

Dozent: Prof. Dr. Michael Eichberg
Kontakt: michael.eichberg@dhbw.de, Raum 149B
Version: 1.0

1

1. AES - Grundlagen

2

Übung

1.1. Grundlagen

1. Was sind die Blockgröße und die typischen Schlüsselgrößen bei AES?
2. Welche vier Hauptoperationen werden in einem AES-Rundendurchlauf durchgeführt? Erläutern Sie kurz jede davon.
3. Was ist die Rolle des "Key Schedule" in AES? Wie viele Rundenschlüssel werden bei AES-128 erzeugt?
4. Wie unterscheidet sich AES-128 von AES-256 außer durch die Schlüssellänge?
5. Was versteht man unter "Diffusion" und "Konfusion"? Wie werden diese Konzepte in AES umgesetzt?



3

2. AES - rechnen

4

Rechenübung

2.1. AES durchführen


Nehmen wir an, dass der Zustand (*State*) folgendermaßen sei:


6A 59 CB BD
4E 48 12 A0
98 9E 30 9B
8B 3D F4 9B

Führen Sie die *Mix Columns Transformation* durch für das fehlende Feld ($S'_{0,3}$):

15 C9 7F ??
CE 4D 4B CB
89 71 BE 86
65 47 97 CA



 Nr.



1

2

3

4

5

6

7

8


9

<<

<

>

>>

 ?