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]
----------------------------
i = 0
e_i = 1
z^2 = 1 (mod 16157)
z*24 = 24*24 = 24 (mod 16157)
```

שם: שחר אשר
ת.ז. 209305408

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