Vorlesung „Kryptographie I“ (Wintersemester 2021/2022)

10-ECTS-Klausur (28.2.2022, 13:30-15:00, Hörsaal H11)

Anmerkungen:

(1) Neben dem Aufgabenblatt gibt es noch ein Blatt „Hilfen zur VIGENERE-Verschlüsselung“.
(2) Sonst ist als Hilfsmittel nur noch ein Taschenrechner erlaubt.
(3) Zur Lösung einer Aufgabe gehören auch Darstellung des Lösungswegs und Begründungen.

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

```
GWWFR FOAME RZSKIYAHGX,
MRZB XVRGBQ IAAC VSX OMZQ ZEHLFLWGMU. JTS NRSDXFF RH WABFB, OIAZ WPA IND SARR SFBLSK
BOXJRQHNLSK KCWTSQFR. WEOES EIVZIAZ WAVFVI ZUQU LENI WFXRDSFLIKISF.
ZVQZR ZRAVGKI, QQWAX NOTVLI ZMFVXLAZGW
```

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 PAUL schnell eine MASC-Verschlüsselung ausschließen?
(2) Bestimme das verwendete VIGENERE-Schlüsselwort.
(3) Entschlüssle die erste Zeile der Nachricht. Für wen ist die Nachricht bestimmt?
(4) Entschlüssle das sechste Wort der zweiten Zeile, also `ZEHLFLWGMU`.

Aufgabe 2: Die Dezimaldarstellung der Zahl $n = 2^{256} + 1$ ist

$$n = 115792089237316195423570985008687907853269984665640564039457584007913129639 * *,$$

wobei aber die letzten beiden Dezimalstellen „verlorengegangen“ sind.

(1) Berechne n mod 4.
(2) Was besagt der Satz von Euler über die Eulersche φ-Funktion?
(3) Berechne $\varphi(25)$.
(4) Berechne n mod 25.
(5) Bestimme die letzten beiden Dezimalstellen von n.

Aufgabe 3:

(1) Beschreibe den Miller-Rabin-Test zur Basis 2 für eine ungerade Zahl $n > 1$. Welche Ergebnisse sind möglich?
(2) Besteht $n = 2^{256} + 1$ den Miller-Rabin-Test zur Basis 2?

Aufgabe 4: $N = 407427353$ 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.

Aufgabe 5: $(N, e) = (5352499, 4860851)$ ist ein öffentlicher RSA-Schlüssel. 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 6: $(p, g, e) = (1999, 3, 13)$ ist ein privater ElGamal-Signatur-Schlüssel.

(1) Bestimme den zugehörigen öffentlichen Schlüssel (p, g, f). $f = 1170$
(2) Welche Formeln benötigt man zur Erstellung einer ElGamal-Signatur? ✓ $b = g^z \bmod p$, $c = \frac{1}{z}(h - be)$
(3) Signiere ein Dokument mit Hashwert $h = 1001$ unter Verwendung der „Zufallszahl" $z = 19$. Welche Signatur erhält man? 858, 707
(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?

$1 \leq b \leq p-1$, $g^h = f^b b^c \bmod p$