Vorlesung „Kryptographie I“ (Wintersemester 2019/2020)

10-ECTS-Klausur (24.2.2020, 8:15-9:45, Hörsaal H11)

Anmerkungen:

(1) Als Hilfsmittel ist nur ein Taschenrechner erlaubt.
(2) Zur Lösung einer Aufgabe gehören auch Darstellung des Lösungswegs und Begründungen.
(3) Großbuchstaben werden in der Klausur in folgender Weise mit Zahlen identifiziert:

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

Aufgabe 1: Maximilian erhält von einem Freund folgende, vermutlich VIGENERE-chiffrierte Nachricht:

```
YODPB YOKBMOCWSR,
VOV UTBK XSZSRDH, QTSY UI VMPT UHM MOK EMEAFSAVOSGILIEZ OHLKKEBKX.
VOV JNEXUS EME SSEGE KZBWR XMISXN, QRBFWG PI ZBR KZBWR RYDSXHRVB?
NMRXS TKUKJGW, QVOVNXL
```

(1) Bestimme das zugehörige VIGENERE-Schlüsselwort.
(2) Wie heißt der Freund?

Aufgabe 2: Für $n = 123573112003$ gilt $6^{\frac{n-1}{2}} \equiv 6 \bmod n$.

(1) Beschreibe den Miller-Rabin-Test zur Basis 6. Welche Ergebnisse sind möglich?
(2) Besteht n den Miller-Rabin-Test zur Basis 6?
(3) Besteht n den Fermat-Test zur Basis 6?

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

Aufgabe 3: $N = 70286971$ ist eine RSA-Zahl.

(1) Faktorisiere N mit der Fermatschen Faktorisierungsmethode.
(2) Bestimme die kleinste natürliche Zahl $e > 1$, sodass (N, e) ein öffentlicher RSA-Schlüssel ist.
(3) Bestimme ein $d > 1$, sodass (N, d) ein zu (N, e) passender privater RSA-Schlüssel ist.

Aufgabe 4: Einem Diffie-Hellman-Schlüsselaustausch liegen $p = 67$ und $g = 2$ zugrunde. Die öffentlichen Schlüssel von Ute und Vera sind $f_U = 44$ und $f_V = 55$.

(1) Zeige, dass $g = 2$ eine Primitivwurzel modulo $p = 67$ ist.
(2) Berechne den privaten Schlüssel von Ute oder Vera.
(3) Bestimme den gemeinsamen Diffie-Hellman-Schlüssel k_{UV} von Ute und Vera.

Aufgabe 5: $(p, g, e) = (2017, 5, 11)$ ist ein privater ElGamal-Signatur-Schlüssel.

(1) Bestimme den zugehörigen öffentlichen Schlüssel (p, g, f).
(2) Signiere ein Dokument mit Hashwert $h = 12$ unter Verwendung der „Zufallszahl“ $z = 13$.
(3) 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?

Datei: ki_klausur_1.tex. Version vom 18.2.2020