לכן

$m^{ed} = m^{1+k(p-1)(q-1)} = m \cdot m^{k(p-1)(q-1)}$

<u>משפט Fermat הקטן</u>: יהי p ראשוני ויהי a שאינו מתחלק ב-p מתקיים $p | a^{p-1} - 1$. ניסוח אחר: לכל $0 \neq a \in Z_p$ מתקיים $a^{p-1} = 1 \mod p$.

נניח m זר ל-n (אינו כפולה של p, q) מתקיים

$m^{k(q-1)(p-1)} = (m^{p-1})^{k(q-1)} = 1^{k(q-1)} (\mod p) = 1 \mod p$

באותו אופן $m^{k(q-1)(p-1)} = 1 \mod q$ ולכן $pq | m^{k(q-1)(p-1)} - 1$

ולכן $m^{k(q-1)(p-1)} = 1 \mod n \Rightarrow m^{ed} = m \mod n$ ■

<u>היבטים אלגוריתמיים:</u>

1. בחירת e אי זוגי וזר ל-$\varphi(n)$ וקטן - ההצפנה פשוטה (העלאה בחזקת מספר קטן יחסית). (אורך הראשוניים עד 1000 בדוק זר ל-$\varphi(n)$).
2. בחירת $d = e^{-1} (\mod \varphi(n))$. כלומר d הוא ההופכי של e בחבורה $Z^*_{\varphi(n)}$ (איך בוחרים: כיוון ש-e זר ל-$\varphi(n)$ קיימים וניתנים למציאה ביעילות מס' שלמים x, y כך ש- $xe + y\varphi(n) = 1$ נבחר $d = x \mod \varphi(n)$).

<u>הערה</u>: הן ההצפנה והן הפענוח בשיטת RSA הן יעילות. אם β הוא אורך הייצוג הבינארי של n מתקיים ש- ההצפנה עולה $O(\beta^2)$ פעולות והפענוח עולה $O(\beta^3)$ פעולות ביט.

• ניסוח אסימפטוטי לצפיפות מס' ראשוניים בין 1 ל-x: $\pi(x) =$ מס' הראשוניים הקטנים מ-x; $\pi(x) \sim x/\ln(x)$ ולכן $\pi(1000) \geq \frac{1000}{\ln 1000} \geq 200$

זאת הסיבה שקל למצוא d בהתאם לדרישות שהצגנו.

כדי לשבור את ההצפנה מספיק לדעת את $\varphi(n)$, לשם כך צריך לדעת את $p, q \Leftarrow$ הפירוק של n. (לשבור את ההצפנה $\Rightarrow$ לדעת את d)