

## Sicherheit: Fragen und Lösungsansätze – Übung 6

### AUFGABE 1 (AES Verschlüsselungsverfahren) (45 Min, 10p):

In dieser Aufgabe wird die AES Verschlüsselung an einem Beispiel durchgeführt. Dabei wird die Schleife einmal durchlaufen (wenn man die finale unvollständige Anwendung hinzuzählt: 2mal).

1. Gegeben ist der initiale Schlüssel  $K_s$ . Führen sie die Expansion des Schlüssels für zwei Runden (eine vollständige und eine finale Runde durch).

Schlüssel				Runde 1				Runde 2			
F4	5D	51	18								
B4	9E	F4	98								
58	CD	5E	9C								
EA	A8	CF	A6								

(2P)

2. Gegeben ist ein Klartextblock der zu verschlüsselnden Nachricht  $m$ . Wählen sie den für die initiale Verknüpfung benötigten Schlüssel  $K_s$  aus. Führen Sie die initiale Verknüpfung mit dem Schlüssel  $K_s$  vor dem Rundenstart durch und tragen Sie das Ergebnis in die dazugehörige Zustandsmatrix 1 ein.

Klartext				$K_s$				Zustandsmatrix 1			
35	81	22	6B								
66	76	BB	7E								
AF	56	3E	60								
3E	50	B1	48								

(1P)

3. Für die Operation SubByte (Step (1) in den Folien) ist nun eine S-Box der Größe  $16 \times 16$  mit Werten in hexadezimaler Form gegeben (Folie Tabular representation of the substitution function). Mittels der S-Box ist nun die Operation auf obige Zustandsmatrix 1 anzuwenden. Im Ergebnis entsteht die Zustandsmatrix 2.

Zustandsmatrix 2			

(1P)

4. Führen Sie nun die ShiftRow Operation (Step (2) in den Folien) durch. Dabei wird in Abhängigkeit der Blocklänge eine Verschiebung des Inhalts der Zeilen durchgeführt. Für die Blocklänge von 32 Byte tragen Sie das Resultat in die Zustandsmatrix 3 ein.

Zustandsmatrix 3			

(1P)

5. Für die Operation MixColumn benötigen wir die abgebildete Konstantenmatrix A. Bestimmen Sie für die leer stehenden Felder der Zustandsmatrix 4 die entsprechenden Elemente und geben Sie die Lösungsschritte an. Hinweis : Die Elemente der Zustandsmatrix 4 ergeben sich durch Multiplikation der Zeilenvektoren der Konstantenmatrix A mit den entsprechenden Spaltenvektoren der Zustandsmatrix 3.

Konstantenmatrix				Zustandsmatrix 4			
02	03	01	01	BE		A5	26
01	02	03	01	16	16		31
01	01	02	03	20		12	1C
03	01	01	02	93	35	EE	D6

(2P)

6. Führen Sie den Schritt AddRoundKey (Step (4) in den Folien) durch. Wählen sie dafür den richtigen Schlüssel und tragen sie das Ergebnis in die Zustandsmatrix 5 ein.

Ks				Zustandsmatrix 5			

(1P)

7. Welche Schritte (z.B. MixColumn, ShiftRow, SubByte, AddRoundKey) werden in welcher Reihenfolge in der finalen Runde genutzt. Geben Sie die fertige Verschlüsselung in der Zustandsmatrix 6 an.

Zustandsmatrix 6			

(2P)