RSA

תהליך יצור המפתחות

1. בוחרים שני ראשוניים גדולים p, q – סודיים

2. חישוב של

$$n := pq$$

$$t := (p-1)(q-1)$$

3. בחירת מעריך e "הצפנה"

encryption

דרישות ל-e

$1 < e < t$

e ראשוני ל t

4. חישוב מעריך "הפענוח"

d: decryption

$1 < d < t$
d ראשוני
$de \equiv 1 \pmod{t}$

5. (e, n) המפתח הציבורי — מכריזים עליו לכולם

(d, n) המפתח הפרטי — רק המקבל יודע

שימוש במספרים ראשוניים

- לתרגם את המידע (לקסט פשוט)
- למספר טבעי m: $m < n$ — message
- **הצפנה:** $c := m^e \bmod n$ — ciphertext
- **פענוח:** $m = c^d \bmod n$ — משפט Euler
- תרגום של m לקסט פשוט

יסוד מתמטי – משפט Euler

למה $m = c^d \bmod n$?

משפט הקטן של P. Fermat עבור p ראשוני $x^{p-1} \equiv 1 \pmod p$

הכללה:

משפט (L. Euler) $x^{\varphi(n)} \equiv 1 \pmod n$

כאשר $\varphi(n)$ = כמות מספרים $1 \le k < n$: $\gcd(k,n) = 1$

הערה: עבור k, ℓ זרים, $\varphi(k\ell) = \varphi(k)\varphi(\ell)$

עבור p ראשוני $\varphi(p) = p - 1$