



Musterlösung zur Klausur zu “Einführung in die Kryptographie”

SS 2000

1. Aufgabe: Euklidischer Algorithmus (10 Punkte)

Berechnen Sie mit Hilfe des erweiterten euklidischen Algorithmus den ggT von 35 und 96 inklusive Darstellung.

Wir wenden den erweiterten euklidischen Algorithmus an und erhalten folgende Tabelle

k	0	1	2	3	4	5
r_k	96	35	26	9	8	1
q_k		2	1	2	1	8
x_k	1	0	1	1	3	4
y_k	0	1	2	3	8	11

Damit ist $1 = \gcd(96, 35) = -4 \cdot 96 + 11 \cdot 35$.

2. Aufgabe: Schnelle Exponentiation (10 Punkte)

Berechnen Sie mit dem in der Vorlesung vorgestellten Algorithmus zur schnellen Exponentiation $6^{19} \bmod 26$.

$$6^2 \equiv 10 \pmod{26}$$

$$6^4 \equiv 22 \pmod{26}$$

$$6^8 \equiv 16 \pmod{26}$$

$$6^{16} \equiv 22 \pmod{26}$$

Damit ist $6^{19} \equiv 6^{16}6^26 \equiv 22 \cdot 10 \cdot 6 \equiv 20 \pmod{26}$. Also ist $6^{19} \bmod 26 = 20$.

3. Aufgabe: Chinesischer Restsatz (10 Punkte)

Berechnen Sie die kleinste, nicht negative Lösung der simultanen Kongruenz $x \equiv 2 \pmod{4}$, $x \equiv 3 \pmod{9}$ und $x \equiv 1 \pmod{11}$.

Wir finden

$$\begin{aligned}99^{-1} &\equiv 3 \pmod{4}, \\44^{-1} &\equiv 8 \pmod{9}, \\36^{-1} &\equiv 4 \pmod{11}.\end{aligned}$$

Damit gilt für die Lösung x der simultanen Kongruenz

$$\begin{aligned}x &\equiv 2 \cdot 3 \cdot 99 + 3 \cdot 8 \cdot 44 + 1 \cdot 4 \cdot 36 \pmod{396} \\ &\equiv 210.\end{aligned}$$

Damit ist $x = 210$ die kleinste, nicht negative Lösung der simultanen Kongruenz.

4. Aufgabe: Wurzel modulo n (10 Punkte)

Berechnen Sie eine 35-te Wurzel von 2 modulo 119. Hinweis: $119 = 7 \cdot 17$.

Die Gruppenordnung von $\mathbb{Z}/(119\mathbb{Z})^*$ ist $6 \cdot 16 = 96$. Wir berechnen d , so dass

$$d \cdot 35 \equiv 1 \pmod{96}.$$

Nach Aufgabe 1) ist $d = 11$ eine Lösung der Kongruenz. Dann ist 2^d eine 35-te Wurzel aus 2, denn es ist $(2^d)^{35} \equiv 2 \pmod{119}$. D.h. eine 35-te Wurzel aus 2 modulo 119 ist

$$2^{11} \equiv 25 \pmod{119}.$$

5. Aufgabe: Pohlig-Hellman Algorithmus (10 Punkte)

Lösen Sie $2^x \equiv 7 \pmod{29}$ mit dem Pohlig-Hellman Algorithmus.

Die Gruppenordnung ist $p - 1 = 2^2 \cdot 7$. Wir bestimmen die Lösung modulo 2^2 und 7, und wenden dann den Chinesischen Restsatz an.

(a) $x \pmod{2^2}$

Wir potenzieren die Kongruenz mit 7 und erhalten die neue Kongruenz

$$12^{x_0+2 \cdot x_1} \equiv 1 \pmod{29},$$

mit $0 \leq x_0, x_1 < 2$. Durch Quadrieren finden wir $x_0 = 0$ und ebenso $x_1 = 0$, also ist

$$x \equiv 0 \pmod{2^2}.$$

(b) $x \pmod{7}$

Wir potenzieren die Kongruenz mit 4 und erhalten die neue Kongruenz

$$16^x \equiv 23 \pmod{29}.$$

Wir finden $16^2 \equiv 24$, $16^3 \equiv 7$, $16^4 \equiv 25$ und schließlich $16^5 \equiv 23$. Also ist

$$x \equiv 5 \pmod{7}.$$

Wir lösen die simultane Kongruenz für x mit dem Chinesischen Restsatz. Es ist $x \equiv 5 \cdot 2 \cdot 4 \equiv 12 \pmod{28}$. Also ist

$$x = 12.$$

6. Aufgabe ElGamal-Verschlüsselung (10 Punkte)

Der öffentliche ElGamal-Schlüssel von Alice ist $p = 29$, $g = 2$, $A = 7$.

(a) Berechnen Sie eine ElGamal Verschlüsselung der Nachricht $m = 10$ für Alice. Wählen Sie als zufällige Zahl 5.

(b) Sie haben herausgefunden, dass der geheime Schlüssel von Alice 12 ist. Alice erhält die Nachricht $(c, B) = (21, 10)$. Wie lautet der Klartext? Hinweis: Das Inverse von 20 modulo 29 ist 16.

(a) Wir berechnen

$$B \equiv 2^5 \equiv 3 \pmod{29}.$$

Wir erhalten als Schlüssel $K \equiv 7^5 \equiv 16 \pmod{29}$. Damit ist

$$c \equiv 10 \cdot 16 \equiv 15 \pmod{29}.$$

Der Chiffretext ist also

$$(c, B) = (15, 3).$$

(b) Alice berechnet den gemeinsamen Schlüssel

$$K \equiv 10^{12} \equiv 20 \pmod{29}.$$

Laut Hinweis wissen wir, dass $K^{-1} \equiv 16 \pmod{29}$ ist. Damit ist der Klartext

$$m \equiv 21 \cdot 16 \equiv 17 \pmod{29}.$$

7. Aufgabe DSA (10 Punkte)

Sei $p = 29$ mit Primitivwurzel $x = 2$. Der geheime Schlüssel von Alice ist $a = 4$. Der Hashwert einer Nachricht m sei $h(m) = 6$. Wählen Sie $q = 7$.

(a) Berechnen Sie die DSA-Signatur der Nachricht mit $k = 2$.

(b) Geben Sie die Formeln zur Verifikation an und verifizieren Sie die Signatur.

(a) Wir führen die Schlüsselerzeugung fort. Wir rechnen in der Untergruppe, die von

$$g \equiv 2^4 \equiv 16 \pmod{29}$$

erzeugt wird. Zum Erzeugen der Signatur berechnen wir zuerst

$$r = (16^2 \pmod{29}) \pmod{7} = 24 \pmod{7} = 3.$$

Es ist

$$\begin{aligned}s &= k^{-1}(h(m) + ar) \bmod 7 \\ &= 4 \cdot (6 + 4 \cdot 3) \bmod 7 \\ &= 2.\end{aligned}$$

Damit lautet die Signatur

$$(r, s) = (3, 2).$$

(b) Wir vervollständigen die Schlüsselerzeugung. Der öffentliche Schlüssel ist

$$A \equiv 16^4 \equiv 25 \bmod 29.$$

Wir überprüfen für die Signatur $(r, s) = (3, 2)$, dass $0 \leq r, s < q = 7$. Weiterhin berechnen wir

$$\begin{aligned}&(g^{(s^{-1}h(m)) \bmod q} A^{(s^{-1}r) \bmod q}) \bmod p \bmod q \\ &= (16^{4 \cdot 6 \bmod 7} \cdot 25^{4 \cdot 3 \bmod 7}) \bmod 29 \bmod 7 \\ &= (16^3 \cdot 25^5) \bmod 29 \bmod 7 \\ &= (7 \cdot 20) \bmod 29 \bmod 7 \\ &= 24 \bmod 7 \\ &= 3 = r.\end{aligned}$$

Also ist die Signatur korrekt.

8. Aufgabe: Rabin-Verschlüsselung (10 Punkte)

Übertragen Sie die Low-Exponent-Attacke, die beim RSA-Verfahren besprochen wurde, auf das Rabin-Verfahren und schlagen Sie eine entsprechende Gegenmaßnahme vor.

Übertragen Sie die Low-Exponent-Attacke, die beim RSA-Verfahren besprochen wurde, auf das Rabin-Verfahren und schlagen Sie eine entsprechende Gegenmaßnahme vor.

Bob habe den öffentlichen Rabin-Schlüssel n_1 und Charlie habe n_2 . Wir nehmen an, dass $ggT(n_1, n_2) = 1$.

Das Szenario ist wie folgt. Alice schickt eine Nachricht m mit $0 \leq m < \min\{n_1, n_2\}$ verschlüsselt an Bob und Charlie, d.h. sie berechnet

$$c_1 = m^2 \bmod n_1, c_2 = m^2 \bmod n_2,$$

und sendet c_1 bzw. c_2 an Bob bzw. Charlie.

Der Lauscher Oskar berechnet aus c_1, n_1 und c_2, n_2 die Nachricht, indem er mit dem chinesischen Restsatz ein c bestimmt, so dass

$$c = c_1 \bmod n_1, c = c_2 \bmod n_2.$$

Er wählt $0 \leq c < n_1 n_2$. Dann ist

$$c = m^2.$$

Durch Quadratwurzelberechnung über \mathbb{Z} ermittelt Oskar m .

9. Aufgabe: Birthday-Paradoxon (10 Punkte)

Sie wählen zufällig und gleichverteilt 16 Personen aus, die in der Zeit vom 1. bis 17. Mai Geburtstag haben. Zeigen Sie, dass die Wahrscheinlichkeit dafür, dass 2 davon am gleichen Tag Geburtstag haben, größer als 0,98 ist.

Es gibt 17 mögliche Geburtstage und 16 Kandidaten. Die Menge aller Elementarereignisse ist also

$$\{(x_1, \dots, x_{16}) \mid 1 \leq x_i \leq 17, 1 \leq i \leq 16\}.$$

Es gibt 17^{16} Ereignisse. Dabei gibt es $17!$ viele Ereignisse, bei denen alle Geburtstage verschieden sind. Die Wahrscheinlichkeit, dass ein solches Ereignis eintritt, ist bei Annahme der Gleichverteilung

$$\frac{17!}{17^{16}} = (1 - 0/17)(1 - 1/17) \cdots (1 - 15/17).$$

Wir verwenden die Ungleichung $1 + x \leq e^x$ für $x \geq 0$ und schätzen damit diese Wahrscheinlichkeit nach oben ab. Es ist

$$\begin{aligned} \frac{17!}{17^{16}} &\leq e^{0 - 1/17 - 2/17 - \dots - 15/17} \\ &= e^{-1/17 \cdot 1/2 \cdot 15 \cdot 14} \\ &= e^{-105/17} \\ &< 2^{-6}. \end{aligned}$$

Damit ist die Wahrscheinlichkeit, dass 2 Personen am gleichen Tag Geburtstag haben, größer gleich

$$1 - 2^{-6} = 63/64 > 0,98.$$