Prof. Dr. Holger Schmidt
Professur für IT-Sicherheit, Informatik
Fachbereich Informatik – Fachhochschule Dortmund

Fachhochschule Dortmund
University of Applied Sciences and Arts

Übungsblatt 5 **Informationssicherheit SoSe 2023** Datum: 16.05.2023

Hinweis Zur Lösung der Aufgaben ist eine selbstständige Recherche notwendig, um ein genaues und über die Vorlesung hinausgehendes Verständnis zu entwickeln. Lesetipps:
- FIPS-197 [2023]
- Menezes et al. [2001]
- [Schmeh, 2016, Kapitel 8]: Downlad, aufgerufen am 3. Juli 2023
- Freiermuth et al. [2014]

Aufgabe 5.1 K20

Berechnen Sie den Wert für das erste Byte (erste Zeile, erste Spalte) der Ausgabe des AES Algorithmus vor (!) *AddRoundKey* am Ende der ersten Runde für die nachfolgend angegebenen Werte. Beachten Sie, dass das Whitening auf dem Klartext schon durchgeführt wurde.
Beachten Sie, dass die Multiplikationen in $GF(2^8)$ durchzuführen sind. Das zugehörige, irreduzible Polynom lautet $x^8 + x^4 + x^3 + x + 1$. Benennen Sie die jeweilige Phase des AES Algorithmus, berechnen Sie die Werte und geben Sie alle relevanten Zwischenergebnisse an, damit Ihr Rechenweg nachvollziehbar ist!

Tipp: Für die Berechnung des ersten Byte sind nicht alle eingehenden Bytes in den verschiedenen Schritten relevant. Ein genauer Blick auf $ShiftRows()$ und die nachfolgenden Schritte hilft Ihnen den Berechnungsaufwand zu minimieren.

Klartext $\bigoplus$ 0. Rundenschlüssel:

$1A$	23	06	13
$B2$	$E3$	17	04
32	18	FA	42
70	51	44	55

Verwenden Sie die S-Box und die Spaltenmixmatrix aus FIPS-197 [2023].

Aufgabe 5.2 K12

Berechnen Sie den ersten Rundenschlüssel nach der ersten Runde der Schlüsselaufbereitung von AES. Achten Sie darauf, dass Ihre Berechnung nachvollziehbar ist und geben Sie alle relevanten Zwischenergebnisse an.

0. Rundenschlüssel:

16	14	$C1$	48
12	10	$B5$	17
08	15	10	36
10	02	$A1$	27

Rundenkonstante RCON[1]: 0x01000000
Verwenden Sie die S-Box aus FIPS-197 [2023].

Prof. Dr. Holger Schmidt
Professur für IT-Sicherheit, Informatik
Fachbereich Informatik – Fachhochschule Dortmund

Aufgabe 5.3 K10

Ein Klartext von 56 Byte Länge wurde mit AES und 128 Bit Schlüssel verschlüsselt. Betrachten Sie den nun vorliegenden Geheimtext.

CTR Beantworten Sie folgende Fragen unter der Annahme, dass CTR benutzt wurde.

a) Wie lang ist der Geheimtext?

b) Welche Eingaben sind für die Entschlüsselung des Geheimtextes notwendig?

c) Im Geheimtext kippt ein Bit im 18. Byte. Welche Bytes können fehlerfrei entschlüsselt werden?

CBC Beantworten Sie folgende Fragen unter der Annahme, dass CBC und PKCS#7 benutzt wurde.

a) Wie viele Padding Bytes waren notwendig? Welche Werte haben die Padding Bytes?

b) Wie lang ist der Geheimtext?

c) Welche Eingaben sind für die Entschlüsselung des Geheimtextes notwendig?

d) Im Geheimtext kippt ein Bit im 18. Byte. Welche Bytes können fehlerfrei entschlüsselt werden?

Literatur

FIPS-197. Federal Information Processing Standards Publication (FIPS 197). Advanced Encryption Standard (AES), 2023. URL https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf.

Karin Freiermuth, Juraj Hromkovič, Lucia Keller, and Björn Steffen. *Einführung in die Kryptologie – Lehrbuch für Unterricht und Selbststudium*. 2nd edition, 2014. doi: 10.1007/978-3-8348-2269-7.

Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 5th edition, 2001. ISBN 0849385237. URL https://cacr.uwaterloo.ca/hac/.

Klaus Schmeh. *Kryptografie – Verfahren - Protokolle - Infrastrukturen*. dpunkt.verlag, 6 edition, 2016.