DMA - Serie 11

Pascale Welsch
13-204-821

① x = Anzahl Guezli

Für x gilt:

$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$
$x \equiv 1 \pmod 8$

Dieses System kann mit dem chinesischen Restsatz gelöst werden:

$m = 5 \cdot 7 \cdot 8 = 280$

i	m_i	a_i	$M_i = m/m_i$	$M_i \pmod{m_i}$	$y_i \equiv M_i^{-1} \pmod{m_i}$	$a_i \cdot M_i \cdot y_i$
1	5	3	56	1	1	163
2	7	2	40	5	3	+ 240
3	8	1	35	3	3	+ 105
						513

$x = 513 \bmod 280 \equiv 233 \pmod{280}$

$\Rightarrow$ Anna kauft 233 Guezli

② a) Wenn die Ordnung von $a \in \mathbb{Z}_p^*$ $p-1$ ist, dann ist die kleinste natürliche Zahl x, s.d. $a^x \equiv 1 \pmod p$ gerade $p-1$. D.h. $\forall x < (p-1)$ gilt $a^x \not\equiv 1 \pmod p$.
Da der kleine Fermatsche Satz besagt, dass die Folge $a^1, a^2, \ldots a^{p-1} \pmod p$ zyklisch ist, existiert somit für jedes $y \in \mathbb{Z}_p^*$ ein $x \in \mathbb{Z}_{p-1}$, s.d. $y \equiv a^x \pmod p$.

b) Da für jedes $a \in \mathbb{Z}_p^*$ gilt, dass $a^{p-1} \equiv 1 \pmod p$ und die Folge $a^1, a^2, \ldots a^{p-1} \pmod p$ zyklisch ist, gilt $a^x \equiv 1 \pmod p$ nur, falls x entweder $p-1$ oder ein Teiler davon ist, da sonst die Folge nicht zyklisch sein könnte.

③ a) i. $Enc((N,e),x) : \quad c := x^e \pmod N$

$c = 11^3 \bmod 15$

$11^1 \bmod 15 = 11$

$11^2 \bmod 15 = 1$

$11^3 \bmod 15 = 11 \quad \Rightarrow \underline{\underline{c = 11}}$

ii) $d := e^{-1} \pmod{\varphi(N)}$

$\varphi(N) = \prod_{i=1}^{n} (p_i - 1) \cdot p_i^{e_i - 1}$, p_i = Primfaktoren von N

$N = 3^1 \cdot 5^1$

$\varphi(N) = [(2) \cdot 3^0] \cdot [(4) \cdot 5^0] = 8$

$d \cdot 3 \equiv 1 \pmod 8 \rightarrow \underline{\underline{d = 3}}$

$3 \cdot 3 = 9 \equiv 1 \pmod 8$

b) N ist das Produkt zweier großer Primzahlen p und q.

$\varphi(N) = (p-1)\cdot(q-1)$ und $N = p \cdot q \Leftrightarrow p = \frac{N}{q}$

$\Rightarrow \varphi(N) = \left(\frac{N}{q} - 1\right)(q-1) = N - \frac{N}{q} - q + 1$

$\Leftrightarrow -q - \frac{N}{q} + N + 1 - \varphi(N) = 0 \quad | \cdot q$

$\Leftrightarrow -q^2 + q(N+1-\varphi(N)) - N = 0$

$$q_{1;2} = \frac{-(N+1-\varphi(N)) \pm \sqrt{(N+1-\varphi(N))^2 - 4 \cdot (-1) \cdot (-N)}}{-2}$$

Falls ein q negativ ist, kann man es ausschließen.
Danach kann $p = \frac{N}{q}$ berechnet werden