Bijlage D

Theoremata

Kleine stelling van Fermat

Stel p een priemgetal en a een positief natuurlijk getal waarvoor $\text{ggd}(a, p) = 1$. Dan is

$$a^{p-1} \stackrel{p}{=} 1$$

Algemene pseudorandomgenerator

$$x_{i+1} = (a \cdot x_i + c) \bmod m \qquad (i \in \mathbb{N})$$

Lehmer pseudorandomgenerator

Een Lehmer pseudorandomgenerator is een pseudorandomgenerator met m een priemgetal of een macht van en priemgetal, $c = 0$, $\text{ggd}(m, x_0) = 1$ en a geen nuldeler van $\mathbb{Z}_m$.

Voor een Lehmer pseudorandomgenerator met $m = 2^k$ ($k \in \mathbb{N}$, $k > 2$) is de maximale periode $\frac{m}{4}$. Als $a \stackrel{8}{=} \pm 3$, dan is de periode gelijk aan $\frac{m}{4}$.

Een Lehmer pseudorandomgenerator heeft maximale periode $m - 1$ indien m priem is en indien a een generator is voor $\mathbb{Z}_m$.

Hull–Dobell

De periode van een algemene pseudorandomgenerator is maximaal en gelijk aan m als en slechts als:

- $c \neq 0$,
- $\text{ggd}(c, m) = 1$,
- $a - 1$ is deelbaar door alle priemfactoren van m,
- $a - 1$ is deelbaar door 4 als m deelbaar is door 4.

RSA

Oorspronkelijk bericht: M
Geëncrypteerd bericht: C

- Kies 2 grote priemgetallen p en q en een exponent e met $\text{ggd}(e, (p-1)\cdot(q-1)) = 1$
- Bereken de inverse d van e modulo $(p-1)\cdot(q-1)$.
- Bereken $n = p \cdot q$. De publieke sleutel is (n, e).
- Encrypteer M: $C = M^e \bmod n$
- Decrypteer C: $M = C^d \bmod n$

Hulpstelling

Voor elke priemmacht $q = p^k$ is het product van alle monische irreduciebele veeltermen in $\mathbb{Z}_q[x]$ van graad d, met d een deler van n, exact gelijk aan $x^{q^n} - x$.

Rabin test

Voor f een monische veelterm van graad n met coëfficienten in $\mathbb{Z}_p$. Noem $p_1, p_2, \ldots, p_k$ de unieke priemdelers van n, en noem $n_i = \frac{n}{p_i}$, met $1 \leq i \leq k$. De veelterm f is ondeelbaar in $\mathbb{Z}_p[x]$ als en slechts als:

1. $\text{ggd}\left(f, x^{p^{n_i}} - x\right) = 1$, voor alle $1 \leq i \leq k$,
2. f deelt $x^{p^n} - x$.

Alternatieve versie van de Rabin test

Een monische veelterm f van graad n is irreduciebel in $\mathbb{Z}_p[x]$ als voor elke $0 < i \leq \frac{n}{2}$ geldt: $\text{ggd}\left(f, x^{p^i} - x\right) = 1$.