3.2 Kryptologie – Beaufort Chiffre

Im Jahr 1857 präsentierte Sir Francis Beaufort eine Chiffre als „das neue Verschlüsselungssystem für Telegramme und Postkarten".
Die Beaufort-Chiffre verwendet ein Schlüsselwort, um Nachrichten buchstabenweise zu verschlüsseln. In der folgenden Tabelle sind die ersten vier Zeilen des Beaufort-Tableaus für das Schlüsselwort „ABITUR" dargestellt. In der grauen Zeile befinden sich die Klartextbuchstaben und in der grauen Spalte das Schlüsselwort. Den jeweiligen Geheimtextbuchstaben erhält man, wenn man das Zeichen in der Spalte des gegebenen Klartextbuchstabens und der Zeile des aktuell gewählten Buchstaben des Schlüsselwortes wählt. Das erste Klartextzeichen wird mit dem ersten Zeichen des Schlüsselworts chiffriert, das zweite mit dem zweiten, usw. Sind alle Zeichen des Schlüsselwortes aufgebraucht, beginnt man wieder von vorne mit dem Schlüsselwort.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
B	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C
I	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J
T	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U
U																										
R																										

3.2.1. Ergänzen Sie in der gleichen Vorgehensweise die letzten beiden Zeilen des Beaufort-Tableau für das Schlüsselwort „ABITUR".

3.2.2. Verschlüsseln Sie mit dem Schlüsselwort „ABITUR" den Klartext „INFORMATIK".

3.2.3. Klassifizieren Sie die Beaufort-Chiffre und nehmen Sie Stellung zur Sicherheit bei einer Kryptoanalyse mittels Häufigkeitsverteilung!

3.1 RSA-Verfahren

3.1.1 Begründen Sie zu $p = 23$ und $q = 11$ die Werte $n = 253$ sowie $\varphi(n) = 220$.

3.1.2 Bestimmen Sie zu $p = 23$, $q = 11$ und $e = 17$ den Wert d des privaten Schlüssels.

3.1.3 Verschlüsseln Sie die Botschaft $m = 3$ mit dem öffentlichen Schlüssel $(e, n) = (17{,}253)$.

3.1.4 Die Sicherheit des RSA Verfahrens beruht darauf, dass man glaubt (und hofft), ein bekanntes Problem sei nur sehr schwer lösbar. Nennen Sie dieses Problem.

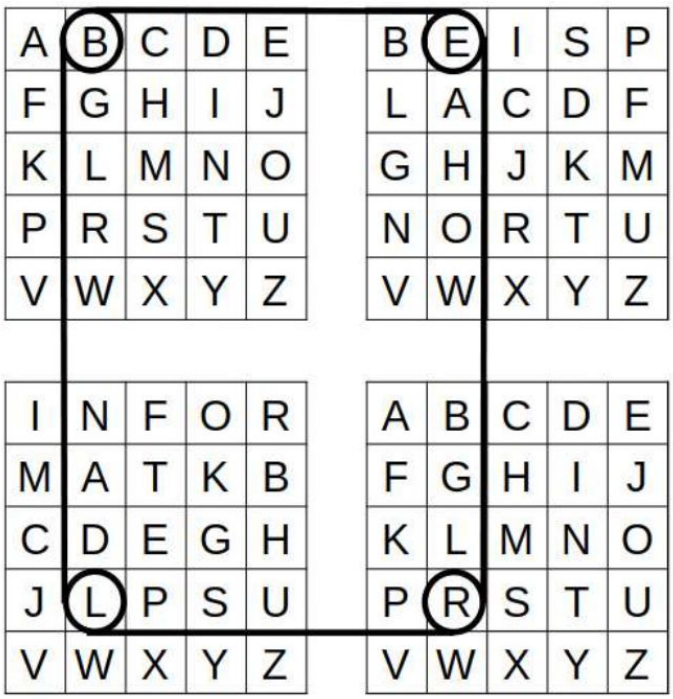
3.1.5 Begründen Sie, dass $\varphi(n)$ für beliebige Primzahlen p und q mit $p \neq q$ immer eine gerade Zahl ist und dass deshalb sowohl *d* als auch *e* niemals gerade sein dürfen.

3.1.6 Prüfen Sie, welche Wertekombinationen für n, d und e im Sinne des RSA-Verfahrens geeignet sind:

(1) $n = 91, d = 5, e = 31$ (2) $n = 55, d = 13, e = 37$ (3) $n = 41, d = 3, e = 17$

3.2 Klassische Verschlüsselungsverfahren – Four Square Verfahren

Bei dem Verfahren werden einzelne Buchstabenpaare (Bigramme genannt) zur Verschlüsselung herangezogen. Bei der Verschlüsselung selbst zerlegt man zuerst den Klartext in einzelne Bigramme. Wenn für das letzte Bigramm ein Buchstabe fehlt, wird ein zufälliger Buchstabe hinzugefügt. Zum Verschlüsseln werden vier mit Buchstaben gefüllte Quadrate mit jeweils 25 unterschiedlichen Buchstaben verwendet. Man verteilt also das gesamte Alphabet mit Ausnahme des selten vorkommenden Buchstabens Q auf jedes der vier Quadrate. Vor dem Verschlüsseln wird aus dem Klartext der Buchstabe Q entfernt. Die Verständlichkeit der Nachricht nimmt dadurch üblicherweise nicht ab. Die vier Quadrate sind in einem 2x2-Raster angeordnet, wie im dargestellten Beispiel ersichtlich.



Um ein Bigramm zu verschlüsseln, wird der erste Buchstabe im Quadrat links oben markiert und der zweite Buchstabe im Quadrat rechts unten. Diese beiden Buchstaben bilden die linke obere und rechte untere Ecke eines Rechtecks. Sie werden beim Verschlüsseln ersetzt durch die linke untere und rechte obere Ecke des Rechtecks. Im abgebildeten Beispiel wird das Bigramm BR also zum Bigramm LE verschlüsselt.

Dabei werden zwei Schlüssel verwendet, mit Hilfe derer die Quadrate links unten und rechts oben aufgebaut werden. In die Quadrate werden zunächst die Schlüsselwörter ohne Buchstabendopplungen eingetragen (hier links unten : *Informatik* und rechts oben : *Beispiel*) und anschließend das restliche Alphabet aufgefüllt (ohne Q). In das linke obere und das rechte untere Quadrat wird immer das Alphabet (ohne Q) wie abgebildet eingetragen.

3.2.1 Geben Sie an, zu welchem Buchstabenpaar das Bigramm HA mit Hilfe der abgebildeten Quadrate verschlüsselt wird.

3.2.2 Ordnen Sie das Verfahren begründet den Substitutions- und Transpositionsverfahren zu.

3.2.3 Notieren Sie die vier Quadrate die sich ergeben, wenn man als Schlüssel SAARLAND (rechts oben) und GYMNASIUM (links unten) verwendet.

3.2.4 Entschlüsseln Sie den Geheimtext `SYJAEBAUFS` mit den Schlüsselwörtern SAARLAND und GYMNASIUM.

3.2.5 Beurteilen Sie die Sicherheit des Verfahrens.

RSA – Verfahren

3.2 Gegeben ist ein RSA-Kryptosystem.

3.2.1 Das öffentliche Schlüsselpaar ist $(e, N) = (7, 589)$. Verschlüsseln Sie die Nachricht mit dem Klartext $m = 25$.

3.2.2 Angenommen es wurde ein Verfahren gefunden, mit dem die Faktorisierung des Produktes zweier Primzahlen in annehmbarer Zeit ermittelt werden kann. Stellen Sie dar, wie mit Hilfe dieses Verfahrens und dem öffentlichen Schlüssel (e, N) ein abgefangener Geheimtext c entschlüsselt werden kann.

3.2.3 Erläutern Sie die Idee der digitalen Signatur anhand des RSA-Verfahrens.

Kryptologie

3.3 Das im Folgenden beschriebene One-Time-Pad-Verfahren (OTP-Verfahren) ist ein Verschlüsselungsverfahren zur geheimen Nachrichtenübermittlung. Kennzeichnend ist, dass ein Schlüssel verwendet wird, der so lang ist wie die Nachricht selbst.

Sei $n \in \mathbb{N}$.
Für $i \in \{0; \ldots; n-1\}$ werden beim OTP-Verfahren die einzelnen Zeichen m_i, c_i und s_i aus der Menge der Binärziffern gewählt, es gilt also $m_i \in \{0;1\}$, $c_i \in \{0;1\}$ und $s_i \in \{0;1\}$. Der Klartext $M = m_0 m_1 \ldots m_{n-1}$, der Geheimtext $C = c_0 c_1 \ldots c_{n-1}$ und der Schlüssel $S = s_0 s_1 \ldots s_{n-1}$ sind jeweils eine Folge von Binärziffern. Klartext M, Geheimtext C und Schlüssel S haben jeweils die gleiche Länge n.

Der Operator $\oplus$ heißt XOR-Verknüpfung zweier Binärziffern a und b.
Er ist wie folgt definiert:

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

Für jedes $i \in \{0; \ldots; n-1\}$ berechnet sich das Geheimtextzeichen c_i aus dem Klartextzeichen m_i und dem Schlüsselzeichen s_i wie folgt: $\boldsymbol{c_i = m_i \oplus s_i}$

3.3.1 Verschlüsseln Sie in der folgenden Tabelle den Klartext $M = 0110$ mit dem Schlüssel $S = 0011$ durch das beschriebene OTP-Verfahren.

Klartext M	0	1	1	0
Schlüssel S	0	0	1	1
Geheimtext C				

3.3.2 Man kann beim OTP-Verfahren zum Entschlüsseln den gleichen Algorithmus wie zum Verschlüsseln verwenden. Zeigen Sie, dass gilt:

$$\boldsymbol{m_i = c_i \oplus s_i, \text{für alle } i \in \{0; \ldots; n-1\}}$$

3.3.3 Entscheiden Sie, ob es sich beim OTP-Verfahren um ein symmetrisches oder ein asymmetrisches Verfahren handelt.

3.3.4 Mit dem beschriebenen OTP-Verfahren lassen sich Folgen von Binärziffern verschlüsseln. Beschreiben Sie eine Möglichkeit, wie das OTP-Verfahren zum Verschlüsseln von Zeichenfolgen über dem deutschen Alphabet $\Sigma = \{a, b, c, \ldots, z\}$ angewendet werden kann.

3.3.5 Beurteilen Sie die Praktikabilität des OTP-Verfahrens zur Verschlüsselung eines langen Textes, wie etwa dem Inhalt der Bibel.

3.1 Kryptologie

Alice und Bob möchten über den Diffie-Hellman-Schlüsselaustausch einen gemeinsamen Schlüssel für ihre Kommunikation vereinbaren. Sie wählen als öffentlich bekannte Primzahl $p = 13$ und als öffentlich bekannte Zahl $g = 2$.

3.1.1 Berechnen Sie den gemeinsamen Schlüssel, wenn Alice den geheimen Wert $a = 4$ wählt und Bob den geheimen Wert $b = 5$.

3.1.2 Alice will die öffentlich bekannte Zahl auf den Wert $g = 3$ ändern. Bob äußert Bedenken bezüglich der Sicherheit des Schlüsselaustauschs bei der Wahl von $g = 3$.
Bestätigen Sie, dass die Bedenken von Bob – unabhängig von der Wahl der geheimen Werte a und b – gerechtfertigt sind.

Die zu übertragenden Daten sollen nun mit dem RSA-Verfahren verschlüsselt werden.

3.1.3 Für das Verfahren wurden die Primzahlen $p = 17$ und $q = 23$ sowie die Zahl $e = 235$ festgelegt. Bestimmen Sie den privaten Schlüssel (d, N) und begründen Sie, dass die Zahl e korrekt gewählt wurde.

3.1.4 Entschlüsseln Sie die Nachricht $c = 15$ mit dem privaten Schlüssel $(5{,}493)$. Geben Sie alle wichtigen Schritte an.