שם: שחר אשר
ת.ז. 209305408

מבוא להצפנה – תרגיל 4

1.

א.

```
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
-----------------
```

שם: שחר אשר
ת.ז. 209305408

```
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)
============================
```

שם: שחר אשר
ת.ז. 209305408

ב.

```
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]
```

שם: שחר אשר
ת.ז. 209305408

```
-----------------------------
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)
============================
```

שם: שחר אשר
ת.ז. 209305408

.2

.א

```
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
```

שם: שחר אשר
ת.ז. 209305408

ב.

```
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)
===================================
```

שם: שחר אשר
ת.ז. 209305408

```
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
```

שם: שחר אשר
ת.ז. 209305408

```
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)
===================================
```

שם: שחר אשר
ת.ז. 209305408

ג.

נחשב את $L_{18}(3)$, $L_{18}(11)$, $L_{18}(7)$.

$$\begin{cases} 18^{54} = 27 = 3^3 \ mod\ 349 \\ 18^{211} = 33 = 3 \times 11 \ mod\ 349 \\ 18^{284} = 77 = 7 \times 11 \ mod\ 349 \end{cases}$$

$$\Rightarrow \begin{cases} 54 = 3L_{18}(3) \ mod\ 348 \\ 211 = L_{18}(3) + L_{18}(11) \ mod\ 348 \\ 284 = L_{18}(7) + L_{18}(11) \ mod\ 348 \end{cases}$$

$$L_{18}(3): 18 = L_{18}(3) \ mod\ 116$$

$$18 \ mod\ 116$$
$$18 + 116 = 134 \ mod\ 116$$
$$134 + 116 = 250 \ mod\ 116$$

$$L_{18}(3) = 18, 134, 250 \ mod\ 348$$

נבדוק איזה ערך ייתן את $L_{18}(3)$:

$$18^{18} = 17 \ mod\ 348$$

$$18^{134} = 329 \ mod\ 348$$

$$18^{250} = 3 \ mod\ 348$$

לכן, $L_{18}(3) = 250$

$$\Rightarrow \begin{cases} 250 = L_{18}(3) \ mod\ 348 \\ 211 = L_{18}(3) + L_{18}(11) \ mod\ 348 \\ 284 = L_{18}(7) + L_{18}(11) \ mod\ 348 \end{cases}$$

$$\Rightarrow \begin{cases} 250 = L_{18}(3) \ mod\ 348 \\ 309 = L_{18}(11) \ mod\ 348 \\ 284 = L_{18}(7) + L_{18}(11) \ mod\ 348 \end{cases}$$

$$\Rightarrow \begin{cases} 250 = L_{18}(3) \ mod\ 348 \\ 309 = L_{18}(11) \ mod\ 348 \\ 323 = L_{18}(7) \ mod\ 348 \end{cases}$$

<u>לסיכום</u>, $L_{18}(3) = 250$, $L_{18}(11) = 309$, $L_{18}(7) = 323$.

שם: שחר אשר
ת.ז. 209305408

ד.

נחשב את $L_{18}(100)$.

$$100 \times 18^3 = 21 = 3 \times 7 \ mod \ 349$$

$$\Longrightarrow L_{18}(100) + 3 \equiv L_{18}(3) + L_{18}(7) \ mod \ 348$$

$$\Longrightarrow L_{18}(100) + 3 \equiv 250 + 323 \ mod \ 348$$

$$\Longrightarrow L_{18}(100) + 3 \equiv 225 \ mod \ 348$$

$$\Longrightarrow L_{18}(100) \equiv 222 \ mod \ 348$$

$\Longleftarrow$ $L_{18}(100) \equiv 222$

שם: שחר אשר
ת.ז. 209305408

.3

```
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
===================
```

שם: שחר אשר
ת.ז. 209305408

.4
.א

```
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
============================================
```

שם: שחר אשר
ת.ז. 209305408

ב.

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

<u>ההתקפה</u>:
אליס שולחת לבוב את $K_1 = K^a \; mod \; p$.

מלורי שנמצאת באמצע בוחרת $C \in \mathbb{Z}^*{}_{p-1}$ הופכי, ומוסיפה ללא ידיעת אליס ובוב את $K_1{}' = K_1{}^c = K^{ac} \; mod \; p$ ושולחת את $K_1{}'$ לבוב, ללא ידיעת אליס ובוב.

בוב מחשב את $K_2{}' = (K_1{}')^b = K^{abc}$ למרות שהוא ואליס חושבים שהוא מחשב את: $K_2 = K_1{}^b = K^{ab}$.

לאחר מכן אליס מחשבת את: $K_3{}' = (K_2{}')^{-a} = K^{bc}$.
ובוב מחשב את: $K' = K_4{}' = (K_3{}')^{-b} = K^c$.

כעת לבוב יש את: $K' = K^c$.

מלורי מחשבת כעת את: $K = K'^{-c} = (K_4{}')^{-c} = K$.

<u>ולסיכום</u>: לבוב יש את בסוף האלגוריתם את: $K' = K^c$.
ולמלורי יש בסוף האלגוריתם את: K.

שם: שחר אשר
ת.ז. 209305408

5.

בהצפנת אל גמאל בוחרים $1 < k < p - 1$ אקראי.
הצפנה של הודעה x היא $(\alpha^k \ mod \ p, x\beta^k \ mod \ p)$.
בשתי ההודעות המוצפנות של בוב יש את אותו רכיב ראשון, לכן אנו יודעים כי בוב השתמש באותו רכיב k עבור שתי ההודעות.
נסמן ב- x_1, x_2 את שתי ההודעות לפי הנתון, $x_1 = 222 \ mod \ 349$.

לכן,

$$97 = 222 \times \beta^k \ mod \ 349$$
$$\Longrightarrow \beta^k = 97 \times 222^{-1} \ mod \ 349$$

לפי הנתון:

$$114 = x_2\beta^k = x_2 \times 97 \times 222^{-1} \ mod \ 349$$

ולכן,

$$x_2 = 114 \times 222 \times 97^{-1} \ mod \ 349$$
$$\Longrightarrow x_2 = 114 \times 222 \times 18 \ mod \ 349$$

$$\Longrightarrow x_2 = 99 \ mod \ 349$$

<u>לסיכום</u>: הפענוח של ההודעה השנייה היא –

$$x_2 = 99 \ mod \ 349$$
