

Primzahlen und ihr Nutzen für die Kryptographie

PHILIPP MORITZ

$$f_k(m) = m^a \pmod{n}$$

$$a = \prod_{k=1}^n p_k^{e_k}$$

$$a^{p-1} \equiv 1 \pmod{p}$$

$$a^b = \prod_{k=0}^n (a^{2^k})^{b_k}$$

$$m^{ed} \equiv m \pmod{n}$$