

Vorlesung „Kryptographie I“ (Wintersemester 2024/2025)

10-ECTS-Klausur (3.3.2025, 10-12 Uhr, Hörsäle H11 und H12)

Anmerkungen:

- (1) Bearbeitungszeit: 90 Minuten.
- (2) Als Hilfsmittel ist nur ein Taschenrechner und das beliebige Blatt „Hilfen zur VIGENERE-Verschlüsselung“ erlaubt.
- (3) Zur Lösung einer Aufgabe gehören auch Darstellung des Lösungswegs und Begründungen.

Aufgabe 1: Erich findet eine verschlüsselte Nachricht, die vermutlich von seiner Freundin Friederike verfasst wurde, aber wohl nicht für ihn bestimmt ist:

CWWFR FOAME SRFYEEQHR,
HNQVZ GXGA VNM JG/SODH TQPHKTYKOY. ANE VNXLZJH VY QMJBG, WKEB AGU UVZ SUS
XSTYFEGGTG KZB SUHMFRELHZZV QNXS, NNF JVA VEF IOYUEXCO RY FQVRG IYK?
JAIYQ UENEYJS, VIVZS ABCNKS XVVQRRKIQV

Da ihn Verschlüsselungen reizen, versucht er, die Nachricht zu entschlüsseln. Eine MASC-Verschlüsselung schließt er schnell aus. Dann probiert er es mit VIGENERE - mit Erfolg.

- (1) Warum kann Erich schnell eine MASC-Verschlüsselung ausschließen?
- (2) Bestimme das verwendete VIGENERE-Schlüsselwort.
- (3) Entschlüsse die erste Zeile der Nachricht. Für wen ist die Nachricht eigentlich bestimmt?
- (4) Entschlüsse das sechste Wort der zweiten Zeile, also TQPHKTYKOY.

Aufgabe 2: Für $n = 3003202030032020300320203003202030042023$ gilt $2^{\frac{n-1}{2}} \equiv 8 \pmod n$.

- (1) Beschreibe den Miller-Rabin-Test zur Basis 2. Welche Ergebnisse sind möglich?
- (2) Was ist ℓ in der Zerlegung $n-1 = 2^\ell u$ mit $u \equiv 1 \pmod 2$?
- (3) Besteht n den Miller-Rabin-Test zur Basis 2?

(Hinweis: Zur Lösung der Aufgabe braucht man keinen Taschenrechner.)

Aufgabe 3: $N = 407427353$ ist eine RSA-Zahl.

- (1) Faktorisier N mit der Fermatschen Faktorisierungsmethode.
- (2) Bestimme die kleinste natürliche Zahl $e > 1$, sodass (N, e) ein öffentlicher RSA-Schlüssel ist.

Aufgabe 4: $(N, e) = (6011003, 2826353)$ ist ein öffentlicher RSA-Schlüssel. Der Kettenbruchangriff ist erfolgreich, der private Exponent d kommt im 3. Näherungsbruch von $\frac{e}{N}$ vor.

- (1) Bestimme den 0., 1., 2. und 3. Näherungsbruch von $\frac{e}{N}$.
- (2) Bestimme den privaten Exponenten d .
- (3) Bestimme $\varphi(N)$.

Aufgabe 5: Einem Diffie-Hellman-Schlüsselaustausch liegen $p = 59$ und $g = 2$ zugrunde. Die öffentlichen Schlüssel von Yvonne und Zoe sind $f_Y = 5$ und $f_Z = 10$.

- (1) Zeige, dass $g = 2$ eine Primitivwurzel modulo $p = 59$ ist.
- (2) Berechne den privaten Schlüssel von Yvonne oder Zoe.
- (3) Bestimme den gemeinsamen Diffie-Hellman-Schlüssel von Yvonne und Zoe.

Aufgabe 6: $(p, g, e) = (2027, 5, 11)$ ist ein privater ElGamal-Signatur-Schlüssel.

- (1) Bestimme den zugehörigen öffentlichen Schlüssel (p, g, f) .
- (2) Welche Formeln benötigt man zur Erstellung einer ElGamal-Signatur?
- (3) Signiere ein Dokument mit Hashwert $h = 543$ unter Verwendung der „Zufallszahl“ $z = 13$. Welche Signatur erhält man?
- (4) Welche Bedingungen müssen erfüllt sein, damit ein Zahlenpaar (b, c) als gültige Signatur der Person mit dem öffentlichen ElGamal-Signatur-Schlüssel (p, g, f) für ein Dokument mit Hashwert h akzeptiert wird?

Hilfen zur VIGENERE-Verschlüsselung:

Identifikation der Großbuchstaben A,...,Z mit den Zahlen 0,...,25:

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

Die „Addition“ $x + y \text{ mod } 26$ für Buchstaben:

$f(x,y)$	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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