &\equiv x^2 + 2 \pmod{5} &\Rightarrow &\text{keine Nullstelle} \pmod{5}, \\
 &\equiv (x+2)^2 - 1 \pmod{7} &\Rightarrow x &\equiv -1, 4 \pmod{7},
 \end{aligned}$$

(b) In der vorangegangenen Aufgabe haben wir ermittelt, daß der Funktionswert  $f(x)$  genau dann durch 2, 3 und 7 teilbar ist, wenn

$$x \equiv 1 \pmod{2}, \quad x \equiv 0, 1 \pmod{3} \quad \text{und} \quad x \equiv -1, 4 \pmod{7}.$$

Nach dem Chinesischen Restsatz gibt es damit 4 Restklassen  $x$  zum Modul 42, für die  $42 \mid f(x)$ . Im Intervall  $[0, 83]$  gibt es daher genau 8 Argumente  $x$ , für die  $42 \mid f(x)$ .

(c) Wir haben  $n = 10123$  und  $m = 100$ . Es gilt  $f(X) = (X + 100)^2 - 10123$ . Wir ergänzen das gegebene Sieb wie folgt:

$x$	1	3	5	7	9	11	13	15
$2 \mid f(x)$	$x$	$x$	$x$	$x$	$x$	$x$	$x$	$x$
$3 \mid f(x)$	$x$	$x$		$x$	$x$		$x$	$x$
$5 \mid f(x)$								
$7 \mid f(x)$						$x$	$x$	
Rest( $x$ )	13	1	451	221	293	157	1	517

$$\begin{aligned}
 f(3) &\equiv (3+m)^2 &\equiv 2 \cdot 3^5 &\pmod{n} \\
 f(13) &\equiv (13+m)^2 &\equiv 2 \cdot 3^3 \cdot 7^2 &\pmod{n}
 \end{aligned}$$

Wir erhalten einen Faktor von  $n$  als

$$\begin{aligned}
 &\gcd((m+3) \cdot (m+13) - 2 \cdot 3^4 \cdot 7, n) = \\
 &\gcd(11639 - 1134, n) = \\
 &\gcd(10505, 10123) = \\
 &\gcd(382, 10123) = \\
 &\gcd(382, 191) = \\
 &191.
 \end{aligned}$$

Wir können nun verifizieren:  $10123 = 191 \cdot 53$

## Aufgabe 5 (Endliche Körper I)

- (a) • Wir stellen zunächst fest, daß die Abbildung  $\pi$  linear ist:

$$\pi(a + b) = \sum_{i=0}^{m-1} (a_i + b_i) X^i = \pi(a) + \pi(b)$$

- Die Multiplikation mit einem festen Element  $b$  in einem endlichen Körper ist eine lineare Abbildung
  - Die Abbildungen  $\phi_b$  ist daher eine Hintereinanderausführung mehrerer linearer Abbildungen und damit wieder linear. Daher läßt sie sich auch mit der Matrix  $G_b \in \mathbb{Z}_2^{m \times m}$  beschreiben.
- (b) Um die Bijektivität der Abbildung zu zeigen, beweisen wir, daß  $G_{g^i} = (G_g)^i$  für alle  $i \in \mathbb{N}$  gilt. Zunächst stellen wir fest, daß die 1 auf die Einheitsmatrix abgebildet wird:  $G_{g^0} = G_g^0$ . Wir zeigen nun also den Induktionsschritt  $(i - 1) \mapsto i$ : Für alle  $a \in \mathbb{F}_2^m$  gilt:

$$\begin{aligned} aG_g^i &= aG_g G_g^{i-1} && \text{mit } aG_g = \phi_g(a) = \pi^{-1}(\pi(a)g) \\ &= \pi^{-1}(\pi(a)g)G_g^{i-1} && \text{Induktionvoraussetzung} \\ &= \pi^{-1}(\pi(a)g)G_{g^{i-1}} \\ &= \pi^{-1}(\pi(a)gg^{i-1}) \\ &= \pi^{-1}(\pi(a)g^i) \\ &= aG_{g^i} \end{aligned}$$

Aus dieser Aussage folgt direkt die Multiplikativität.

- (c) Die multiplikative Untergruppe hat genau  $2^m - 1$  Elemente, da jedes Ihrer Elemente mit einem der Elemente des endlichen Körpers korrespondiert. Wer diskrete Logarithmen in  $\mathcal{G}$  berechnen kann, der kann auch diskrete Logarithmen in  $\mathbb{F}_{2^m}^\times$  berechnen und umgekehrt, daher ist das Problem, diskrete Logarithmen zu berechnen in beiden Gruppen gleich schwer.
- (d) Wir erhalten das folgende Verschlüsselungsverfahren:
- Klartextraum:  $\mathcal{P} = \mathcal{G}$ .
  - Schlüsseltextraum:  $\mathcal{C} = \mathcal{P}$ .
  - Schlüsselraum:  $\mathcal{K} = \{((\mathcal{G}, G, A), a) \mid G, A \in \mathcal{G}; a \in \mathbb{N}; A = G^a\}$ .
  - Schlüsselgenerierung: Wähle zufällig einen Generator  $G$  von  $\mathcal{G}$  und  $a \in \mathbb{N}$  und berechne  $A = G^a$ . Der öffentliche Schlüssel ist  $(\mathcal{G}, G, A)$ , der geheime  $a$ . Der gesamte Schlüssel ist daher  $k = ((\mathcal{G}, G, A), a) \in \mathcal{K}$ .
  - Verschlüsselung: Wähle zufällig  $b \in \mathbb{N}$  und berechne  $B = G^b$ . Für die Nachricht  $M \in \mathcal{P}$  berechne  $C = A^b M$ . Der Schlüsseltext ist  $(B, C)$ .
  - Entschlüsselung: Berechne die Nachricht  $M = B^{-a} C$ .
- (e) Die Ordnung von  $\pi(g) = X \in \mathbb{F}_{2^m}^\times$  ist nicht 1. Das Polynom  $X$  ist ein Generator von  $\mathbb{F}_{2^m}^\times$ , da die Ordnung von  $X$  die Ordnung von  $\mathbb{F}_{2^m}^\times$  teilen muß, welche 31 und damit eine Primzahl ist. Wir erhalten die Matrix, die  $\phi_g$  beschreibt, indem wir in die  $i$ -te Zeile von  $G$  den Vektor  $\pi^{-1}(gX^{5-i})$  eintragen. Es gilt dann:

$$\phi_g : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m \\ x \mapsto xG$$

mit

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$