Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

WS 2018/19
5. Dez. 2018

Übungen zur Vorlesung Kryptographie

Blatt 8

Aufgabe 29

Sei $m \geqslant 5$ eine zu 6 teilerfremde natürliche Zahl. Man beweise mit Hilfe des quadratischen Reziprozitäts-Gesetzes für das Jacobi-Symbol

$$\left(\frac{3}{m}\right) = \begin{cases} +1 & \text{für } m \equiv \pm 1 \bmod 12, \\ -1 & \text{für } m \equiv \pm 5 \bmod 12. \end{cases}$$

Aufgabe 30

Seien $n \geqslant 2$ und $k \leqslant 2^n$ natürliche Zahlen mit $3 \nmid k$. Man beweise:

$$N := k \cdot 2^n + 1$$

ist genau dann prim, wenn

$$(*) \qquad 3^{(N-1)/2} \equiv -1 \bmod N.$$

(Ein Beispiel für eine solche Primzahl ist $N := 13 \cdot 2^{1000} + 1$.)

Anleitung. Zur Notwendigkeit der Bedingung benutze man Aufgabe 29.
Für die Umkehrung zeige man: Besitzt N einen Primteiler $q \mid N$ und gilt $(*)$, so hat das Element $3^k \bmod q$ in $(\mathbb{Z}/q)^*$ die Ordnung 2^n, insbesondere ist dann $2^n \leqslant q - 1$.

Aufgabe 31

Sei p eine Primzahl mit $p \equiv 3 \bmod 4$ und a eine ganze Zahl mit

$$\left(\frac{a}{p}\right) = 1.$$

a) Man zeige: Von den zwei Quadratwurzeln $x_{1/2} \in (\mathbb{Z}/p)^*$ von a modulo p hat genau eine die Eigenschaft, dass sie selbst ein Quadrat modulo p ist.

b) Diese eindeutig bestimmte Quadratwurzel wird gegeben durch

$$x := a^{(p+1)/4} \bmod p.$$

c) Sei $N := pq$, wobei $q \neq p$ eine weitere Primzahl mit $q \equiv 3 \bmod 4$ ist. Sei $a \in (\mathbb{Z}/N)^*$ ein Quadrat modulo N. Dann besitzt a vier Quadratwurzeln modulo N, wovon genau eine selbst ein Quadrat modulo N ist.

d) Sind x_1, x_2 zwei Quadratwurzeln von a mit $x_1 \neq \pm x_2 \bmod N$, so kann man daraus die Faktorzerlegung von N ableiten.

---

b.w.

Aufgabe 32

Die 320-Bit-Zahl N, hexadezimal

```
9962 F79B 4849 2E56 B41B FD78 59B0 746F 567E EF48
F6A0 0FAF A469 020C C2DA 4770 688D 6355 62AA 2365
```

sei der Modul eines *Blum-Blum-Shub Pseudo-Zufallsgenerators*, d.h. $N = pq$ mit Primzahlen $p \equiv q \equiv 3 \bmod 4$, $p \neq q$. Ausgehend von einem quadratischen Rest $z_0 := x^2 \bmod N$, $\gcd(x, N) = 1$, sei die Folge $(z_i)_{i \geqslant 0}$, $1 \leqslant z_i < N$, rekursiv definiert durch $z_{i+1} := z_i^2 \bmod N$. Diese Folge definiert eine Pseudo-Zufallsfolge von Bits $b_i := z_i \bmod 2$, die als One-Time-Pad verwendet werden kann.

Der folgende Geheimtext der Länge von 198 Bytes

```
4FEB C7FD 42DD 544E BB70 CD8F 2F39 77C1 4145 F5E7 0DF9 9180 C1FA FD74 38D9
0FD7 217D 8D5C 09BE 4C5A BD22 E7E4 ECAC 27CA F543 79A0 F7A6 AC9D 245A A0A0
9793 2B0F C09C 4AFE 328B E398 CB8D 15CC 7981 BC85 1541 BECB EA67 BD15 BB51
6C84 57D2 6B38 52AF 8F10 D0BA C3C1 1644 7A66 6402 CD84 D423 89BD 6D75 6510
49F4 2401 63BA 0A7A 158C 9C5B C198 562E 304A AEF5 7800 D66B B9AF E40B 0358
C9C4 3FC3 9DAB E300 06C4 12BB B7C0 E5B8 6DD8 B4B2 4DF5 F97D 9A07 294A 9103
F374 CB38 75A9 7AB2 23C1 288A 0064 9767 7463
```

entstand aus einem Klartext von 157 Bytes auf folgende Weise:

Die Bits $(b_i)_{0 \leqslant i < 1256}$ wurden zu einem One-Time-Pad der Länge 157 Bytes (= 1256 Bits) zusammengefasst. (Jeweils 8 Bits $\beta_0, \beta_1, \ldots, \beta_7$ ergeben ein Byte $\xi = \sum_{i=0}^{7} \beta_i \cdot 2^i$.) Das One-Time-Pad wurde durch bitweises XOR auf den Klartext addiert, was die ersten 157 Bytes des Geheimtextes liefert. Anschließend folgt ein Nullbyte und dann 40 Bytes, welche die Zahl z_{1256} in hexadezimaler Schreibweise (MSF, *most significant byte first*) darstellen.

Man bestimme z_0 und entschlüssele den Geheimtext.

Hinweis. Der Modul N ist mit dem $(p-1)$-Faktorisierungs-Algorithmus zerlegbar.