

Kryptoanalyse

Aufgabe 1 Berechnen Sie mit Hilfe des euklidischen Algorithmus $ggT(233, 144)$ und mit Hilfe des erweiterten euklidischen Algorithmus zwei ganze Zahlen s, t mit $ggT(233, 144) = s \cdot 233 + t \cdot 144$.

Aufgabe 2 Wir betrachten ein Kryptosystem, bei dem die Klartexte und die Geheimtexte aus Zeichen des deutschen Alphabets bestehen. Das Verschlüsselungsverfahren ist eine verallgemeinerte Caesar-Addition: Jedem Buchstaben des Klartexts wird als Geheimtext der Buchstabe zugeordnet, der sich um eine feste Stellenzahl s weiter hinten im Alphabet befindet. Bei der klassischen Caesar-Addition ist $s = 3$. Entschlüsseln Sie den folgenden Geheimtext unter Verwendung der Häufigkeit der einzelnen Buchstaben:

FQQJWFSKFSLNXYXHMBJWTIJWFZHMSNHMY

Aufgabe 3 Wir betrachten ein Kryptosystem, dessen Klar- und Geheimtexte endliche Folgen über dem Alphabet $\{B, C, E, F, O, R, T, U\}$ sind. Das Alphabet wird mit den Elementen von $\mathbb{Z}_8$ identifiziert:

B	1	C	2	E	3	F	4	O	5	R	6	T	7	U	0
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Der folgende Geheimtext wurde durch eine Verschlüsselungsfunktion $f_k : \mathbb{Z}_8 \rightarrow \mathbb{Z}_8, x \mapsto k \cdot x + 3 \pmod{8}$ verschlüsselt:

COEFUTROBU

Finden Sie den Klartext durch einen Brute-Force-Angriff. Dabei wird davon ausgegangen, dass f_k eine zulässige Verschlüsselungsfunktion eines Kryptosystems mit den angegebenen Klar- und Geheimtexten ist.

Aufgabe 4 Wir identifizieren die Buchstaben des deutschen Alphabets wie üblich mit den Elementen von $\mathbb{Z}_{26}$. Die Klar- und Geheimtexte des betrachteten Kryptosystems seien Folgen von Zeichen des deutschen Alphabets. Diese werden paarweise verschlüsselt mit einer Verschlüsselungsfunktion der Form $f : \mathbb{Z}_{26}^2 \rightarrow \mathbb{Z}_{26}^2, x \mapsto Ax + b \pmod{26}$. Der Schlüssel besteht aus dem Paar (A, b) , wobei A eine 2×2 -Matrix bezeichnet und $b \in \mathbb{Z}_{26}^2$ gilt. Wir rechnen komponentenweise modulo 26. Bekannt ist, dass die gesuchte Verschlüsselungsfunktion den Klartext SENDEN in den Geheimtext CIPHER Verschlüsselt. Führen Sie einen Klartextangriff durch, um den folgenden Geheimtext zu bestimmen:

VEEMQXIMRYYFGVNEBP

Kryptoanalyse

Aufgabe 5 Der folgende Geheimtext wurde durch eine monoalphabetische Substitution erzeugt:

PVZHZJGZCGDFJPZEZJHSWRFZHHZRGPMQV
GHVZFZIZOTNZOOZODVZQMOQNONMRLWMIZ
GVHSWZHFIHGVGFGVNOZOTOMSTGMRRZJPV
OXHVHGPZJGZCGHNONSWAFTFJAPMJFQHGJ
ZFZODVJPMHDNJGQVHHVHHVLLVMRHIZVHL
VZRZVOZHTNVOAVPZOAQFHGZJHZVO

Entschlüsseln Sie ihn.

Aufgabe 6 Stellen Sie das Vigenère-Verfahren als Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ im Sinne von Definition 1.1 dar.

Aufgabe 7 Der folgende Geheimtext wurde mit dem Vigenère-Verfahren verschlüsselt. Entschlüsseln Sie ihn, indem Sie zunächst durch Suche von Parallelstellen die Länge des Schlüsselworts herausfinden.

ARUBSXWSPUPHVJJFJPYNTKKUQWRYUJYJJNPSTFUMABBGGYA
YQCPTBNKYZZXXJVJIIILNQMWEVNJVJARPNEYWREJNMHXUQ
WNYQLPZFJYAGAESNUMAWLSHXHWELOYRFVZNLOGZJAGAWJMO
WSPPNYNGYAXYQLRIXLJNMLWKTWPNYJFMSQPNUJWSWJJCZH
VJAIWKJJJJGABZJFZFLCNNJBZWGAATTBTSQLQHGSYAXYQL
WGZTXPRAZHNGSEBAIWJHTHHHQDMSGACPXQMWXQKZYWYMYEX
UMWJJGARDNFIVNABBGYAYQCPTBXNTNBJMFNXYRXUISWHTO
RANCSARPNEYOGZFAWNNULWRWLOYRNWPHJZXWXUMAOWVAIWW
LXSDOQHMWKLYWXUMAWZZPXLNPDANCSAXPMHXJNYJJNYJJJJ
KWQYJB

Aufgabe 8 Welche der folgenden Zahlen ist ein zulässiger DES-Schlüssel (hexadezimal geschrieben)?

133457799BBCDFF1

133457799BBCDEF1

Berechnen Sie den ersten Rundenschlüssel K_1 des gültigen Schlüssels.

Kryptoanalyse

Aufgabe 9 Gegeben sei eine Blockchiffre der Länge 8 mit Alphabet $\{0, 1\}$. Der Schlüsselraum sei $\mathcal{K} = S_8$, wobei S_8 die Menge der Permutationen der Menge $\{1, 2, 3, 4, 5, 6, 7, 8\}$ bezeichne.

a) Es sei π die folgende Permutation:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 1 & 5 & 2 & 4 & 8 & 6 \end{pmatrix}$$

Finden Sie die Entschlüsselungsfunktion D_π zur Verschlüsselungsfunktion

$$E_\pi : \{0, 1\}^8 \rightarrow \{0, 1\}^8, \quad b_1 b_2 b_3 b_4 b_5 b_6 b_7 b_8 \mapsto b_{\pi(1)} b_{\pi(2)} b_{\pi(3)} b_{\pi(4)} b_{\pi(5)} b_{\pi(6)} b_{\pi(7)} b_{\pi(8)}.$$

b) Der folgende Geheimtext c wurde im CBC-Mode mit Initialisierungsvektor $IV = 01100101$ mit der Verschlüsselungsfunktion E_π verschlüsselt:

$$c = 01100101 \ 10010011 \ 01101100 \ 10000000 \ 00111001 \ 11001101$$

Entschlüsseln Sie ihn. Wenn man jedes Byte des Klartexts mit einem Zeichen des erweiterten ASCII-Codes identifiziert, so ergibt sich ein Lösungswort.

Aufgabe 10 Wir betrachten den Bitstring $(L_1, R_1) :=$

$$(1111 \ 0000 \ 1010 \ 1010 \ 1111 \ 0000 \ 1010 \ 1010, \\ 1100 \ 1111 \ 0100 \ 1011 \ 0110 \ 0101 \ 0100 \ 0100).$$

Es handelt sich dabei um das Ergebnis der ersten DES-Runde mit dem Schlüssel $133457799BBCDFF1$ (hexadezimal geschrieben). Finden Sie den Klartext.

Aufgabe 11 Beweisen Sie, dass die S-Box S_1 nicht linear ist.

Aufgabe 12 a) Es gelte $K_1 = K_2 = \dots = K_{16}$. Was gilt für die Bits in C_1 und für die Bits in D_1 ?

b) Folgern Sie, dass es genau vier DES-Schlüssel gibt, für die alle Runden-schlüssel gleich sind. Dies sind die sogenannten *schwachen DES-Schlüssel*.

Kryptoanalyse

Aufgabe 13 Wir betrachten ein Verschlüsselungsverfahren, bei dem vier DES-Runden zur Verschlüsselung durchgeführt werden. Die initiale Permutation wird nicht durchgeführt. Klartext- und Schlüsselraum seien wie im DES gewählt. Gegeben seien zwei bekannte Klartexte (Bitstrings der Länge 64) mit der Differenz

20 00 00 00 00 00 00 00 (hexadezimale Schreibweise).

Außerdem seien die zugehörigen Geheimtexte gegeben. Wie kann man den bei dieser Verschlüsselung verwendeten Schlüssel bestimmen (zumindest einige Bits)?

Aufgabe 14 a) Ist die Zahl 341 eine Primzahl?

b) Ist $n := 2^{25} + 1$ eine Primzahl?

Aufgabe 15 Bestimmen Sie die kleinste 512-Bit-Primzahl.

Kryptoanalyse

Vorbemerkung Ein Verfahren zur schnellen Exponentiation:

Sei $g \in \mathbb{Z}_n$ für ein $n \in \mathbb{N}$ und sei $e \in \mathbb{N}$. $e = \sum_{i=0}^k e_i 2^i$ sei die Binärentwicklung von e . Dann gilt

$$g^e = g^{\sum_{i=0}^k e_i 2^i} = \prod (g^{2^i})^{e_i} = \prod_{0 \leq i \leq k, e_i=1} g^{2^i}$$

Aus dieser Formel gewinnt man die Idee für folgendes Verfahren:

1. Berechne die sukzessiven Quadrate $g^{2^i} \bmod n$, $0 \leq i \leq k$.
2. Bestimme $g^e \bmod n$ als Produkt derjenigen g^{2^i} , für die $e_i = 1$ ist.

Aufgabe 16 Berechnen Sie $6^{73} \bmod 100$ gemäß der Methode aus der Vorbemerkung. Zählen Sie die Anzahl der benötigten Rechenoperationen und vergleichen Sie sie mit der Anzahl benötigter Rechenoperationen, wenn Sie $6^{73} \bmod 100$ nur durch Multiplikation berechnen.

Aufgabe 17 a) Wenn man mit dem RSA-Verfahren eine Nachricht m zweimal verschlüsselt und zwar mit den öffentlichen Schlüsseln (n, e) und (n, f) und wenn $gfT(e, f) = 1$ gilt, dann kann man den Klartext m aus den beiden Geheimtexten $c_e = m^e \bmod n$ und $c_f = m^f \bmod n$ berechnen. Wie geht das?

b) Die Nachricht m wird mit den öffentlichen RSA-Schlüsseln $(493, 3)$ und $(493, 5)$ verschlüsselt. Die Geheimtexte sind 293 und 421. Bestimmen Sie m .

Aufgabe 18 Alice sei Nutzerin des RSA-Verfahrens. Ihr öffentlicher Schlüssel sei $(n, e) = (10403, 3)$. Jemand schickt ihr die Nachrichten m und $m + 1$. Sie fangen die beiden Geheimtexte c_1 von m und c_2 von $m + 1$ ab. Es gilt

$$c_1 = 5791, \quad c_2 = 473.$$

Finden Sie den Klartext m , ohne n zu faktorisieren.

Kryptoanalyse

Aufgabe 19 Bestimmen Sie mit dem quadratischen Sieb einen echten Faktor von 11111.

Hinweis: Ein geeignetes Siebintervall ist z. B. die Menge $\{-10, -9, \dots, 9, 10\}$.

Aufgabe 20 Der folgende Geheimtext wurde mit dem RSA-Verfahren verschlüsselt. Der verwendete öffentliche Schlüssel lautet $(n, e) = (11111, 6353)$. Der Klartext bestand aus den 26 Buchstaben des deutschen Alphabets. Diese wurden gemäß der Tabelle auf Seite 12 des Vorlesungsskripts mit dem Elementen von $\mathbb{Z}_{26}$ identifiziert. Der Klartext wurde vor der Verschlüsselung in Blöcke unterteilt und jeder der Blöcke wurde als Zahl zur Basis 26 dargestellt. Entsprechend wurde nach der Verschlüsselung jeder Geheimtextblock in Buchstaben rückübersetzt. Je drei Buchstaben bilden einen Geheimtextblock. Der Geheimtext lautet nun

BBS MOT MQV

Entschlüsseln Sie ihn.

Aufgabe 21 Der Geheimtext wurde mit dem Vigenère-Verfahren verschlüsselt das Schlüsselwort ist der Klartext aus Aufgabe 20. Finden Sie den Klartext.

MMHEFABHZGWXLFWXKNJDENMATVKNZKFJW

Kryptoanalyse

Aufgabe 22 Alice sendet eine Nachricht an Bob gemäß Shamirs No-Key-Protokoll. Die beiden haben sich auf die Primzahl $p = 31$ geeinigt, d. h. sie rechnen in $\mathbb{Z}_{31}^*$. Alice schickt einzelne Buchstaben an Bob, jeden Buchstaben identifiziert sie zunächst mit einem Element von $\mathbb{Z}_{26}$ gemäß der Tabelle auf Seite 12 des Vorlesungsskripts. Um die Nachricht lesen zu können, muss Bob die einzelnen Buchstaben wieder zusammenfügen. Sie beobachten, dass zur Übermittlung des ersten Buchstaben s_1 die Zahlen

$$x_1 = 28, \quad y_1 = 18, \quad z_1 = 20$$

zwischen Alice und Bob ausgetauscht werden, zur Übermittlung des zweiten Buchstaben s_2 die Zahlen

$$x_2 = 23, \quad y_2 = 23, \quad z_2 = 15.$$

Wie lautet die Nachricht im Klartext?

Vorbemerkung Sei p eine Primzahl. Dann existiert bekanntlich ein erzeugendes Element von $\mathbb{Z}_p^*$, d. h. ein Element g mit $\mathbb{Z}_p^* = \{g^n | n = 1, \dots, p-1\}$. Ein erzeugendes Element erzeugt also die ganze Gruppe. Ist $h \in \mathbb{Z}_p^*$ kein erzeugendes Element, so ist $\{h^n | n = 1, \dots, p-1\}$ eine echte Teilmenge von $\mathbb{Z}_p^*$. Wir definieren für $h \in \mathbb{Z}_p^*$: $o(h) := |\{h^n | n = 1, \dots, p-1\}|$. Es läßt sich nun beweisen, dass für jedes $a \in \mathbb{Z}_p^*$ und jedes $k \in \mathbb{Z}$ gilt: Ist $o(a) = n$ für ein $n \in \mathbb{N}$, so folgt

$$o(a^k) = \frac{n}{\gcd(n, k)}.$$

Aufgabe 23 Sie möchten mit Alice einen geheimen Schlüssel k mit dem Diffie-Hellman-Schlüsselaustausch vereinbaren. Sie einigen sich auf die Primzahl $p = 29$ und wählen $g = 2$ als erzeugendes Element von $\mathbb{Z}_{29}^*$. Alice wählt ihr geheimes a und sendet Ihnen das öffentliche $\alpha = g^a = 28$. Wieviele verschiedene Schlüssel k kommen noch in Frage?

Aufgabe 24 Alice und Bob vereinbaren einen geheimen Schlüssel k gemäß dem Diffie-Hellman-Austausch. Sie wählen die Primzahl $p = 2017$ und das erzeugende Element $g = 5$. Es gelte $\alpha = 3$, $\beta = 288$. Den gemeinsam vereinbarten Schlüssel verwenden sie als Schlüssel für eine Caesar-Verschlüsselung. Alice sendet an Bob den folgenden Geheimtext:

ABOYBPQBPZEIRBPPBIXRPQXRPZEEFICQKFZEQPTBKK
AXPSBOPZEIRBPPBIRKDPSBOCXEOBKWRMOFJFQFSFPQ

Entschlüsseln Sie ihn.

Kryptoanalyse

Aufgabe 25 Um Geld von ihrem Bankautomaten abzuheben verwendet Alice das RSA-Signaturschema ohne Hashfunktion. Ihr RSA-Modul ist $n = 253$, ihr öffentlicher Verifikationsexponent lautet $e = 3$. Erhält der Automat eine Eingabe s , so interpretiert er dies als Signatur von Alice. Er berechnet $m = s^e \bmod n$ und gibt m Euro aus. Oskar möchte sich auf Kosten von Alice bereichern. Welches s soll er dem Automaten eingeben?

Aufgabe 26 Alice benutzt das ElGamal-Signaturverfahren mit $(p, g) = (2237, 2)$. Ihr geheimer Schlüssel lautet $a = 1234$. Sie signiert für Sie eine Nachricht m , die bei der verwendeten Hashfunktion h den Hashwert $h(m) = 111$ habe. Sie wählt $k = 87$. Wie lautet das Signaturpaar (r, s) , das Sie von Alice erhalten? Wie verifizieren Sie die Signatur?

Aufgabe 27 Wir betrachten das ElGamal-Signaturverfahren mit $(p, g) = (101, 2)$. Die zu signierenden Dokumente bestehen aus Großbuchstaben des deutschen Alphabets. Einem Dokument wird ein Hashwert zugeordnet, indem die Buchstaben des Dokuments gemäß dem ASCII-Code als natürliche Zahl interpretiert werden. Jeder solchen natürlichen Zahl wird dann ihre Binärdarstellung zugeordnet, vorne so mit Nullen aufgefüllt, dass sie genau acht Bit lang ist. Nun werden sämtliche durch die Buchstaben des Dokuments gegebenen Bytes per *XOR* addiert. Das resultierende Byte ist der Hashwert des Dokuments. Alice war faul und hat die beiden Dokumente "ALLES", "KLAR" mit dem gleichen k signiert. Sie erhalten die beiden zugehörigen Signaturen $(s_1, r_1) = (64, 89)$ und $(s_2, r_2) = (57, 89)$. Finden Sie Alice' geheimen Signaturschlüssel a .

Aufgabe 28 Das ElGamal-Signaturverfahren werde ohne Hashfunktion angewendet, d. h. zur Verifikation der Signatur (r, s) einer Nachricht x wird überprüft, ob gilt $1 \leq r \leq p - 1$ und ob folgende Gleichung erfüllt ist:

$$\alpha^r r^s = g^x \bmod p.$$

Dabei bezeichnet p eine für das Verfahren fest gewählte Primzahl und g ein erzeugendes Element von $\mathbb{Z}_p^*$. Bei diesem Verfahren ist existentielle Fälschung möglich! Geben Sie eine Signatur (r, s) und ein Dokument x an, so dass (r, s) und x die Verifikation überstehen.