

RSA - מפתח

מחרת ההוכחה: יש מחרת הפונקציה f ויש f^{-1} ויש $\{0, \dots, n-1\}$

אם $n = pq$ (האורק n הוא מכפלה של שני מספרים ראשוניים)

אז $\phi(n) = (p-1)(q-1)$

1. נבחר e מספר טבעי גדול מ-1, p, q

2. נבחר d כך ש- $ed \equiv 1 \pmod{\phi(n)}$

3. נבחר $m \in \{0, \dots, n-1\}$ - מספר

4. $c = m^e \pmod{n}$ - מספר

מספר - פונקציה (ההפוך)

5. $m = c^d \pmod{n}$ - מספר

ההפוך $m \rightarrow m^e \pmod{n}$

ההפוך $m' \rightarrow m'^d \pmod{n}$

$p(S(m')) = m'$, $S(P(m)) = m$ אם $m \in \mathbb{Z}_n$

$S(P(m)) = S(m^e \pmod{n}) = (m^e)^d \pmod{n} = m^{ed} \pmod{n}$ ההפוך

אם $ed \equiv 1 \pmod{\phi(n)}$ אז $d = e^{-1} \pmod{\phi(n)}$ אם $m \in \mathbb{Z}_n$

$k \in \mathbb{N}$ אז $ed = 1 + k(p-1)(q-1)$