

## Übungsblatt 6

### Aufgabe 30

*mündlich*

- (a) Definieren Sie formal, wann zwei Kryptosysteme als gleich (besser: äquivalent) anzusehen sind. Betrachten Sie auch den Fall, dass Wahrscheinlichkeitsverteilungen auf den Schlüsselräumen gegeben sind.
- (b) Zeigen Sie, dass die affine Chiffre idempotent ist.

### Aufgabe 31

*mündlich*

Seien  $S_1$  und  $S_2$  Vigenère-Chiffren mit fester Schlüsselwortlänge  $d_1$  bzw.  $d_2$ .

- (a) Zeigen Sie: Ist  $d_1$  ein Teiler von  $d_2$ , so ist  $S_1 \times S_2 = S_2$ .
- (b) Lässt sich Teilaufgabe (a) verallgemeinern zu  $S_1 \times S_2 = S_3$ , wobei  $S_3$  die Vigenère-Chiffre mit Schlüsselwortlänge  $d = \text{kgV}(d_1, d_2)$  ist?

### Aufgabe 32

*mündlich*

Seien  $H_1, H_2$  und  $H_3$  Hill-Chiffren mit Blocklängen  $l_1, l_2$  und  $l_3$ .

- (a) Zeigen Sie, dass  $H_1 \times H_1 = H_1$  ist.
- (b) Was muss für  $l_1, l_2$  und  $l_3$  gelten, damit  $H_1 \times H_2 = H_3$  ist?  
Hierbei bezeichne  $H_1 \times H_2$  (abweichend vom Skript) die Chiffre mit Blocklänge  $\text{kgV}(l_1, l_2)$ , die erst  $H_1$  und dann  $H_2$  blockweise anwendet.

### Aufgabe 33

*mündlich*

Überlegen Sie, wie sich ein durch ein SPN verschlüsselter Kryptotext  $y = E_{f, \pi_s, \pi_P}(K, x)$  wieder zu  $x$  entschlüsseln lässt.

### Aufgabe 34

*mündlich*

Sei  $E$  die Chiffrierfunktion einer (binären) Blockchiffre  $S$  mit Blocklänge  $l$  und Schlüsselraum  $\{0, 1\}^k$ . Wir betrachten einen Angriff bei *bekanntem Klartext*, d. h. es steht eine ausreichende Zahl von Klartext-Kryptotext-Paaren  $(x_i, y_i), i = 1, \dots, t$ , zur Verfügung, die alle mit demselben unbekanntem Schlüssel  $K$  generiert wurden.

- (a) Bestimmen Sie heuristisch die erwartete Anzahl von Schlüsseln  $K$ , die zu allen Paaren  $(x_i, y_i)$  »passen«, d. h. es gilt  $E_K(x_i) = y_i$  für  $i = 1, \dots, t$ .

*Hinweis:* Gehen Sie davon aus, dass für einen zufällig gewählten Schlüssel  $K$  die Wahrscheinlichkeit  $\Pr[E_K(x) = y]$ , dass  $K$  einen gegebenen Klartext  $x$  durch den Kryptotext  $y$  chiffriert, gleich  $2^{-l}$  ist (selbst dann, wenn bereits bekannt ist, dass  $K$  gewisse Klartexte  $x_i \neq x$  durch gewisse Kryptotexte  $y_i$  chiffriert).

- (b) Wie lässt sich im Fall  $t \geq k/l$  der benutzte Schlüssel  $K$  mittels  $t2^k$  Verschlüsselungen bestimmen?
- (c) Um die Sicherheit zu erhöhen, wird nun das Kryptosystem  $S \times S$  verwendet, d. h. die Schlüssellänge verdoppelt sich auf  $2k$ . Zeigen Sie, dass sich dadurch die benötigte Anzahl  $t$  an Klartext-Kryptotext-Paaren  $(x_i, y_i)$  ebenfalls (auf  $2k/l$ ) verdoppelt.
- (d) Wie lässt sich im Fall  $t \geq 2k/l$  der benutzte Schlüssel  $(K, K')$  unter Verwendung eines Speichers der Größe  $(lt + k)2^k$  mittels  $t2^{k+1}$  Ver- und Entschlüsselungen bestimmen?
- (e) Überlegen Sie, wie sich der Platzbedarf in (d) auf Kosten der Rechenzeit reduzieren lässt. Suchen Sie nach einer möglichst allgemeinen Beziehung für diesen so genannten *Time-Memory-Tradeoff*.

### Aufgabe 35

**5 Punkte**

Bestimmen Sie für die durch folgende Permutation  $\pi_{S'}$  definierte S-Box  $S'$  sämtliche Werte  $L(a, b)$  für  $a, b \in \{0, 1\}^4$ .

$z$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_{S'}(z)$	8	4	2	1	C	6	3	D	A	5	E	7	F	B	9	0

### Aufgabe 36

**5 Punkte**

Seien  $X_1, X_2, X_3$  unabhängige Zufallsvariablen mit Wertebereich  $W(X_i) = \{0, 1\}$  und Bias  $\varepsilon_i = \varepsilon(X_i)$  für  $i = 1, 2, 3$ . Zeigen Sie, dass die Zufallsvariablen  $X_1 \oplus X_2$  und  $X_2 \oplus X_3$  genau dann unabhängig sind, wenn  $\varepsilon_1 = 0$  oder  $\varepsilon_3 = 0$  oder  $\varepsilon_2 = \pm 1/2$  ist.