שיעור 8 צופן אל-גמאל

הגדרה 8.1 צופן אל-גמאל

 $a\in\{2,3,\dots,p-2\}$ ויהי ווצר של $\left(\mathbb{Z}_p^*, imes_p
ight)$ ויהי ווצר lpha מספר ראשוני (גדול), מספר חוצר של וואר וואר $P=\mathbb{Z}_p^*$ נגדיר קבוצת מפתחות יהי הקבוצת טקסט גלוי וואר וואר וואר וואר וואר מפתחות

$$K = \{ (p, \alpha, a, \beta) \mid \beta = \alpha^a \mod p \} .$$

נגדיר $d=\{2,3,\ldots,p-2\}$ רו $(y_1,y_2)\in P$ גדיר גדיר וגדיר $d=\{2,3,\ldots,p-2\}$

$$e_k\left(x,d\right) = \left(y_1, y_2\right)$$

-1 $y_2=eta^dx \mod p$, $y_1=lpha^d \mod p$ כאשר

$$d_k(y_1, y_2) = (y_1^a)^{-1} y_2 \mod p$$
.

מפתח סודי. a מפתח סודי. מפתח סודי.

משפט 8.1 צופן אל-גמאל צופן חוקי

אם $a\in\mathbb{Z}_p^*$ -ו $eta=lpha^a\mod p$, $a\in\{2,3,\dots,p-2\}$, $\left(\mathbb{Z}_p^*, imes_p\right)$ אז לכל $a\in\{2,3,\dots,p-2\}$ $d\in\{2,3,\dots,p-2\}$ $\left(\left(lpha^d\right)^a\right)^{-1}\beta^dx=x\mod p\ .$

הוכחה: תרגיל בית.

כלל 8.1 אלגורים הצפנת אל-גמאל

(B) שולחת הודעה לבוב ((A)

שלב הרכבת המפתח

- $(\mathbb{Z}_p^*, imes_p)$ איוצר מספר ראשוני גדול p ויוצר p וווצר מספר ווצר B 1
 - $a \in \{2,3,\ldots,p-2\}$ בוחר באקראי שלם B 2
 - $.eta=lpha^a\mod p$ -פך שכ B 3
- . בכתובת על a כמפתח שומר ציבורית בכתובת בכתובת על (p,α,β) כמפתח אומר את שומר שומר B

שלב הצפנה

- . איס את המפתח איבורי מהכתובת איבורי (p, α, β) אליס את את קוראת את אליס (A) אליס
 - $d\in\{2,3,\ldots,p-2\}$ שלם באקראי אבוחרת A 6
- $y_2 = eta^d x \mod p$ ו- $y_1 = lpha^d \mod p$ מחשבת (A) אליס אליס (x < p כדי להצפין הודעה x כדי להצפין הודעה (x < p

B -שולחת הטקסט מוצפן (y_1,y_2) ל- 8

 $x=\left((y_1)^a\right)^{-1}y_2$ את כדי לפענח הסודי a משמש המפתח משמש מוצפן (y_1,y_2) מוצפן פרי לפענח את את מחסו p

דוגמה 8.1 הצפנת אל-גמאל

נניח כי אליס שולחת הטקסט גלוי x=123. בוב בוחר במספר ראשוני p=727, יוצר $\alpha=80$ ומפתח סודי a=6. אליס בוחרת ב- a=6. מצאו את הטקסט מוצפן.

פתרון:

$$\beta=\alpha^a\mod p=80^6\mod 727=514\ .$$

$$y_1=\alpha^d\mod p=80^7\mod 727=408\ ,\qquad y_2=\beta^dx\mod p=514^7\cdot 123\mod 727=390\ .$$

דוגמה 8.2 הצפנת אל-גמאל

נניח כי בוב מקבל את הטקסט מוצפן $(y_1,y_2)=(408,390)$. בוב בחר במספר ראשוני p=727 יוצר גניח כי בוב מקבל את הטקסט מוצפן .a=6 ומפתח סודי a=6 . ואליס בחרה ב- a=6 פענחו את הקטסט מוצפן.

פתרון:

$$\beta=\alpha^a\mod p=80^6\mod 727=514\ .$$

$$x=\left(\left(y_1^a\right)^{-1}\right)y_2\mod p=\left(\left(480^6\right)^{-1}\right)\cdot 390\mod 727$$

בעזרת משפט פרמה,

$$\left(408^6\right)^{-1} \mod 727 = 408^{727-1-6} \mod 727 = 408^{720} \mod 727 = 375 \ .$$