**מבוא להצפנה – תרגיל 4**

In this capter we calculate the private key d using the extended Euclidean algorithm.

i = 0, r = 33,        s = 0, t = 1

i = 1, r = 17, q = 1, s = 1, t = 0

i = 2, r = 16, q = 1, s = -1, t = 1

i = 3, r = 1, q = 16, s = 2, t = -1

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

we got that 1 = 17\*(2) + 33\*(-1)

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

So:

The value of s is 2

The value of t is -1

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

Now we calculate:

C\_a^s\*C\_b^t = m^(se\_a)\*m^(te\_b) = m^(se\_a + te\_b) = m (mod 16157)

Calculate 11671^-1:

First we need to calculate the inverse of 11671: 11671^-1 = 11671^-1 (mod 16157)

Now we calculate it using the extended Euclidean algorithm:

i = 0, r = 16157,        s = 0, t = 1

i = 1, r = 11671, q = 1, s = 1, t = 0

i = 2, r = 4486, q = 2, s = -1, t = 1

i = 3, r = 2699, q = 1, s = 3, t = -2

i = 4, r = 1787, q = 1, s = -4, t = 3

i = 5, r = 912, q = 1, s = 7, t = -5

i = 6, r = 875, q = 1, s = -11, t = 8

i = 7, r = 37, q = 23, s = 18, t = -13

i = 8, r = 24, q = 1, s = -425, t = 307

i = 9, r = 13, q = 1, s = 443, t = -320

i = 10, r = 11, q = 1, s = -868, t = 627

i = 11, r = 2, q = 5, s = 1311, t = -947

i = 12, r = 1, q = 2, s = -7423, t = 5362

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

we got that 1 = 11671\*(-7423) + 16157\*(5362)

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

So:

The value of s is -7423

The value of t is 5362

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

The inverse of 11671 is -7423 (mod 16157)

11671^-1 = -7423 = 8734 (mod 16157)

Now we calculate 11671^-1 = 8734^1 (mod 16157):

using the square and multiply algorithm:

1 in binary is [1]

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

i = 0

e\_i = 1

z^2 = 1 (mod 16157)

z\*8734 = 8734\*8734 = 8734 (mod 16157)

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

And we got that 11671^-1 = 8734 (mod 16157)

============================

Now we calculate:

7224^2 = (mod 16157)

2 in binary is [1, 0]

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

i = 0

e\_i = 1

z^2 = 1 (mod 16157)

z\*7224 = 7224\*7224 = 7224 (mod 16157)

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

i = 1

e\_i = 0

z^2 = 1^2 = 15223 (mod 16157)

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

And we got that 7224^2 = 15223 (mod 16157)

============================

The message is: 15223X8734 = 1729 (mod 16157)

============================

In this capter we calculate the private key d using the extended Euclidean algorithm.

i = 0, r = 33,        s = 0, t = 1

i = 1, r = 17, q = 1, s = 1, t = 0

i = 2, r = 16, q = 1, s = -1, t = 1

i = 3, r = 1, q = 16, s = 2, t = -1

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

we got that 1 = 17\*(2) + 33\*(-1)

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

So:

The value of s is 2

The value of t is -1

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

Now we calculate:

C\_a^s\*C\_b^t = m^(se\_a)\*m^(te\_b) = m^(se\_a + te\_b) = m (mod 16157)

Calculate 11449^-1:

First we need to calculate the inverse of 11449: 11449^-1 = 11449^-1 (mod 16157)

Now we calculate it using the extended Euclidean algorithm:

i = 0, r = 16157,        s = 0, t = 1

i = 1, r = 11449, q = 1, s = 1, t = 0

i = 2, r = 4708, q = 2, s = -1, t = 1

i = 3, r = 2033, q = 2, s = 3, t = -2

i = 4, r = 642, q = 3, s = -7, t = 5

i = 5, r = 107, q = 6, s = 24, t = -17

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

we got that 107 = 11449\*(24) + 16157\*(-17)

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

So:

The value of s is 24

The value of t is -17

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

The inverse of 11449 is 24 (mod 16157)

11449^-1 = 24 = 24 (mod 16157)

Now we calculate 11449^-1 = 24^1 (mod 16157):

using the square and multiply algorithm:

1 in binary is [1]

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

i = 0

e\_i = 1

z^2 = 1 (mod 16157)

z\*24 = 24\*24 = 24 (mod 16157)

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

And we got that 11449^-1 = 24 (mod 16157)

============================

Now we calculate:

13910^2 = (mod 16157)

2 in binary is [1, 0]

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

i = 0

e\_i = 1

z^2 = 1 (mod 16157)

z\*13910 = 13910\*13910 = 13910 (mod 16157)

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

i = 1

e\_i = 0

z^2 = 1^2 = 8025 (mod 16157)

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

And we got that 13910^2 = 8025 (mod 16157)

============================

The message is: 8025X24 = 14873 (mod 16157)

============================

To check if 18 is a creator of the group Z\_349 we will calculate the following:

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

1. Check what are the factors of n-1 = 348:

The factors of 348 are: [2, 3, 29]

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

2. Check if

18^174 != 1 mod 349

18^116 != 1 mod 349

18^12 != 1 mod 349

for all factors of 348

if they are all not equal to 1 then 18 is a creator of the group Z\_349

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

18^174 = 18 mod 349

18^116 = 18 mod 349

18^12 = 18 mod 349

YES 18 is a creator of the group Z\_349

a = |G|

We are going to find the value of k such that ord(18^k) = 348 (mod 349)

We are going to find that by the formula: ord(a^k) = |G|/gcd(k, |G|)

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

k = 2

18^k = 18^2 = 324

gcd(k, 348) = 2

ord(18^k) = ord(18^2) = 174

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

k = 3

18^k = 18^3 = 80

gcd(k, 348) = 3

ord(18^k) = ord(18^3) = 116

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

k = 4

18^k = 18^4 = 313

gcd(k, 348) = 4

ord(18^k) = ord(18^4) = 87

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

k = 5

18^k = 18^5 = 168

gcd(k, 348) = 1

ord(18^k) = ord(18^5) = 348

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

===================================

The value of k is: 5, and the order of 18^5 is: 348 (mod 349)

===================================

b = 29

We are going to find the value of k such that ord(18^k) = 29 (mod 349)

We are going to find that by the formula: ord(a^k) = |G|/gcd(k, |G|)

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

k = 2

18^k = 18^2 = 324

gcd(k, 348) = 2

ord(18^k) = ord(18^2) = 174

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

k = 3

18^k = 18^3 = 80

gcd(k, 348) = 3

ord(18^k) = ord(18^3) = 116

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

k = 4

18^k = 18^4 = 313

gcd(k, 348) = 4

ord(18^k) = ord(18^4) = 87

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

k = 5

18^k = 18^5 = 168

gcd(k, 348) = 1

ord(18^k) = ord(18^5) = 348

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

k = 6

18^k = 18^6 = 313

gcd(k, 348) = 6

ord(18^k) = ord(18^6) = 58

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

k = 7

18^k = 18^7 = 301

gcd(k, 348) = 1

ord(18^k) = ord(18^7) = 348

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

k = 8

18^k = 18^8 = 171

gcd(k, 348) = 4

ord(18^k) = ord(18^8) = 87

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

k = 9

18^k = 18^9 = 224

gcd(k, 348) = 3

ord(18^k) = ord(18^9) = 116

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

k = 10

18^k = 18^10 = 88

gcd(k, 348) = 2

ord(18^k) = ord(18^10) = 174

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

k = 11

18^k = 18^11 = 41

gcd(k, 348) = 1

ord(18^k) = ord(18^11) = 348

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

k = 12

18^k = 18^12 = 280

gcd(k, 348) = 12

ord(18^k) = ord(18^12) = 29

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

===================================

The value of k is: 12, and the order of 18^12 is: 29 (mod 349)

===================================

נחשב את *, , .*

*נבדוק איזה ערך ייתן את*

*לכן,*

*לסיכום, , , .*

נחשב את *.*

We are solving the discrete log problem with shanks algorithm.

The order of the group is 348 and m = ceil(sqrt(348)) = 19

Now we are looking for 0<=i,j<=19 such that:

18^(i+19\*j) 202 mod 349 <=> 18^i = 202X(18^((-19)^j) mod 349

Let's calculate the values of 18^i mod 349 for 0<=i<=19:

i = 0: 18^0 mod 349 = 1

i = 1: 18^1 mod 349 = 18

i = 2: 18^2 mod 349 = 324

i = 3: 18^3 mod 349 = 248

i = 4: 18^4 mod 349 = 276

i = 5: 18^5 mod 349 = 82

i = 6: 18^6 mod 349 = 80

i = 7: 18^7 mod 349 = 44

i = 8: 18^8 mod 349 = 94

i = 9: 18^9 mod 349 = 296

i = 10: 18^10 mod 349 = 93

i = 11: 18^11 mod 349 = 278

i = 12: 18^12 mod 349 = 118

i = 13: 18^13 mod 349 = 30

i = 14: 18^14 mod 349 = 191

i = 15: 18^15 mod 349 = 297

i = 16: 18^16 mod 349 = 111

i = 17: 18^17 mod 349 = 253

i = 18: 18^18 mod 349 = 17

Now let's calculate the values of 18^((-19)^j) mod 349 for 0<=j<=19 antil we find a match in the i values:

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

j = 0:

202 X 18^((-19)^0) mod 349 = 202

202 is not in the i values

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

j = 1:

202 X 18^((-19)^1) mod 349 = 44

===================

We found a match in the i values: 44 = 18^7 mod 349

202X(18^((-19)^1) = 18^7 mod 349

<=> 202 = 18^7+19\*1 = 18^26 mod 349

- Therefore the discrete log of 202 in base 18 mod 349 is 26

===================

We are going to send a symmetric key k = 111 using the following algorithm:

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

1. Alice generates a random number 'a' from 'Z\*\_2002'.

a = 1229

a^1 = 821

2. Bob generates a random number 'b' from 'Z\*\_2002' to.

b = 795

b^1 = 345

3. Alice calculates K\_1 = (k^a) mod p = (111^1229) mod 2003 = 1059

And then sends K\_1 to Bob.

4. Bob calculates K\_2 = (K\_1^b) mod p = (1059^795) mod 2003 = 1700

And then sends K\_2 to Alice.

5. Alice calculates K\_3 = (K\_2^(-a)) mod p = (1700^(-1229)) mod 2003 = 1059

And then sends K\_3 to Bob.

6. Bob calculates K\_4 = (K\_3^(-b)) mod p = (1059^(-795)) mod 2003 = 111

And then sends K\_4 to Alice.

============================================

final we have K\_4 = 111 which is the symmetric key k = 111.

K\_4 = 111, k = 111

============================================

נציג מתקפה מסוג "man in the middle" עבור הפרוטוקול הזה, שהתוצאה של המתקפה היא שאליס חושבת שהיא שולחת את לבוב אבל בסוף ההתקפה התוקף מלורי מקבל את ובוב מקבל בסוף מפתח שנקבע על ידי מלורי.

ההתקפה:

אליס שולחת לבוב את .

מלורי שנמצאת באמצע בוחרת הופכי, ומוסיפה ללא ידיעת אליס ובוב *את ושולחת את לבוב, ללא ידיעת אליס ובוב.*

*בוב מחשב את למרות שהוא ואליס חושבים שהוא מחשב את: .*

*לאחר מכן אליס מחשבת את: .*

*ובוב מחשב את: .*

*כעת לבוב יש את: .*

*מלורי מחשבת כעת את: .*

*ולסיכום: לבוב יש את בסוף האלגוריתם את: .*

*ולמלורי יש בסוף האלגוריתם את: .*

בהצפנת אל גמאל בוחרים אקראי.

הצפנה של הודעה היא .

בשתי ההודעות המוצפנות של בוב יש את אותו רכיב ראשון, לכן אנו יודעים כי בוב השתמש באותו רכיב עבור שתי ההודעות.

נסמן ב- את שתי ההודעות לפי הנתון, .

לכן,

*לפי הנתון:*

*ולכן,*

*לסיכום: הפענוח של ההודעה השנייה היא –*