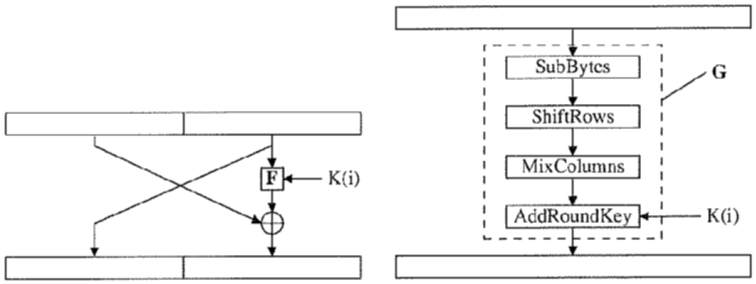
Aufgabe 1.
Kreuzen Sie für die folgenden Aussagen jeweils an, ob sie wahr oder falsch sind.
Für jede richtige Antwort gibt es einen Punkt, für jede falsche Antwort wird ein Punkt abgezogen. Für nicht beantwortete Fragen erhält man keine Punkte. Die minimale Gesamtpunktzahl für diese Aufgabe ist 0.

Aussage	**wahr**	**falsch**
Ist ein Kryptosystem $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$ perfekt sicher, dann sind die Zufallsvariablen $\hat{M}$ und $\hat{C}$ stochastisch unabhängig.	☐	☐
Im i-ten SBB des DES gilt: $R_i = L_{i-1} \oplus f(L_{i-1}, K_{i-1})$.	☐	☐
Die Rundenschlüssel im AES sind 128 Bits lang.	☐	☐
Wird der AES im CBC-Modus betrieben, so berechnet man die Kryptogrammblöcke mittels $C_i = \mathrm{AES}_K(M_i \oplus C_{i-1})$, $i \geq 1$.	☐	☐
Für die Euler-φ-Funktion gilt: $\varphi(p^2) = 2p$.	☐	☐
2 ist ein starker Zeuge dafür, dass 15 zusammengesetzt ist, d.h. $2 \in W(15)$.	☐	☐
2 ist eine Primitivwurzel modulo 15.	☐	☐
Die Berechnung des diskreten Logarithmus ist eine Einwegfunktion.	☐	☐
Gegeben seien eine Primzahl p und eine Primitivwurzel a sowie $a^x \mod p$ und $a^y \mod p$. Das Diffie-Hellman-Problem besteht darin, $xy \mod p-1$ zu berechnen.	☐	☐
Das Paar $(899, 37)$ ist ein geeigneter öffentlicher RSA-Schlüssel.	☐	☐

Aufgabe 2:



(a) Struktur 1 (b) Struktur 2

Abbildung 2.1: Strukturen für Blockchiffren

(a) Betrachten Sie die Strukturen in Bild 2.1. Nennen Sie jeweils ein Beispiel für Chiffren, in denen diese Strukturen eingesetzt werden.

(b) Welche elementaren Eigenschaften müssen die jeweiligen Funktionen F und G besitzen, um damit Blockchiffren entwickeln zu können? Welche Eigenschaften erhöhen die Sicherheit der Chiffren?

(c) Nun wird eine an DES angelehnte Chiffre betrachtet. Die Veränderungen sind:

- keine Expansion,

- es wird nur eine SBox genutzt, die 4 Eingangsbits auf 4 Ausgangsbits abbildet,
- XOR wird durch Addition von 4 Bites (mod 16) ersetzt,
- die Permutation (PBox) ist vereinfacht und arbeitet auf 4 Bit-Blöcken,
- keine Ein- und Ausgangspermutation,
- die Schlüsseladdition erfolgt nach der SBox.

Der Basisblock ist in Abbildung 2.2(a) dargestellt. Die SBox ist in Abbildung 2.2(d) spezifiziert. Für die einzelnen Rundenschlüssel wird wie folgt vorgegangen (Abbildung 2.2(c)):

- Rotation von K_l und K_r jeweils um eine Position (4 Bit) nach links,
- Wählen der Blöcke 0, 2, 4 und 6 von K_l und K_r als Rundenschlüssel.

Berechnen Sie auf dem Hilfsblatt (Abbildung 2.3) zwei Runden der dargestellten Chiffre für den Text $p = 0x31169dcef4d86c4a$ mit dem Schlüssel $K = 0x257b91278c7ab9$.

(d) In der vorgestellten Chiffre wird 8 mal die gleiche SBox genutzt. Welche Vor- und Nachteile bezüglich Implementation und Sicherheit hätte die Verwendung von unterschiedlichen SBoxen? Gelten diese Aussagen auch für die SubBytes Operation im AES?

Aufgabe 3.
Alice und Bob führen den Diffie-Hellman-Schlüsselaustausch mit der Primzahl $p = 107$ und der Primitivwurzel $a = 2$ durch. Alice wählt die Zufallszahl $x_A = 66$, und Bob wählt $x_B = 33$.

(a) Berechnen Sie den gemeinsamen geheimen Schlüssel.

(b) Zeigen Sie, dass auch $b = 103$ eine Primitivwurzel ist.

(c) Welcher gemeinsame Schlüssel ergibt sich, wenn Alice und Bob die Primitivwurzel 103 verwenden?

Aufgabe 4:
Alice schickt die Nachricht $c = 4675$, die sie mit dem RSA-Verfahren verschlüsselt hat, an Bob. Alice und Bob haben die öffentlichen RSA-Schlüssel $K_A = (n_A, e_A) = (4819, 2753)$ und $K_B = (n_B, e_B) = (6557, 3703)$. Wie lautet die Nachricht m, die Alice verschlüsselt hat?

Aufgabe 5:
Gegeben sei eine Blockchiffre E, die Nachrichten einer festen Länge k verschlüsselt und Blöcke der gleichen Länge als Schlüsseltext ausgibt. Die Verschlüsselung der Nachricht m mit dem Schlüssel $K \in \{0,1\}^k$ werde mit $E_K(m)$ bezeichnet. Betrachten Sie folgenden Algorithmus:

Input: Eine Nachricht $m \in \{0,1\}^*$
Output: Einen Bitstring $H(m) \in \{0,1\}^k$
Fülle m am Ende mit Nullbits auf, bis die Länge durch k teilbar ist
Teile m in Blöcke $(m_0, m_1, m_2, \ldots, m_n)$ der Länge k.
$c \leftarrow 000\ldots0 \in \{0,1\}^k$
for $(i \leftarrow 0; i \leq n; i++)$ **do**

$d \leftarrow E_{m_0}(m_i)$
$c \leftarrow c \oplus d$
end for
return $c = h(m)$

(a) Geben Sie eine geschlossene Darstellung für $H(m)$ an.

(b) Ist die Funktion H kollisionsresistent?

(c) Finden Sie ein Urbild zu $000\ldots0 \in \{0,1\}^k$.

(d) Ist die Funktion H kollisionsresistent, wenn im Algorithmus die Zeile $c \leftarrow c \oplus d$ durch $c \leftarrow c \wedge d$ ersetzt wird? Dabei ist $\wedge$ das bitweise logische UND.

(e) Nehmen Sie an, dass bei festem K und beliebig gewählter Nachricht $\tilde{m} \in \{0,1\}^k$ jedes Bit in $E_K(\tilde{m})$ mit Wahrscheinlichkeit $1/2$ gleich 1 ist. Bestimmen Sie für die Funktion aus (d) die Wahrscheinlichkeit dafür, dass das erste Bit in $H(m)$ gleich 0 ist in Abhängigkeit von der Anzahl n der Nachrichtenblöcke. Was passiert, wenn die Nachricht sehr lang ist?

Aufgabe 6.
Sie kennen die ElGamal-Signaturen $(r_1, s_1) = (3, 262)$ und $(r_2, s_2) = (3, 411)$ der Nachrichten m_1 und m_2. Die Hashwerte der Nachrichten lauten $h(m_1) = 123$ und $h(m_2) = 448$. Die dem ElGamal-System zugrundeliegenden öffentlichen Parameter sind die Primzahl $p = 509$ und die Primitivwurzel $a = 2$ modulo p.
Bestimmen Sie öffentlichen und privaten Schlüssel des Unterzeichners.
Aufgabe 7:

(a) Beschreiben Sie das in der Vorlesung behandelte Verfahren zum Werfen einer Münze über das Telefon. Welche Funktionen haben die einzelnen Schritte des Protokolls?

(b) Betrachten Sie folgendes Protokoll:

1. A wählt $p, q : p, q \pmod 4 \equiv 1$ oder $p, q \pmod 4 \equiv 3$. $N = p \cdot q$, sende N an B.
2. B: rate, ob $p, q \pmod 4 \equiv 1$ oder $p, q \pmod 4 \equiv 3$.
3. A: sende p, q an B.

Wenn B richtig geraten hat, gewinnt B, ansonsten gewinnt A. Welche Funktionen erfüllen die einzelnen Schritte? Auf welchem Problem basiert das Protokoll?

(c) Wie ließe sich das Werfen einer Münze mit Hilfe einer kryptografischen Einwegfunktion $y = h(x)$ realisieren?

(d) Nun soll eine Blockchiffre $y = E_k(x)$ genutzt werden. Das Protokoll ist wie folgt spezifiziert:

1. A und B vereinbaren einen Schlüssel k.
2. A wählt x, berechnet $y = E_k(x)$, sendet y an B.
3. B rät, ob x gerade oder ungerade ist.
4. A sendet x an B.

Wenn B richtig geraten hat, gewinnt B, ansonsten gewinnt A. Wie bewerten Sie die Fairness dieses Protokolls? Wie lässt sich das Protokoll verbessern?

Aufgabe 8.
Betrachten Sie die Kurvengleichung

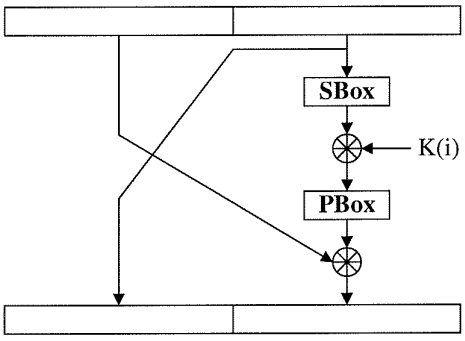
$$E_{a,b} : y^2 = x^3 + ax + b$$

mit $a, b \in \mathbb{F}_7$.

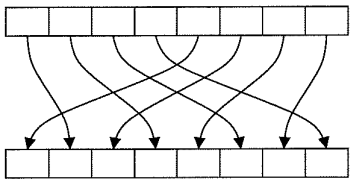
(a) Bestimmen Sie die Parameter a, b, die zu der Kurve gehören, auf der die Punkte $P_1 = (1, 1)$ und $P_2 = (6, 2)$ liegen. Definieren diese Parameter eine elliptische Kurve?

(b) Zeigen Sie, dass $E_{6,1}$ eine elliptische Kurve ist. Bestimmen Sie die Menge der $\mathbb{F}_7$-rationalen Punkte auf $E_{6,1}$ und geben Sie zu jedem Punkt P sein Inverses $-P$ an. Welchen Wert hat die Spur t von $E_{6,1}$?

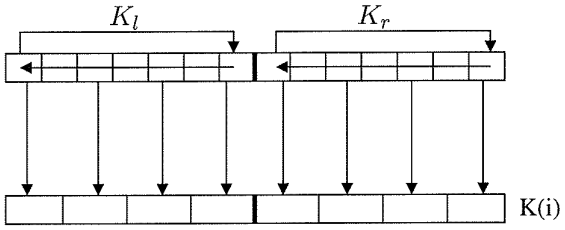
(c) Berechnen Sie $2P$ für $P = (0, 1)$ in $E_{2,1}(\mathbb{F}_7)$.



(a) Vereinfachter DES



(b) PBox



(c) Generierung der Rundenschlüssel

SBox								
IN	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7
OUT	0x4	0xe	0xf	0xd	0x1	0xc	0x3	0x2
IN	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
OUT	0x5	0x9	0x8	0x6	0xb	0xa	0x0	0x7

(d) SBox

Abbildung 2.2: Symmetrische Chiffre

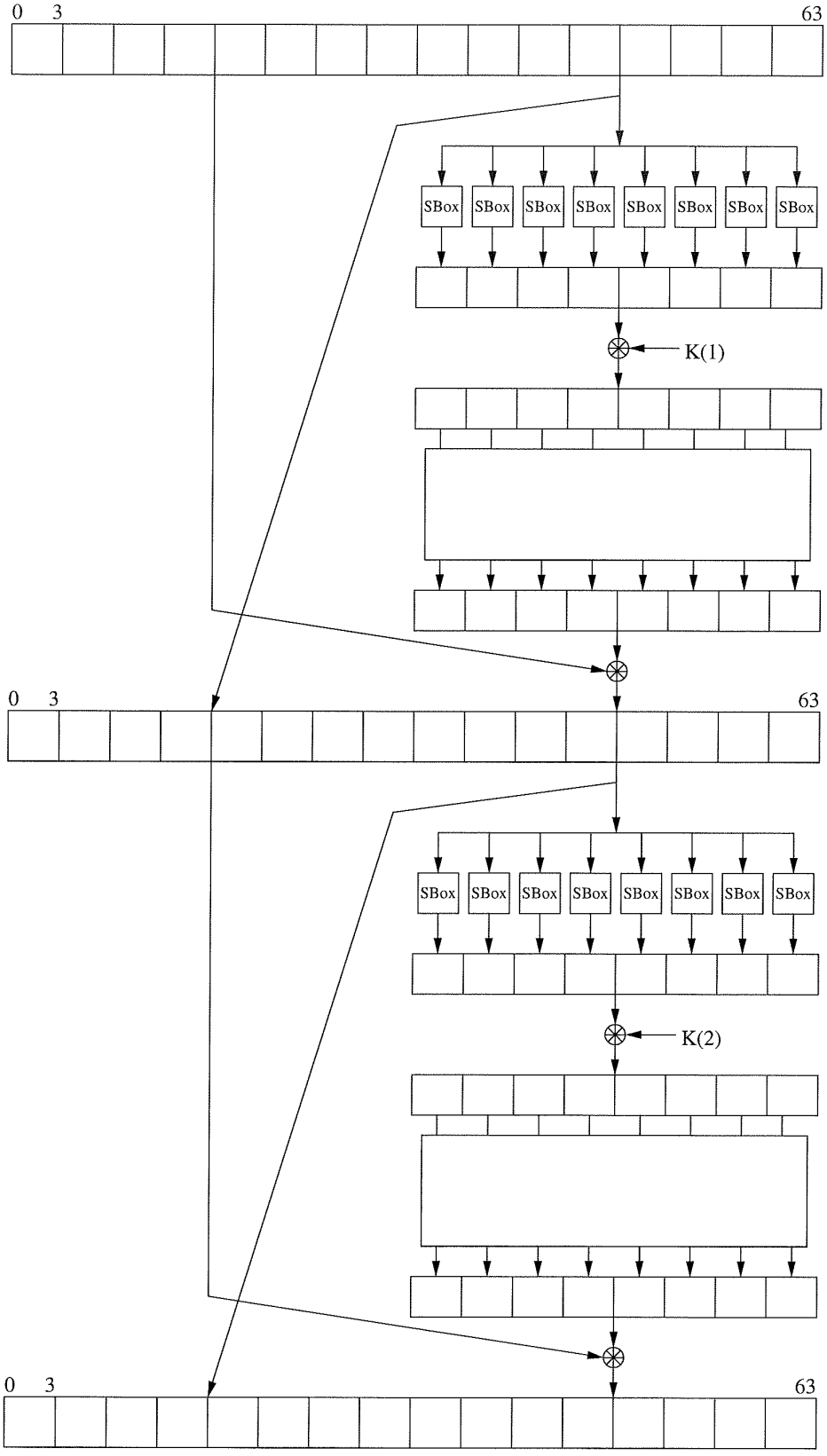


Abbildung 2.3: Zwei Runden der Chiffre