

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:

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

ולאחר מכן אליס מחשבת את החתימה על ידי:

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

כאשר $1 \leq k \leq n$.

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

$$m = x^e \bmod n$$

לאחר מכן, אליס מחשבת את:

$$t = mk^e = x^e k^e \bmod n$$

כאשר $1 \leq k \leq n$.

כאשר בוב מבצע את החתימות הוא מחשב:

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

.2

.א

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

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

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

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

$$\Leftrightarrow \alpha^\delta = (\alpha^a)^\gamma (\alpha^k)^x \bmod p$$

$$\Leftrightarrow \alpha^\delta = (\beta)^\gamma (\gamma)^x \bmod p$$

החתימה תקינה אם: $\alpha^\delta = (\beta)^\gamma (\gamma)^x \bmod p$.

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 :

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

$$\Leftrightarrow \delta_1 - \delta_2 = kx_1 - kx_2 \bmod (p-1)$$

$$\Leftrightarrow \delta_1 - \delta_2 = k(x_1 - x_2) \bmod (p-1)$$

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

נציב בשביל למצוא את הפתרונות:

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

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

נציב כעת ב- $a^k \bmod p$ ונבדוק אם שווה ל- $\gamma = 738$.
 $3^k \bmod p$

$$493 = 3^{35} \bmod p$$

$$1061 = 3^{240} \bmod p$$

$$568 = 3^{445} \bmod p$$

$$738 = 3^{650} \bmod p$$

.3

.א

```
////////////////////////////////////
-----
b = 4524
-----

number b = 4524 have roots modulo n = 10117 iff he have roots modulo p
= 67 and q = 151

=====
by 67:
-----
temp_b = 4524
-----
so -  $4524 = 35 \bmod 67$ .
so - 35 is root modulo 67 iff he is the root of:  $\rightarrow$ 
 $35^{((67+1)/4)} = 54 \bmod 67$ .
We will check if  $54^2 = b \bmod 67 \rightarrow$ 

 $54^2 = 35 \bmod 67$ .
and that is why  $35 = -(54)^2 \bmod 67$ .

=====
by 151:
-----
temp_b = 4524
-----
so -  $4524 = 145 \bmod 151$ .
so - 145 is root modulo 151 iff he is the root of:  $\rightarrow$ 
 $145^{((151+1)/4)} = 121 \bmod 151$ .
We will check if  $121^2 = b \bmod 151 \rightarrow$ 

 $121^2 = 145 \bmod 151$ .
and that is why  $145 = -(121)^2 \bmod 151$ .

=====

4524 has 4 roots modulo 10117 and they are: 54, 121.
Now we will use the Chinese Residue Theorem to find the number in
 $\mathbb{Z}_{(67 \times 151)}$ 
```

```
-----  
(13, 30) ->  
c = 9996 mod 10117
```

```
-----  
(13, 121) ->  
c = 5708 mod 10117
```

```
-----  
(54, 30) ->  
c = 4409 mod 10117
```

```
-----  
(54, 121) ->  
c = 121 mod 10117
```

```
////////////////////////////////////
```

```
////////////////////////////////////
-----
b = 7776
-----

number b = 7776 have roots modulo n = 10117 iff he have roots modulo p
= 67 and q = 151

=====
by 67:
-----
temp_b = 7776
-----
so -  $7776 = 4 \pmod{67}$ .
so - 4 is root modulo 67 iff he is the root of: ->
 $4^{((67+1)/4)} = 65 \pmod{67}$ .
We will check if  $65^2 = b \pmod{67}$  ->

 $65^2 = 4 \pmod{67}$ .
and that is why  $4 = -(65)^2 \pmod{67}$ .

=====
by 151:
-----
temp_b = 7776
-----
so -  $7776 = 75 \pmod{151}$ .
so - 75 is root modulo 151 iff he is the root of: ->
 $75^{((151+1)/4)} = 128 \pmod{151}$ .
We will check if  $128^2 = b \pmod{151}$  ->

 $128^2 \neq 75 \pmod{151}$ .
and that is why b = 75 is not a root modulo 151.
=====

7776 has 2 roots modulo 10117 and they are: 65, None.
Now we will use the Chinese Residue Theorem to find the number in
 $Z_{(67 \times 151)}$ 

-----
(2, 0) ->
c = 1208 mod 10117

-----
(2, 0) ->
c = 1208 mod 10117
////////////////////////////////////
```

```
////////////////////////////////////
-----
b = 4757
-----

number b = 4757 have roots modulo n = 10117 iff he have roots modulo p
= 67 and q = 151

=====
by 67:
-----
temp_b = 4757
-----
so -  $4757 \equiv 0 \pmod{67}$ .
4757 has only one root modulo 67 and it is 0.

=====
by 151:
-----
temp_b = 4757
-----
so -  $4757 \equiv 76 \pmod{151}$ .
so - 76 is root modulo 151 iff he is the root of:  $\rightarrow$ 
 $76^{((151+1)/4)} \equiv 128 \pmod{151}$ .
We will check if  $128^2 \equiv b \pmod{151} \rightarrow$ 

 $128^2 \equiv 76 \pmod{151}$ .
and that is why  $76 \equiv -(128)^2 \pmod{151}$ .

=====

4757 has 3 roots modulo 10117 and they are: 0, 128.
Now we will use the Chinese Residue Theorem to find the number in
 $\mathbb{Z}_{(67 \times 151)}$ 

-----
(0, 23)  $\rightarrow$ 
c = 6365 mod 10117

-----
(0, 128)  $\rightarrow$ 
c = 3752 mod 10117
////////////////////////////////////
```

ב.

4.