Das Pohlig Hellman Verfahren

$p=$ (große) Primzahl $\|$ $N=$ Klartext $|$ $N \in \mathbb{Z}_p^\times$ $\|$ $e,d=$ Schlüssel

Wähle $e \in \mathbb{N}$ mit $ggT(e, p-1) = 1$

Bestimme d mit:

$$ed \equiv 1 (mod\, p-1) \rightarrow ed - r(p-1) = 1$$

Verschlüsseln:

verschlüsselte Nachricht $\mathcal{C} = N^e$

Entschlüsseln:

$$\mathcal{C}^d = (N^e)^d = N^{ed} = N^{1+r(p-1)} = N^1 \cdot (N^{(p-1)})^r \overset{\text{satz von euler - fermat}}{=} N$$

Wähle p am bessten mit $\frac{p-1}{2}$ auch prim $\leftarrow$ sichere Primzahl

RSA-Verfahren:

$S =$ Sender $\mid$ $R =$ Empfänger $\mid$ $N =$ Nachricht $\mid$ $\mathcal{C} = N^e =$ Geheimtext

$e^d = N^{ed} \overset{!}{=} N$

(e, n) öffentlicher Schlüssel

$N \in \mathbb{Z}_n$

$c = N^e$

$e^d = N^{ed} \overset{!}{=} N$

kein vorheriger Schlüsselaustausch nötig $\rightarrow$ assymterisches Verfahren/public Key Verfahren

<u>Konstruktion der Schlüssel durch R:</u>

- große Primzahlen $p, q \approx 2^{1024}$

$p + -1, q + -1$ müssen große Primetiler haben.

Setze $n = p \cdot q$

$\rightarrow |\mathbb{Z}_N^\times| = |\{a \in 1, \ldots, n\}| ggT(a, n) = 1| = \varphi(n) = \varphi(pq) = (p-1)(q-1)$

Wähle $e \in \{1, \ldots, n\}$ und $ggT(e, \varphi(n)) = 1$

Besitmme d mit $ed \equiv 1 mod \varphi(n)$

geheim: $d, p, q, \varphi(n)$

Waum gilt $N^{ed} = N$?