IT-Sicherheit – Sicherheit vernetzter Systeme

Vorlesung im Wintersemester 2024/2025 (LMU)

12.12.2024
WS 2024/2025

Aufgabe 1: (T) Substitution

Übungsblatt 7:
Aufgabe 1: (T) Substitution

Verschlüsselungsverfahren *f*

+ Zeichen$_{ij}$ → ij
+ „m“ → 32
+ `vorlesung` (zeichenweise)
  → 51 34 42 31 15 43 45 33 22

	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

Übungsblatt 7:
Aufgabe 1: (T) Substitution

- Wie lauten die beiden Alphabete A1 und A2 für $f : A_1^n \rightarrow A_2^n$?
  - $A_1 = \{a,b,\ldots,z\}$ $(=Z_{25})$ (ohne „j“ für 5x5 Matrix ;))
  - $A_2 = \{1,2,3,4,5\}$

- Handelt es sich dabei um ein symmetrisches oder asymmetrisches Verfahren?
  - Gleicher „Schlüssel“/Abbildung zur Ver- und Entschlüsselung → Sym.

Übungsblatt 7:
Aufgabe 1: (T) Substitution

- Verschlüsseln Sie den Klartext uebung mit f.
  - 451512453322
- Entschlüsseln Sie Ciphertext 31341543453322 mit f^{-1}.
  - loesung

Übungsblatt 7:
Aufgabe 1: (T) Substitution

Beispielhaft in python

Output:

```
{' ': ' ', 'a': '11', 'b': '12',
'c': '13', 'd': '14', 'e': '15',
'f': '21', 'g': '22', 'h': '23',
'i': '24', 'k': '25', 'l': '31',
'm': '32', 'n': '33', 'o': '34',
'p': '35', 'q': '41', 'r': '42',
's': '43', 't': '44', 'u': '45',
'v': '51', 'w': '52', 'x': '53',
'y': '54', 'z': '55'}
```

Yes, we cheated! Leerzeichen hinzugenommen

```python
import string

# Substitutionstabelle/Dict erstellen
chars = []
for c in string.ascii_lowercase:
  chars.append(c)
chars.remove("j")

substitutionstabelle = {}
substitutionstabelle[" "] = " "
k = 0
for i in range(1,6):
  for j in range(1,6):
    substitutionstabelle[chars[k]] = "{}{}".format(i ,j)
    k+=1

print(substitutionstabelle)
```

Übungsblatt 7:
Aufgabe 1: (T) Substitution

```
# Verschluesselung
klartext = "uebung" # Klartext-String

ciphertext = ""
for b in klartext.lower():
  ciphertext += substitutionstabelle[b]

print(ciphertext)
```

Output:

451512453322

Übungsblatt 7:
Aufgabe 1: (T) Substitution

```
# Entschluesselung
reverse_table = { v: k for k,v in substitutionstabelle.items() } # k:v -> v:k

n = 2 # 2 Ciphertextzeichen werden auf 1 Klartextzeichen abgebildet
for worte in ciphertext.split(" "): # Leerzeichen sind nur 1 Zeichen, nicht im 2er-Raster
  for d in [str(worte[i:i+n]) for i in range(0,len(worte), n)]:
    # String in Liste an Zeichen-2er-Paaren umwandeln
      print(reverse_table[d], end="")
  print(" ", end="")
```

Output:

uebung

Übungsblatt 7:
Aufgabe 1: (T) Substitution

- Entschlüsseln Sie mit Ihrem Script:
- `152433 431323521542 5545 14151334142415421533141542 2215231524324415534 4`
- `Ein schwer zu decodierender Geheimtext`
- Wie schwer zu decodieren ist diese Chiffre wirklich?
  - Leerzeichen trennen Worte, keine Permutation, Häufigkeit der Zeichen, eindeutige Abbildungen, …

Übungsblatt 7:
Aufgabe 1: (T) Substitution

- 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`

- alle Verschlüsselungsverfahren einfach durchtesten…?
  - Aber Parametrisierung (Anzahl Runden, Key etc.)?

- www.cryptool.org Funktion Neural Cipher Identifier
  → Polyalphabetische Substitution

- Welche Substitutionschiffren gibt es (dort)?
  → Caesar Chiffre (Rotation) mit n = 5 (testen/spielen)
  - Klartext: `Die Uebung zur Vorlesung IT Sicherheit`

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

12.12.2024

WS 2024/2025

Übungsblatt 7:
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.

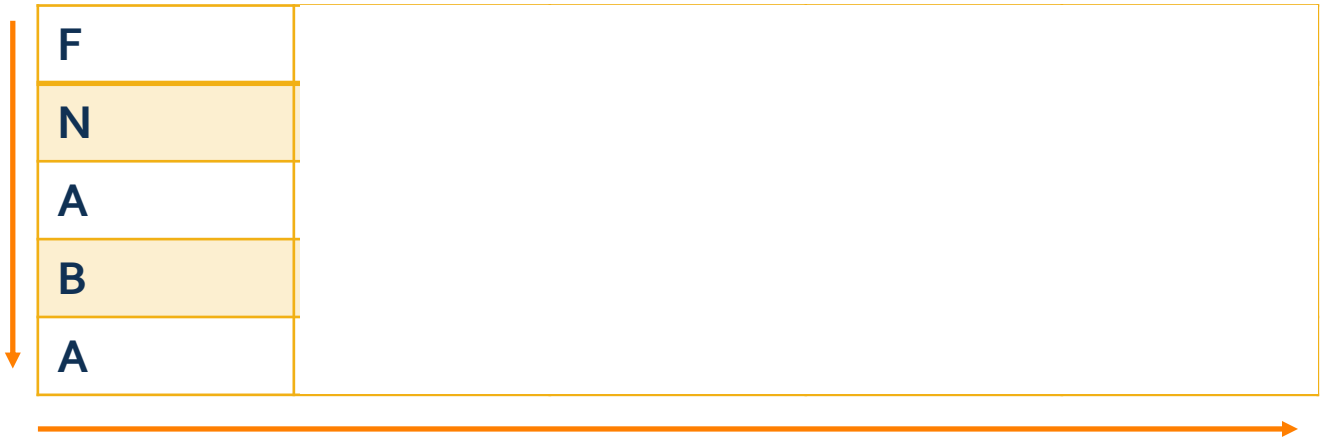
(a) Ein sehr altes kryptographisches Verfahren ist Skytale, welches auch als Spaltentransformation bezeichnet wird. Der Geheimtext nach Anwendung der Transposition lautet

FNABAIHUESNAFNSDUGKEESAL.

Entschlüsseln Sie diesen und verwenden Sie hierbei eine Skytale mit einem Umfang U=5.

Übungsblatt 7:
Aufgabe 2: (T) Einfache Chiffriermethoden & One Time Pads

FNABA IHUES NAFNS DUGKE ESAL



Übungsblatt 7:
Aufgabe 2: (T) Einfache Chiffriermethoden & One Time Pads

FNABA IHUES NAFNS DUGKE ESAL

F	I	N	D	E
N	H	A	U	S
A	U	F	G	A
B	E	N	K	L
A	S	S	E	

Übungsblatt 7:
Aufgabe 2: (T) Einfache Chiffriermethoden & One Time Pads

(b) Neben additiven Chiffren (Caesar-Chiffre) existieren auch multiplikative Chiffren. Hierbei wird einem Buchstaben erst eine Zahl 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 fällt Ihnen bei dieser Substitution auf? Wie sollten Sie den Parameter k wählen, damit dieser Effekt nicht auftritt?

Übungsblatt 7:
Aufgabe 2: (T) Einfache Chiffriermethoden & One Time Pads

A	B	C	D	E	F	G	H	I	J	K	L	M	
1	2	3	4	5	6	7	8	9	10	11	12	13	*Position*
2	4	6	8	10	12	14	16	18	20	22	24	0	*Abbildung*
B	D	F	H	J	L	N	P	R	T	V	X	Z	*Resultat*

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26
2	4	6	8	10	12	14	16	18	20	22	24	0
B	D	F	H	J	L	N	P	R	T	V	X	Z

Aufsteigende Zahlen
als Positionen im Alphabet.
Abbildung:
*(Position * k) mod Alphabetlänge*

Die Abbildung ist nicht eindeutig!
z.B. A → B und N → B
F → L und S → L

Das gewählte *k* muss teilerfremd zur Alphabetlänge (hier 26) sein.
(z.B. 3, 5, 7, 9, …)

Übungsblatt 7:
Aufgabe 2: (T) Einfache Chiffriermethoden & One Time Pads

(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.

Übungsblatt 7:
Aufgabe 2: (T) Einfache Chiffriermethoden & One Time Pads

Alphabet-Substitution:

- HALLOWELT: 8 1 12 12 15 23 5 12 20
- MISTGABEL: 13 9 19 20 7 1 2 5 12

- Chiffre: (HALLOWELT + MISTGABEL) mod 26

  21 10 05 06 22 24 07 17 06

- Alphabet-Substitution: **U J E F V X G Q F**

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

Übungsblatt 07:
Aufgabe 3: (T) Advanced Encryption Standard (AES)

Leiten Sie den Wert für das 1. Byte (1. Zeile, 1. Spalte) der Ausgabe des Rijndael-Algorithmus (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 alle relevanten Zwischenergebnisse an, damit Ihr Rechenweg nachvollziehbar ist!

Übungsblatt 07:
Aufgabe 3: (T) Advanced Encryption Standard (AES)

+ Klartext: $\begin{pmatrix} 23 & 12 & 19 & 27 \\ 08 & 34 & 42 & 10 \\ 37 & 21 & 14 & 32 \\ 15 & 53 & 11 & 45 \end{pmatrix}$

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

+ 0. Schlüssel: $\begin{pmatrix} 12 & 07 & 1A & 32 \\ 30 & 01 & 16 & 54 \\ 14 & 63 & 27 & 11 \\ 44 & 23 & 55 & 10 \end{pmatrix}$

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

Übungsblatt 07:
Aufgabe 3: (T) Advanced Encryption Standard (AES)

- Start AES (Rijndael – Algorithmus): Kopieren der Eingabe in Array „state“
- 1. Step: AddRoundkey (Vorrunde)

$$\begin{pmatrix} 23 & 12 & 19 & 27 \\ 08 & 34 & 42 & 10 \\ 37 & 21 & 14 & 32 \\ 15 & 53 & 11 & 45 \end{pmatrix} \otimes \begin{pmatrix} 12 & 07 & 1A & 32 \\ 30 & 01 & 16 & 54 \\ 14 & 63 & 27 & 11 \\ 44 & 23 & 55 & 10 \end{pmatrix} = \begin{pmatrix} 31 & 15 & 03 & 14 \\ 38 & 35 & 54 & 44 \\ 23 & 42 & 33 & 23 \\ 51 & 70 & 44 & 55 \end{pmatrix}$$

Übungsblatt 07:
Aufgabe 3: (T) Advanced Encryption Standard (AES)

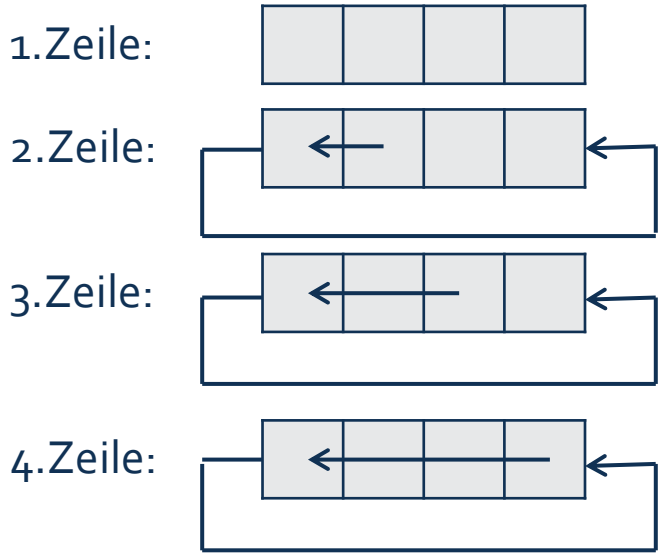
- 2. Step: SubBytes mithilfe der gegebenen S-Box
  Beispiel: Wert „06“: Zeile 0, Spalte 6 = B4

	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

$$\begin{pmatrix} 31 & 15 & 03 & 14 \\ 38 & 35 & 54 & 44 \\ 23 & 42 & 33 & 23 \\ 51 & 70 & 44 & 55 \end{pmatrix} \rightarrow \begin{pmatrix} B4 & 13 & 01 & 10 \\ 89 & A6 & A2 & 40 \\ 89 & 20 & 29 & 89 \\ A1 & A6 & 40 & 09 \end{pmatrix}$$

Übungsblatt 07:
Aufgabe 3: (T) Advanced Encryption Standard (AES)

- 3. Step: ShiftRows



$$\begin{pmatrix} B4 & 13 & 01 & 10 \\ 89 & A6 & A2 & 40 \\ 89 & 20 & 29 & 89 \\ A1 & A6 & 40 & 09 \end{pmatrix}$$

$$\downarrow$$

$$\begin{pmatrix} B4 & 13 & 01 & 10 \\ A6 & A2 & 40 & 89 \\ 29 & 89 & 89 & 20 \\ 09 & A1 & A6 & 40 \end{pmatrix}$$

Übungsblatt 07:
Aufgabe 3: (T) Advanced Encryption Standard (AES)

- 4. Step: MixColumns

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} * \begin{pmatrix} B4 & 13 & 01 & 10 \\ A6 & A2 & 40 & 89 \\ 29 & 89 & 89 & 20 \\ 09 & A1 & A6 & 40 \end{pmatrix} = \begin{pmatrix} A2 & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{pmatrix}$$

02 * {B4} + 03 * {A6} + 01 * {29} + 01 * {09} = A2

Übungsblatt 07:
Aufgabe 3: (T) Advanced Encryption Standard (AES)

- 4. Step: MixColumns

02 = 0000 0010 = x

{B4} = 1011 0100 = $x^7 + x^5 + x^4 + x^2$

$$x \bullet (x^7 + x^5 + x^4 + x^2) = x^8 + x^6 + x^5 + x^3 = 101101000$$

$$x^8 + x^4 + x^3 + x + 1 = \quad 100011011$$

0111 0011 = 73

Übungsblatt 07:
Aufgabe 3: (T) Advanced Encryption Standard (AES)

- 4. Step: MixColumns

03 = 0000 0011 = x + 1

{A6} = 1010 0110 = $x^7 + x^5 + x^2 + x$

$$((1+1)\ mod\ 2)x^2 = 0x^2$$

$$(x+1) \bullet (x^7 + x^5 + x^2 + x) = x^8 + x^6 + x^3 + x^2 + x^7 + x^5 + x^2 + x = 111101010$$

$$x^8 + x^4 + x^3 + x + 1 = \quad 100011011$$

→ 73 + F1 + 29+ 09 = A2

1111 0001 = F1

Übungsblatt 07:
Aufgabe 3: (T) Advanced Encryption Standard (AES)

- 5. Step: AddRoundkey

$$\begin{pmatrix} A2 & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{pmatrix} \otimes \begin{pmatrix} 1A & 5A & EE & 18 \\ B7 & 87 & 26 & B4 \\ 41 & 51 & 43 & 45 \\ 19 & 39 & CA & 18 \end{pmatrix} = \begin{pmatrix} B8 & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{pmatrix}$$