Das Pohlig Hellman Verfahren

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

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

Bestimme d mit:

$$\begin{aligned} ed &\equiv 1 (mod\, p-1) \\ ed &= 1 + r(p-1) \\ 1 &= ed - r(p-1) \end{aligned}$$

Verschlüsseln:

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

Entschlüsseln:

$$\mathcal{C}^d = (\mathcal{N}^e)^d = \mathcal{N}^{ed} = \mathcal{N}^{1+r(p-1)} = \mathcal{N}^1 \cdot (\mathcal{N}^{(p-1)})^r \overset{\text{Satz von Euler - Fermat}}{\equiv} N$$

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

RSA-Verfahren:

Vorbereitung des Empfängers (Erzeugers der Schlüssel):

1. wähle große $p, q \in \mathbb{P}\ :\ p \neq q$ und $p \pm 1, q \pm 1$ müssen große Primteiler haben
2. setze $n = p \cdot q$
3. $\left|\mathbb{Z}_n^\times\right| = \left|\{a \in \{1, \ldots, n\} \mid ggT(a, n) = 1\}\right| = \varphi(n) = \varphi(p \cdot q) = (p-1)(q-1)$
4. wähle $e \in \{1, \ldots, n\}\ :\ ggT(e, \varphi(n)) = 1$
5. berechne $d\ :\ e \cdot d \equiv 1 (mod\, \varphi(n))$
6. veröffentliche Schlüssel (n, e)

Verschlüsselung des Senders:

$$\mathcal{C} \equiv \mathcal{N}^e\ (mod\ n)$$

Entschlüsselung des Empfängers:

$$\mathcal{N} \equiv \mathcal{C}^d\ (mod\ n)$$