a)

Angriffsmodel	Beschreibung	Beispiel Szenario
Ciphertext-Only	Eve ist nur der Ciphertext bekannt	Nur verschlüsselte Zugangsdaten sind bekannt.
Known-Plaintext	Eve erhält zufällige Plaintext/Ciphertext Paare	Alice loggt sich auf ihrem Konto ein und surft auf bekanntem Teil von stud.ip
Chosen-Plaintext	Eve hat Zugriff auf ein Verschlüsselungsorakel, das beliebige Plaintexte verschlüsselt	Eve sendet eine Nachricht an Alice. Alice loggt sich ein und ruft Eve's Nachricht ab.
Chosen-Ciphertext	Eve hat Zugriff auf ein Entschlüsselungsorakel, das beliebige Ciphertexte entschlüsselt	Eve hat für begrenzte Zeit Zugriff auf Alice's Gerät mit verschlüsselter Sitzung (ohne bestehenden Login) und lässt sich manipulierte verschlüsselte Nachricht entschlüsseln. Alice kommt später wieder und loggt sich auf Webseite ein.

b) Die Sicherheit von kryptografischen Verfahren darf nur von der Geheimhaltung der Schlüsselabhängig sein, aber nicht von der Geheimhaltung des Verfahrens.

Security

SoSe 23

LV 4120, 7240

Übungsblatt 5

Aufgabe 5.1 (Angreifermodelle und Kerckhoffs Prinzip):

a) Nennen Sie die vier gängigsten Angreifermodel im Kontext von kryptoanalytischen Angriffen. Beschrieben Sie kurz die Modele

b) Erläutern Sie das Kerckhoffs Prinzip.

Die Sicherheit des Verfahrens muss auf der Geheimhaltung des Schlüssels beruhen anstatt auf der Geheimhaltung des Verfahrens

c) Welches Kriterium muss eine Chiffre erfüllen, damit es nach dem Prinzip von Kerckhoff erfüllt sein muss im Bezug auf Angreifermodelle.

Die Geheimhaltung des Schlüssels. Die Angriffsmodelle aus a) sind, auch im Besitz vieler Chipher- und Plaintextpaaren, wirkungslos.

Aufgabe 5.2 (Monoalphabetische und Polyalphabetische Substitution):

a) Wieviele mögliche Schlüssel gibt es für eine monoalphabetische Substitution?

€ 26 Buchstaben: 26 * 25 * 24 * ... * 1 = 26! (88 bits notwendig)

b) Schreiben Sie ein Programm in einer beliebigen Programmiersprache zum Ver- und Entschlüsseln einen beliebige Zeichenkette mit einer Vigenère-Chiffre.

Aufgabe 5.3 (Algebra):

Welche der folgenden Mengen sind Gruppen? Begründen Sie Ihre Aussage:

a) $<\mathbb{Z}, ->$ Ist keine Gruppe, da das Kommutativgesetz (a - b = b - a) mit dem Minusoperator nicht gilt.

b) $<\mathbb{N}, +>$ Ist keine Gruppe, da es keine 0 und damit auch kein neutrales Element bezüglich der Addition gibt.

c) $<\mathbb{N}_0, +>$ Ist keine Gruppe, da es kein inverses Element (a' = -a) gibt.Es existieren in N keine negativen Zahlen.

d) $<\mathbb{Z}, +>$

ist eine Gruppe, da es das Assoziativgesetz (a+b = b+a) erfüllt, ein neutrales Element (0) bezüglich der Addition besitzt und es ein additives Inversen (a' = -a) gibt. Sie ist auch eine abelsche Gruppe.

Eine nichtleere Menge G von Elementen a, b, c, ... heißt Gruppe, wenn in ihr eine Operation ∘ erklärt ist, die folgenden Axiomen genügt:

1. Die Operation ∘ ist assoziativ, d.h. für alle Elemente $a,\ b,\ c \in G$ gilt $a \circ (b \circ c) = (a \circ b) \circ c$.
2. Die Operation ∘ ist umkehrbar, d.h. zu beliebigen Elementen $a,\ b \in G$ sind die Gleichungen $a \circ x = b$ und $y \circ a = b$ (mit $x \in G$ und $y \in G$) lösbar.

Man nennt G eine abelsche Gruppe, wenn zusätzlich noch gilt:

3. Die Operation ∘ ist kommutativ, d.h. für alle $a,\ b \in G$ gilt $a \circ b = b \circ a$.

Aufgabe 5.4 (Inverse Elemen

Berechnen Sie die Inversen Elemente mi
Sie sich hierzu Kapitel 6.3.2 Der erweitert
tografie verständlich, 2016, Springer durc

a) Berechnen Sie $a = 7^{-1} \mod 29$.

b) Berechnen Sie $a = 23^{-1} \mod 29$.

c) Berechnen Sie $a = 7^{-3} \mod 29$.

```
a)
7 und 29 sind teilerfremd, daraus folgt: ggT(29, 7) = 1.
==> ggT(29, 7) = 1 = s*29 + t*7 = s*7 mod 29 mit den Startwerten r0 = 29 und r1 = 7.
29 = 4 * 7 + 1
7  = 7 * 1 + 0

1 = 29 - 4 * 7 = 1 * 29 - 4 * 7 mod 29

(-4 mod 29 = 25) :)

bzw.: a = 7^-1 mod 29
       -4 = 7^-1 mod 29
       29 - 4 = 25 = 7^-1 mod 29
b)
23 und 29 sind teilerfremd, daraus folgt ggt(29, 23) = 1.
==> ggT(29, 23) ) = 1 = s*29 + t*23 mit den Startwerten r0 = 29 und r1 = 23.
29 = 1 * 23 + 6
23 = 3 * 6  + 5
6  = 1 * 5  + 1
5  = 5 * 1  + 0

1 = 6 - 1 * 5
1 = 6 - 1 * (23 - 3 * 6)
1 = 6 - 1 * 23 + 3 * 6 = -1 * 23 + 4 * 6
1 = -1 * 23 + 4 * (29 - 1 * 23) = -1 * 23 + 4 * 29 - 4 * 23 = -5 * 23 + 4 * 29

-5 mod 29 = 24

c) a = 7^-3 mod 29 = (7^3)^-1 mod 29 = (343 mod 29)^-1 mod 29 = 24^-1 mod 29

29 = 1 * 24 + 5
24 = 4 * 5  + 4
5 =  1 * 4  + 1
4 =  4 * 1  + 0

1 = 5 - 1 * 4
1 = 5 - 1 * (24 - 4 * 5) = 5 - 1 * 24 + 4 * 5 = -1 * 24 + 5 * 5
1 = -1 * 24 + 5 * (29 - 1 * 24) = -1 * 24 + 5 * 29 - 5 * 24 = 5 * 29 - 6 * 24

-6 mod 29 = 23
```

Aufgabe 5.5 (Hill-Chiffre):

Ein affine Hill-Chiffre möge für die Schlüsselmatrix K die Blocklänge 2 sowie für die Berechnung den Modulus n = 26 verwenden:

$$c = (K \cdot p) \mod n$$

Darin bezeichnet der Vektor p den Klartext und der Vektor c den Ciphertext. Die folgende Botschaft:

UHUSQHKX

sei mit einem Hill-Kryptosystem und der Schlüsselmatrix K

$$K = \begin{pmatrix} -8 & -9 \\ -9 & -8 \end{pmatrix}$$

verschlüsselt. Die Zeichencodierung erfolge anhand nachstehender Codierungstabelle:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

a) Wie lautet die zugehörige Entschlüsselungsfunktion $D : c \rightarrow p$?

b) An welche Bedingung ist die Entschlüsselungsvorschrift D geknüpft und warum?

c) Wie lautet der Klartext?

a)
p = (K^-1 * c) mod n

b) Two complications exist in picking the encrypting matrix:

Not all matrices have an inverse. The matrix will have an inverse if and only if its determinant is not zero.

ggT(det(K), N) = 1. Der ggT der Determinante von K und N müssen invertierbar sein.

c) det(K) = 9, det(K)^-1 = 9^-1 = det(K)^-1 = 9^-1 mod 2626 = 2 * 9 + 8

Security Übung 5
Aufgabe 5c
Fortsetzung

$$A^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$$

$$= \frac{1}{\det(A)} \cdot A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} a & -b \\ -c & d \end{pmatrix}$$

$$= \cancel{\frac{1}{\det(A)}^{-1}}$$

$$= \det(A)^{-1} \begin{pmatrix} a & -b \\ -c & d \end{pmatrix} = 3 \cdot \begin{pmatrix} -8 & 9 \\ 9 & -8 \end{pmatrix}$$

$$= \begin{pmatrix} -24 & 27 \\ 27 & -24 \end{pmatrix} \Rightarrow \begin{pmatrix} -24 & 27 \\ 27 & -24 \end{pmatrix} \bmod 26 = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} = K^{-1}$$

$$\Rightarrow \cancel{K^{-1} \cdot c = \begin{pmatrix} -24 & 27 \\ 27 & -24 \end{pmatrix} \cdot \begin{pmatrix} 10 & 20 & 18 & 10 \\ 7 & 18 & 7 & 23 \end{pmatrix}}$$

$$= K^{-1} \cdot c = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 10 & 20 & 18 & 10 \\ 7 & 18 & 7 & 23 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 47 & 58 & 39 & 43 \\ 34 & 56 & 30 & 56 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 21 & 6 & 13 & 17 \\ 8 & 4 & 4 & 4 \end{pmatrix} \to \begin{pmatrix} V & G & N & R \\ I & E & E & E \end{pmatrix}$$

$\Rightarrow$ VIGENERE $= p \triangleq$ Klartext

[redacted]