

Datenschutz und Datensicherheit / Systemsicherheit

2. Übung

1. Aufgabe:

Stellen Sie eine Tabelle für die Multiplikation bezüglich

- a) $(\text{mod } 3)$
- b) $(\text{mod } 4)$
- c) $(\text{mod } 5)$

auf. Was fällt im Hinblick auf die Invertierbarkeit der Multiplikation auf?

2. Aufgabe:

Berechnen Sie den diskreten Logarithmus von 5 zur Basis 3 $(\text{mod } 7)$, d.h. finden Sie die kleinste natürliche Zahl x , für die $3^x \equiv 5 \pmod{7}$ gilt.

3. Aufgabe:

Wir betrachten die Nachricht $m = (001101110100)$.

- a) Verschlüsseln Sie m im Electronic Codebook Mode (ECB) mit Blocklänge 2 und der Verschlüsselungsfunktion

$$E : \begin{array}{ll} 00 & \rightarrow 10 \\ 01 & \rightarrow 11 \\ 10 & \rightarrow 01 \\ 11 & \rightarrow 00 \end{array} .$$

Geben Sie die Entschlüsselungsfunktion D an.

- b) Benutzen Sie die Permutationschiffre um m zu verschlüsseln. Benutzen Sie den Schlüssel $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$. Zur Erinnerung: Die untere Zeile gibt die Reihenfolge der Ursprungsbits an. Zuerst Bit 3 des Klartextes, dann Bit 1, dann Bit 4 und schließlich Bit 2. Geben Sie die Entschlüsselungspemutation an.
- c) Verschlüsseln Sie m im Cipherblock Chaining Mode (CBC) mit Blocklänge 2, der Verschlüsselungsfunktion E aus Aufgabe a) und dem Initialisierungsvektor 01.

- d) Benutzen Sie den Cipher Feedback Mode (CFB) mit Blocklänge $r = 2$ mit dem Initialisierungsvektor 010 und der Verschlüsselungsfunktion

	000	→	101	
	001	→	110	
	010	→	111	
$E :$	011	→	000	
	100	→	101	.
	101	→	010	
	110	→	011	
	111	→	100	

4. Aufgabe:

Bei einem Chosen-Plaintext-Angriff wählt der Angreifer einen Klartext, „schiebt“ diesen dem Verschlüsselnden unter und erhält das Chiffre. Welche Auswirkungen hat dieses Szenario auf die Sicherheit des Schlüssels beim One-Time-Pad?