Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Prof. Dr. Helmut Reiser

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2024/2025
Übungsblatt 7

Besprechung: Do, 12.12.2024 um 14:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben ist es notwendig sich über den Vorlesungsinhalt hinaus, durch Internet- und Literaturrecherche mit dem Thema zu beschäftigen.

Aufgabe 1: (T) Substitution

a. Gegeben sei ein sehr simples Verschlüsselungsverfahren f, das auf *Substitution* basiert. Dabei wird jedes Zeichen des Klartextes auf einen Ciphertext abgebildet, der sich aus Zeilen- und Spaltennummer des Zeichens in untenstehender Tabelle ergibt.
Beispielsweise wird `vorlesung` somit zu `513442311543453322`.

- Wie lauten die beiden Alphabete A_1 und A_2 für $f : A_1^n \rightarrow A_2^n$?
- Handelt es sich dabei um ein symmetrisches oder asymmetrisches Verfahren?
- Verschlüsseln Sie den Klartext `uebung` mit f.
- Entschlüsseln Sie Ciphertext `31341543453322` mit f^{-1}.
- Das Verfahren manuell auszuführen ist aufwändig. Schreiben Sie sich ein kleines Script in einer Sprache Ihrer Wahl, um folgenden Text zu entschlüsseln: `152433 431323521542 5545 14151334142415421533141542 221523152432441553 44`

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

b. In der Kryptoanalyse ist die verwendete Verschlüsselungsfunktion oftmals nicht bekannt. Simple Tools wie `www.cryptool.org` können hier helfen. Entschlüsseln Sie folgenden Ciphertext, der mit einer bereits sehr alten Chiffre erstellt wurde:
`Inj Zjgzsl Ezw atwqjxzsl NY Xnhmjwmjny`

Aufgabe 2: (T) Einfache Chiffriermethoden & One Time Pads

Eines der zentralen Themen in der Informationssicherheit ist die Kryptographie. Neben den bekannten symmetrischen und asymmetrischen Verfahren gibt es zahlreiche, auch sehr einfache und dennoch effektive Methoden, die Vertraulichkeit von Informationen sicher zu stellen.

a. Ein sehr altes kryptographisches Verfahren ist *Skytale*, welches auch als Spaltentransformation bezeichnet wird. Der Geheimtext nach Anwendung der Transposition lautet FNABAIHUESNAFNSDUGKEESAL. Entschlüsseln Sie diesen und verwenden Sie hierbei eine Skytale mit einem Umfang U=5.

b. Neben additiven Chiffren (Caesar-Chiffre) existieren auch multiplikative Chiffren. Hierbei wird einem Buchstaben erst eine Zahl als Position im Alphabet (z.B. aufsteigend) zugeordnet und anschließend mit einem Schlüsselwert k multipliziert. Das Ergebnis gibt die entsprechende Position im Alphabet (A-Z) an. Verwenden Sie den Wert $k = 2$. Der Buchstabe O soll dabei auf den Buchstaben D abgebildet werden. Geben Sie die Berechnungsvorschrift an und berechnen Sie die passenden Werte für alle Buchstaben.
Was fälllt Ihnen bei dieser Substitution auf? Wie sollten Sie den Parameter k wählen, damit der beobachtete Effekt nicht auftritt?

c. One-Time-Pad gilt derzeit als eine der sichersten Verschlüsselungsmethoden. Geben Sie das Chiffrat, d.h. nach Anwendung des One-Time-Pads MISTGABEL für die Eingabe HALLOWELT an.

Aufgabe 3: (T) Advanced Encryption Standard (AES)

Leiten Sie den Wert für das 1. Byte (1. Zeile, 1. Spalte) der Ausgabe des Rijndael-Algorithmus (Block-/Schlüsselgröße 128 Bit) am Ende der 1. Runde für die nachfolgenden Werte her. 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 die **alle** relevanten Zwischenergebnissen an, damit Ihr Rechenweg nachvollziehbar ist!

Klartext: $\begin{pmatrix} 23 & 12 & 19 & 27 \\ 08 & 34 & 42 & 10 \\ 37 & 21 & 14 & 32 \\ 15 & 53 & 11 & 45 \end{pmatrix}$ 0. Rundenschlüssel: $\begin{pmatrix} 12 & 07 & 1A & 33 \\ 30 & 01 & 16 & 54 \\ 14 & 63 & 27 & 11 \\ 44 & 23 & 55 & 10 \end{pmatrix}$

Spaltenmixmatrix: $\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$

Verwenden Sie für ggf. durchzuführende Substitutionen folgende (fiktive) S-BOX:

	0	1	2	3	4	5	6	7	8
0	0x00	0x10	0x20	0x01	0x18	0x19	0xB4	0x45	0x2C
1	0x01	0x25	0xE1	0xCB	0x10	0x13	0xA7	0x3B	0x1A
2	0x2D	0xA1	0x40	0x89	0x9D	0x34	0x12	0x5E	0x2D
3	0x38	0xB4	0x2C	0x29	0x02	0xA6	0xF1	0x01	0x89
4	0x43	0xF2	0x20	0x30	0x40	0x02	0xD8	0x7B	0x6A
5	0xC4	0xA1	0x28	0x34	0xA2	0x09	0x7F	0x4D	0xC2
6	0x32	0x27	0x98	0x45	0x51	0x02	0xE4	0x89	0x2E
7	0xA6	0x2A	0x16	0x46	0x18	0x27	0xB3	0x1D	0xC8

In der ersten Key Expansion wurde folgender, erste Rundenschlüssel berechnet:

1. Rundenschlüssel: $\begin{pmatrix} 1A & 5A & EE & 18 \\ B7 & 87 & 26 & B4 \\ 41 & 51 & 43 & 45 \\ 19 & 39 & CA & 18 \end{pmatrix}$

Aufgabe 4: (H) Advanced Encryption Standard (AES)

Leiten Sie den Wert für das 1. Byte (1. Zeile, 1. Spalte) der Ausgabe des Rijndael-Algorithmus (Block-/Schlüsselgröße 128 Bit) am Ende der 1. Runde für die nachfolgenden Werte her. 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 die **alle** relevanten Zwischenergebnissen an, damit Ihr Rechenweg nachvollziehbar ist!

Klartext: $\begin{pmatrix} 17 & 21 & 03 & 06 \\ 08 & 43 & 24 & 16 \\ 33 & 12 & 41 & 23 \\ 51 & 37 & 11 & 35 \end{pmatrix}$ Schlüssel: $\begin{pmatrix} 11 & 22 & 33 & 44 \\ 2A & 33 & 44 & 11 \\ 32 & 44 & 11 & 22 \\ 44 & 11 & 22 & 33 \end{pmatrix}$

Spaltenmixmatrix: $\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$

S-BOX:

	0	1	2	3	4	5	6	7	8
0	0x00	0x10	0x20	0x01	0x18	0x19	0xB4	0x45	0x2C
1	0x01	0x25	0xE1	0xCB	0x10	0x13	0xA7	0x3B	0x1A
2	0x2D	0xA1	0x40	0x89	0x9D	0x34	0x12	0x5E	0x2D
3	0x38	0x40	0x2C	0x29	0x02	0x27	0xF1	0x01	0x89
4	0x43	0xF2	0x20	0x30	0x40	0x02	0xD8	0x7B	0x6A
5	0xC4	0xA1	0x28	0x34	0xA2	0x09	0x7F	0x4D	0xC2
6	0x32	0x27	0x98	0x45	0x51	0x02	0xE4	0x89	0x2E
7	0xA6	0x2A	0x16	0x46	0x18	0x27	0xB3	0x1D	0xC8

In der ersten Key Expansion wurde folgender erster Rundenschlüssel berechnet:

1. Rundenschlüssel: $\begin{pmatrix} 1A & 5A & EE & 18 \\ B7 & 87 & 26 & B4 \\ 41 & 51 & 43 & 45 \\ 19 & 39 & CA & 18 \end{pmatrix}$

Aufgabe 5: (H) Grundlagen Kryptographische Systeme

a. Wie definiert man allgemein ein kryptographisches System bzw. Kryptosystem? Welche Unterschiede bestehen hierbei zwischen einem symmetrischen und einem asymmetrischen Verfahren?

b. Erklären Sie die Begriffe bzw. Verfahren *Substitution* und *Permutation*? Welche der beiden Verahren setzt z.B. der bekannte symmetrische Verschlüsselungsalgorithmus DES ein? Falls Permutationen verwendet werden, würden Sie sagen, dass sich dadurch die Stärke des DES-Verfahrens erhöht? Verschlüsselungs- und Entschlüsselungsschritten erfolgt. Für die dabei verwendeten Schlüssel gibt es mehrere Möglichkeiten, die auch als *Keying options* bezeichnet werden. Nennen und erläutern Sie diese kurz.