Kryptologie – Wiederholung

Bearbeiten Sie die Aufgaben gemeinsam in einer Kleingruppe.

Aufgabe 1: Klären Sie in der Kleingruppe die Bedeutung der folgenden Begriffe:

- Kryptologie
- Kryptographie
- Kryptoanalyse
- Klartext
- Geheimtext
- Schlüssel
- verschlüsseln
- entschlüsseln
- „knacken“

Aufgabe 2: In Klasse 11 haben Sie das Prinzip der **Transposition** und der **Substitution** zur Verschlüsselung von Texten kennengelernt. Erläutern Sie die beiden Prinzipien und geben Sie jeweils ein Beispiel für ein entsprechendes Verschlüsselungsverfahren an.

Aufgabe 3:

a) Erläutern Sie anhand der angegebenen Zuordnungstabelle, was man unter einer **monoalphabetischen Substitution** versteht. Wie lautet der Geheimtext für den Klartext „sonne“?

Klar-textzeichen	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
Geheim-textzeichen	6	R	2	?	$	Z	1	b	8	!	Y	+	5	7	@	X	3	%	P	[	-	T	A	4	=	)

b) In Klasse 11 haben Sie das Prinzip der **Häufigkeitsanalyse** angewendet, um einen Geheimtext, der mit einer monoalphabetischen Substitution erstellt wurde, zu knacken. Beschreiben Sie das Vorgehen bei der Rekonstruktion eines Klartextes mithilfe einer Häufigkeitsanalyse.

c) Geben Sie Voraussetzungen an, die erfüllt sein sollten, damit eine Häufigkeitsanalyse gelingt.

Aufgabe 4: Begründen Sie, dass das Caesar-Verfahren unsicherer ist als eine monoalphabetische Substitution mit einer beliebigen Zuordnungstabelle. Gehen Sie dabei auf unterschiedliche Ansätze der Kryptoanalyse ein.

Aufgabe 5: In der Kryptologie spielt **Kerkhoffs‘ Prinzip** eine wichtige Rolle: Die Sicherheit eines Verschlüsselungsverfahrens darf nicht von der Geheimhaltung des Verfahrens abhängen, sondern nur von der Geheimhaltung eines Schlüssels.

a) Geben Sie Gründe dafür an, dass die Einhaltung von Kerkhoffs‘ Prinzip die Sicherheit und Nützlichkeit eines Verfahrens erhöht.

b) Welche Konsequenzen ergeben sich für die Kryptoanalyse bzw. die Einschätzung der Sicherheit eines Verfahrens, wenn davon ausgegangen werden kann, dass das Verfahren, mit dem ein Geheimtext erstellt wurde, bekannt ist?

Aufgabe 6*: Ein monoalphabetisches Substitutionsverfahren kann mithilfe einer Häufigkeitsanalyse geknackt werden. Sammeln Sie Ideen, wie ein Substitutionsverfahren sicherer gemacht werden kann, sodass der Angriff mit einer Häufigkeitsanalyse erschwert wird.