Mathematische Grundlagen der Kryptografie

4. Übungsblatt, SS 2006 — 30.05.2006

32. Implementieren Sie in `Mathematica` einen affin linearen Blockchiffre mit Blocklänge 3. Das zugrundeliegende Alphabet ist $\{A, B, C, \ldots, Z\}$ und wird mit den Zahlenwerten $\{0, 1, \ldots, 25\}$ identifiziert. d. h. die Verschlüsselungsfunktion lautet:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \longmapsto A \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$$

mit $A \in GL_2(\mathbb{Z}_{26})$ und $b_1, b_2, b_3 \in \mathbb{Z}_{26}$.

33. *Häufigkeitsanalyse:* Zur Verschlüsselung des Textes im File `bsp33.txt` wurde ein affin, linearer Blockchiffre mit Blocklänge 2 benutzt, das Alphabet ist $\{A, B, C, \ldots, Z\}$ und wird mit den Zahlenwerten $\{0, 1, \ldots, 25\}$ identifiziert, d. h. die Verschlüsselungsfunktion ist von der Form:

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \longmapsto A \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

mit $A \in GL_2(\mathbb{Z}_{26})$ und $b_1, b_2 \in \mathbb{Z}_{26}$.

Die im Ursprungstext häufigsten Buchstabenpaare sind bekannt:

EN	EI	ER	ND	CH	DE
3.71%	3.22%	3.02%	2.73%	2.73%	2.44%

Bestimmen Sie A, b_1, b_2, und entschlüsseln Sie den Text.

34. Man betrachte das folgende Chiffriersystem, bei dem Nachrichten m Elemente $\neq 0$ von $\mathbb{F}_q$ sind: A wählt zufällig ein $h \in \mathbb{N}$ mit $1 \leq h \leq q-1$ und $\mathrm{ggT}(h, q-1) = 1$ und sendet $x = m^h$ an B. B wählt ein zufälliges $k \in \mathbb{N}$ mit $\mathrm{ggT}(k, q-1) = 1$ und sendet $y = x^k$ an A zurück. Nun bildet A die Nachricht $z = y^{h'}$ mit $hh' \equiv 1 \pmod{q-1}$ und sendet z an B. Man zeige, dass bei diesem "No-Key Algorithm" B die geheime Nachricht m entschlüsseln kann.

35. Es ist die Nachricht "VERKAUFEN" chiffriert an eine Person X zu senden, welche beim RSA-Verfahren den öffentlichen Schlüssel $(n_X, e_X) = (7031, 193)$ hat. Jeder Buchstabe werde mit zwei Ziffern entsprechend seiner Stellung im Alphabet codiert, und die Blocklänge der zu verschlüsselnden Zahlenfolge betrage 3.

36. Ein Teilnehmer X am RSA-Verfahren mit $(p_X, q_X) = (397, 479)$ als privatem und $(n_X, e_X) = (190163, 35)$ als öffentlichem Schlüssel erhält die chiffrierte Nachricht 2, welche im Klartext eine natürliche Zahl darstellt. Wie lautet diese Zahl?

37. Ein Teilnehmer im RSA-Verfahren mit dem öffentlichen Schlüssel $(n_X, e_X) = (1271, 7)$ erhält die chiffrierte Nachricht

$$99, 232, 815, 74, 1047, 196, 384, 196, 1122, 0, 171, 771, 243, 257.$$

Die Buchstaben der Nachricht im Klartext wurden mit 2 Ziffern codiert, und die sich ergebende Ziffernfolge wurde in Blöcke der Länge 3 eingeteilt. Wie lautet die Nachricht im Klartext?

38. Der Text aus dem File `bsp38.txt` wurde mit dem RSA-Kryptosystem verschlüsselt. Das zugrundeliegende Alphabet besteht aus den 91 Zeichen mit ASCII-Werten zwischen 32 und 122. Für die Kodierung wird von jedem ASCII-Wert 32 abgezogen, damit alle Zahlenwerte zweistellig bleiben.

Der verwendete Public Key ist

$$(n, e) = (73994897118368822809, 5).$$

Die Plaintext-Blocklänge ist $k = 8$ und die Ciphertext-Blocklänge ist $\ell = 11$ (jeweils zur Basis $N = 91$). Finden Sie den ursprünglichen Text.

39. Wieviele Operationen erfordert die RSA-Verschlüsselung mit dem Exponenten $e = 2^{16} + 1$.

40. *Common Modulus Attacke*: Angenommen, man verschlüsselt ein und dieselbe Nachricht m mit den öffentlichen Schlüsseln (n, e) und (n, f), wobei $\mathrm{ggT}(e, f) = 1$ gilt. Zeigen Sie, dass man dann aus den Ciphertexten $c_1 \equiv m^e \bmod n$ und $c_2 \equiv m^f \bmod n$ die Nachricht m ermitteln kann.

41. Zwei Teilnehmer A,B am RSA-Verfahren haben die öffentlichen Schlüssel $(n_A, e_A) = (2773, 17), (n_A, e_B) = (2773, 3)$. Jemand sendet an A und B dieselbe Nachricht $w \in \mathbb{N}$. A empfängt 948, B 1870. Man finde w, ohne die privaten Schlüssel von A und B zu berechnen.

42. Es seien die folgenden Werte für n, e und d gegeben:

$$401001362194869496648769419399255343890985388222772299940365685326740 93,$$
$$100000000000000000000000000000000069,$$
$$229376619310780247422849760587723078016586729358214678764442841225342 85.$$

(Diese Werte finden sie auch in der Datei `bsp42.txt`.)
Für diese Zahlen gilt $ed \equiv 1 \bmod \varphi(n)$. Bestimmen Sie mit dieser Information die Faktorisierung von n (anhand der in der VO erläuterten, probabilistischen Methode).