שם: שחר אשר
ת.ז. 209305408

מבוא להצפנה – תרגיל 5

.1

~~נסביר איך בעזרת הרעיון של חתימה עיוורת ניתן לקבל זיוף סלקטיבי של חתימה RSA עם התקפת הודעה נבחרת.~~

~~**הסבר:**~~

~~כאשר x היא ההודעה המקורית ו- (n,e) הוא המפתח הציבורי ו- m היא ההודעה המוצפנת.~~

~~את החתימה בוב מבצע על ידי:~~

$$\cancel{t^d = (mk^e)^d \bmod n}$$

~~ולאחר מכן אליס מחשבת את החתימה על ידי:~~

$$\cancel{s = \frac{t^d}{k} = m^d \bmod n}$$

~~כאשר $1 \le k \le n$.~~

~~כאשר משתמשים פעמיים באותו מפתח (n,e) RSA להצפנה ולחתימה, אנו מקבלים:~~

$$\cancel{m = x^e \bmod n}$$

~~לאחר מכן, אליס מחשבת את:~~

$$\cancel{t = mk^e = x^e k^e \bmod n}$$

~~כאשר $1 \le k \le n$.~~

~~כאשר בוב מבצע את החתימות הוא מחשב:~~

$$t^d = (mk^e)^d = (x^e k^e)^d = xk \bmod n$$

שם: שחר אשר
ת.ז. 209305408

2.

א.

תיאור הבדיקה של בוב את החתימה בעזרת המפתח הציבורי של אליס:

$$\delta = (a\gamma + kx) mod (p-1)$$

$$\Leftrightarrow \alpha^{\delta} = \alpha^{(a\gamma+kx)} \; mod \; p$$

$$\Leftrightarrow \alpha^{\delta} = \alpha^{a\gamma}\alpha^{kx} \; mod \; p$$

$$\Leftrightarrow \alpha^{\delta} = (\alpha^{a})^{\gamma}(\alpha^{k})^{x} \; mod \; p$$

$$\Leftrightarrow \alpha^{\delta} = (\beta)^{\gamma}(\gamma)^{x} \; mod \; p$$

החתימה תקינה אם: $\alpha^{\delta} = (\beta)^{\gamma}(\gamma)^{x} \; mod \; p$.

שם: שחר אשר
ת.ז. 209305408

ב.

ניתן לראות ש- γ זהה בשתי החתימות, והערך של γ הוא – 738.
זה אומר שאליס השתמשה באותו k לחתימת שתי ההודעות.

נראה מה קורה כאשר אליס משתמש באותו k:

$$\begin{cases}\delta_1 = (a\gamma + kx_1) mod(p-1) \\ \delta_2 = (a\gamma + kx_2) mod(p-1)\end{cases}$$

$$\Leftrightarrow \delta_1 - \delta_2 = kx_1 - kx_2 \; mod(p-1)$$
$$\Leftrightarrow \delta_1 - \delta_2 = k(x_1 - x_2) mod(p-1)$$

קיבלנו משוואה עם נעלם אחד k. יש לה $gcd(x_1 - x_2, p-1)$ פתרונות.

נציב בשביל למצוא את הפתרונות:

$$\delta_1 - \delta_2 = k(x_1 - x_2) mod(p-1)$$
$$508 - 58 = k(503 - 455) mod(1230)$$
$$450 = 48 \cdot k \; mod(1230)$$
$$8^{-1} \cdot 75 = 8^{-1} \cdot 8 \cdot k \; mod(205)$$
$$35 = k \; mod(205)$$

$$k = 35, 240, 445, 650, 855, 1060 \; mod(1230)$$

נציב כעת ב- $a^{\mathrm{k}} \; mod \; p$ ונבדוק אם שווה ל- $\gamma = 738$.

$$3^{\mathrm{k}} \; mod \; p$$

$$493 = 3^{35} \; mod \; p$$

$$1061 = 3^{240} \; mod \; p$$

$$568 = 3^{445} \; mod \; p$$

$$738 = 3^{650} \; mod \; p$$

ולכן, המפתח הסודי של אליס הוא – 650.

שם: שחר אשר
ת.ז. 209305408

.3