**מבוא להצפנה – תרגיל 5**

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

**~~הסבר:~~**

~~כאשר היא ההודעה המקורית ו- הוא המפתח הציבורי ו- היא ההודעה המוצפנת.~~

~~את החתימה בוב מבצע על ידי:~~

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

*~~כאשר .~~*

*~~כאשר משתמשים פעמיים באותו מפתח RSA להצפנה ולחתימה, אנו מקבלים:~~*

*~~לאחר מכן, אליס מחשבת את:~~*

*~~כאשר .~~*

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

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

*החתימה תקינה אם: .*

ניתן לראות ש- זהה בשתי החתימות, והערך של הוא – .

זה אומר שאליס השתמשה באותו לחתימת שתי ההודעות.

*נראה מה קורה כאשר אליס משתמש באותו :*

*קיבלנו משוואה עם נעלם אחד . יש לה פתרונות.*

*נציב בשביל למצוא את הפתרונות:*

*נציב כעת ב- ונבדוק אם שווה ל- .*

*ולכן, המפתח הסודי של אליס הוא – .*

//////////////////////////////////////////////

----------

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)

--------------------

(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 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

//////////////////////////////////////////////

//////////////////////////////////////////////

----------

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

//////////////////////////////////////////////

אליס בוחרת את: . ושולחת את לבוב.

בוב בוחר ומחשב את ושולח אותו לאליס.

אליס מחשבת את השורשים הריבועיים של ושולחת אחד מהם לבוב.

אם היא שולחת את או , אז בוב אינו מקבל שורש חדש. ולכן אליס ניצחה.

אם היא שולחת את או , אז בוב מכיר עכשיו את כל החישובים של והוא ניצח.

כדי להוכיח זאת, הוא מפרק את בעזרת החישוב:

*והוא שולח את הפירוק לאליס.*