שם: שחר אשר
ת.ז. 209305408

<u>מבוא להצפנה – תרגיל 5</u>

.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 RSA (n,e) 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- $a^k \; mod \; p$ ונבדוק אם שווה ל- $\gamma = 738$.

$$3^k \; mod \; p$$

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

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

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

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

ולכן, המפתח הסודי של אליס הוא – 650.

שם: שחר אשר
ת.ז. 209305408

.3
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 mod 67.
so - 35 is root modulo 67 iff he is the root of: ->
35^((67+1)/4) = 54 mod 67.
We will check if 54^2 = b mod 67 ->

54^2 = 35 mod 67.
and that is why 35 = -+(54)^2 mod 67.

==============================================
by 151:
----------
temp_b = 4524
----------
so - 4524 = 145 mod 151.
so - 145 is root modulo 151 iff he is the root of: ->
145^((151+1)/4) = 121 mod 151.
We will check if 121^2 = b mod 151 ->

121^2 = 145 mod 151.
and that is why 145 = -+(121)^2 mod 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
Z_(67X151)
```

שם: שחר אשר
ת.ז. 209305408

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

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

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

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

שם: שחר אשר
ת.ז. 209305408

```
//////////////////////////////////////////////
----------
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 mod 67.
so - 4 is root modulo 67 iff he is the root of: ->
4^((67+1)/4) = 65 mod 67.
We will check if 65^2 = b mod 67 ->

65^2 = 4 mod 67.
and that is why 4 = -+(65)^2 mod 67.

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

128^2 != 75 mod 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_(67X151)

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

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

שם: שחר אשר
ת.ז. 209305408

```
/////////////////////////////////////////////
----------
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 = 0 mod 67.
4757 has only one root modulo 67 and it is 0.

==============================================
by 151:
----------
temp_b = 4757
----------
so - 4757 = 76 mod 151.
so - 76 is root modulo 151 iff he is the root of: ->
76^((151+1)/4) = 128 mod 151.
We will check if 128^2 = b mod 151 ->

128^2 = 76 mod 151.
and that is why 76 = -+(128)^2 mod 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
Z_(67X151)

--------------------
(0, 23) ->
c = 6365 mod 10117

--------------------
(0, 128) ->
c = 3752 mod 10117
/////////////////////////////////////////////
```

שם: שחר אשר
ת.ז. 209305408

ב.

אליס בוחרת את: $p = 67, q = 151$. ושולחת את $n = 10117$ לבוב.
בוב בוחר $a = 9996$ ומחשב את $a^2 = 9996^2 = b = 4524\ mod 10117$
ושולח אותו לאליס.
אליס מחשבת את השורשים הריבועיים של b ושולחת אחד מהם לבוב.
אם היא שולחת את 9996 או 121, אז בוב אינו מקבל שורש חדש. ולכן אליס ניצחה.
אם היא שולחת את 5708 או 4409, אז בוב מכיר עכשיו את כל החישובים של b והוא ניצח.
כדי להוכיח זאת, הוא מפרק את n בעזרת החישוב:

$$gcd(9996 - 5708, 10117) = 67$$

והוא שולח את הפירוק לאליס.

שם: שחר אשר
ת.ז. 209305408

4.

בשביל להראות כי הפרוטוקול הזה מקיים את שלוש התנאים לפרוטוקול באפס ידעה, אנו צריכים להראות שמתקיימים:

- פגי אינה מגלה שום מידע על הסוד שלה.
- משקיף של ההוכחה אינו מקבל אף מידע על הסוד של פגי.
- משקיף של ההוכחה אינו יודע אפילו אם פגי מכירה את הסוד.

<u>פגי אינה מגלה שום מידע על הסוד שלה</u>:
ויקטור מקבל את הלוג הדיסקרטי של מספר אקראי אחר $(r \ mod \ p-1)$, ולא של β.
ולכן, אינו מקבל שום מידע על a.

<u>משקיף של ההוכחה אינו מקבל אף מידע על הסוד של פגי</u>:
משקיף של ההוכחה אינו יודע שום דבר על הלוג הדיסקרטי של a.

<u>משקיף של ההוכחה אינו יודע אפילו אם פגי מכירה את הסוד</u>:
פגי וויקטור יכולים לביים את התהליך.
הם יכולים להחליט מראש איזה לוג דיסקרטי ויקטור יבקש, ואז פגי מכינה את המספרים בהתאם.
לכן, משקיף של ההוכחה לא יכול להשתכנע שפגי מכירה לוג דיסקרטי של a.

ולכן, הפרוטוקול הזה מקיים את שלוש התאים לפרוטוקול באפס ידיעה.

שם: שחר אשר
ת.ז. 209305408

5.

א.

נסביר למה האלגוריתם הזה אינו הוכחה ב- 0 ידיעה.

ויקטור בוחר - $x \in \mathbb{Z}_n$ אקראי ושולח לפגי את: $y \equiv x^2 \bmod n$.
פגי מחשבת שורש ריבועי s של y ושולחת אותו לויקטור.

אם פגי שולחת לויקטור את $s = x \bmod n$ או- $s = \text{-}x \bmod n$, אזי ויקטור לא מקבל שורש ריבועי חדש, והוא לא יכולה לחשב את הפירוק של n.

אם פגי שולחת לויקטור את $s \neq x \bmod n$ או- $s \neq \text{-}x \bmod n$, אזי ויקטור מכיר עכשיו את כל השורשים של y, והוא יכול לחשב את הפירוק של n על ידי:

$$\gcd(x - s, n) = q$$

לויקטור יש בסך הכל 5 פעמים לנסות לחשב את הפירוק.

לכן, ההוכחה היא לא הוכחה ב- 0 ידיעה כי לויקטור יש סיכוי לגלות את הסוד, שהוא: $n = p \cdot q$.
ואם הוא הצליח לחשב פירוק אזי, פגי גילתה מידע על הסוד שלה.

שם: שחר אשר
ת.ז. 209305408

ב.

משקיף של ההוכחה אינו יודע את הפירוק של n בהתחלה, הוא לא יודע אפילו אם פגי יודעת אותו. בגלל שפגי וויקטור יכולים לביים את התהליך.
הם יכולים להחליט מראש איזה x ויקטור יבקש, ואז פגי מכינה את המספרים בהתאם.
לכן, משקיף של ההוכחה לא יכול להשתכנע שפגי מכירה הפירוק של n.

המשקיף כן יכול לגלות את הפירוק של n רק אם ויקטור הצליח לחשב אותו, ואז הוא יוכל לראות אותו בדיוק כמו ויקטור.