1) DES system:

Process:

Step 1: converted hexadecimal strings (plain or cipher and key) to binary strings.

Step 2: Wrote Sixteensubkeys() function to return array of 16 subkey strings.

Sixteensubkeys():

- Generate 56 bit key from key by doing permutation with PC_I
- Divide 56-bit key c0 and d0 each with 28-bits.
- For each left shift on c0 and d0, store them in ci and di arrays. Do it for 16 times for 16 subkeys.
- For each ci and di, temp_i = ci+di , do permutation PC_II on temp_i to get subkey_i
- Return 16 subkey

Step 3: Do permutation on cipher or plain using IP matrix, call processDES() which returns

respective values for input string.

Wrote various functions like HextoBin(), HextoBinSplit(), PCOnePermutation(), xorFun(), Sbox() in this process.

processDES() do's :

- Divide each string into L and R
- In 16 iterations: for each call xorFun() to do $L_n = R_{n-1}$, $R_n = L_{n-1} + f(R_{n-1},K_n)$

xorFun() do's $f(R_{n-1},K_n)$ on Right bit and key. Also calls Sbox() for intermediate result.

Sbox() do's permutation of 8 sbox matrixes on the input string.

Decryption is done in the same process, but keys are sent in reverse order.

Result:

C:\Users\liebe\Downloads\cryptography\hw2\solution>java desprog1

------ DES cryptosystem ------

1. Encryption

2. Decryption

Enter the choice: 2

Enter Hexadecimal key:

8B2A7FF25E98C35D

Decryption selected

Enter file name:

DES-ciphertext.txt

It will generate desDecryptionResult.txt, which contains fallowing result

Computer security researchers say Internet worms are becÒoè}a
Vre complex

and could cause much more ha<l¹g 1¿previous versions: Inter>L ; *yrity

Systems' X-Force research engineer Neel Mehta says the Blaster worm, for example, necessarily had to connect through a port usually blocked, thus hindering its ability to spread as fast as possible. Nimda, however, represents a more complex worm in that it targeted internal networks and pieces of local networkZ À°beÏere easier to break into and live in. Zone Labs' Fred Felman agrees that worms could do more to penetrate systems by exploiting multiple vulnerabilities or finding other ways to propagate once inside the system. Gartner's Richard Stiennon warns against "low and slow" worm attacks that go unnoticed by administrators and security systems until they unleash a catastrophic attack, while Mehta says encryption advances could allow worms to carry more potent executables without being identified as doing so. A lot of the current security problems are the shared responsibility of users and software vendors, who create connected products that are easy to use but also more vulnerable to Internet attack. Enterprises can do more to protect themselves by adopting advanced firewalls that inspect packets and intrusion-detection systems that break down data into protocols instead of just matching patterns, and companies should also assess their security risks and write rules for when and how applications can connect to the Internet. Stiennon adds that organiza²úðy ç/@ould not rely on a monolithic IT architecture, but vary their components in order to better contain possible break-ins.

Final Result: (After analyzing and guesswork)

Computer security researchers say Internet worms are becoming more complex and could cause much more harm than previous versions: Internet security Systems' X-Force research engineer Neel Mehta says the Blaster worm, for example, necessarily had to connect through a port usually blocked, thus hindering its ability to spread as fast as possible. Nimda, however, represents a more complex worm in that it targeted internal networks and pieces of local networks that were easier to break into and live in. Zone Labs' Fred Felman agrees that worms could do more to penetrate systems by exploiting multiple vulnerabilities or finding other ways to propagate once inside the system. Gartner's Richard Stiennon warns against "low and slow" worm attacks that go unnoticed by administrators and security systems until they unleash a catastrophic attack, while Mehta says encryption advances could allow worms to carry more potent executables without being identified as doing so. A lot of the current security problems are the shared responsibility of users and software vendors, who create connected products that are easy to use but also more vulnerable to Internet attack. Enterprises can do more to protect themselves by adopting advanced firewalls that inspect packets and intrusion-detection systems that break down data into protocols instead of just matching patterns, and companies should also assess their security risks and write rules for when and how applications can connect to the Internet. Stiennon adds that organizations could not rely on a monolithic IT architecture, but vary their components in order to better contain possible break-ins.

2) RSA system

Used BigInteger library in Java to handle large numbers

Encryption Process:

Step 1: Converted Input strings N and b to BIgIntegers

Step 2: Generated cipher test using modPow() function, as fallows

```
BigInteger y = x.modPow(b,N);
```

Decryption process:

Step 1: Converted Input strings N and b to BIgIntegers

Step 2: calculate $\phi(N)$ using RSAfind() function. Which calls Pollard() function to get factor of N.

Step 3: we know, $\phi(N)$ and b, we will find a by calling findA() function.

```
BigInteger a = b.modInverse(ϕ(N));
```

Step 4: Decryption is done on cipher string with N and a , as fallows

```
BigInteger x = y.modPow(a,N);
```

Step 5 : Using matrix.txt , we will decrypt the values to text.

I converted the matrix to ASCII values to easy the process.

```
String[][] alpha = new String[][]{
{"32","33","34","35","36","37","38","39","40","41"},
{"42","43","44", "45", "46", "47", "48", "49", "50", "51"},
{"52", "53", "54", "55", "56", "57", "58", "59", "60", "61"},
{"62", "63", "64", "65", "66", "67", "68", "69", "70", "71"},
{"72", "73", "74", "75", "76", "77", "78", "79", "80", "81"},
{"82", "83", "84", "85", "86", "87", "88", "89", "90", "91"},
{"92", "93", "94", "95", "96", "97", "98", "99", "100", "101"},
{"102", "103", "104", "105", "106", "107", "108", "109", "110", "111"},
{"112", "113","114","115","116","117","118","119", "120", "121"},
{"122", "123", "124", "125", "126","32" ,"32"  ,"10","13","32"  }
};
```

Result:

```
C:\Users\liebe\Downloads\cryptography\hw2\solution1>javac rsaprog2.java

C:\Users\liebe\Downloads\cryptography\hw2\solution1>java rsaprog2
 ------ RSA cryptosystem ------

 1.Encryption

 2.Decryption

 Enter the choice: 2

NN:
681029162415569539013010687455016093901921698710978812 97
```

bb:

3663908873840754089455092320222410180999205934822319116 5

sucess

p :761059198034099969

q :894843875712616235394832743246282393 13

phi n: 6810291624155695381181668117423998584994783634843554201 6

a :74363472352358178218732532727623652372625429 3

b :3663908873840754089455092320222410180999205934822319116 5

Enter file name:

RSA-ciphertext.txt

As the attack was in progress, the bombs began to fall in earnest, the officers began shouting orders for everyone to head to the nearby rifle range to be issued firearms and ammunition.

About this time, the men at Schofield could look down towards the harbor and view theterrible sight unfolding as the attacking planes began to wreak their havoc among the anchored ships in the harbor. They could see what appeared to be a "mist" or "fog" rising from the harbor area. Jacques did not elaborate on this (quite possibly results of the bombing).

After the men were inthe process of being armed,the men who were anti-aircraft trained, such as Jacques, were ordered to head to the mouth of the harbor to man the battery of anti-aircraft guns (3-inch) locatedthere. The guns were situated in a "firing pit" of sorts that allowed for the weapon to rotate to follow attacking aircraft.

Upon reaching this assignment, the men began firing on the attacking aircraft (it is assumed that at this time, the attack had entered into the second wave of aircraft).

The weapons were fired andtargets were plentiful, indeed. The firing was to the extent that the barrels became red hot and the guns began jamming.

Some of thejamming guns would actually"buck like a bucking bronco" and literally fall back onto the gunners in the firing pits! The officers and noncoms on hand began issuing orders to exit the firing pits for fear of the weapons exploding and injuring or killing the men in the pits. Jacques did as he wastold, and got out of the firing pit, and began to run,falling into a large hole. He recalls being dazed, stunned and appeared to have fallen into a large "black hole" in which he had to climb out.(bomb crater?)

Final result:

As the attack was in progress, the bombs began to fall in earnest, the officers began shouting orders for everyone to head to the nearby rifle range to be issued firearms and ammunition.

About this time, the men at Schofield could look down towards the harbor and view the terrible sight unfolding as the attacking planes began to wreak their havoc among the anchored ships in the harbor. They could see what appeared to be a "mist" or "fog" rising from the harbor area. Jacques did not elaborate on this (quite possibly results of the bombing).

After the men were in the process of being armed, the men who were anti-aircraft trained, such as Jacques, were ordered to head to the mouth of the harbor to man the battery of anti-aircraft guns (3-inch) located there. The guns were situated in a "firing pit" of sorts that allowed for the weapon to rotate to follow attacking aircraft.

Upon reaching this assignment, the men began firing on the attacking aircraft (it is assumed that at this time, the attack had entered into the second wave of aircraft).

The weapons were fired and targets were plentiful, indeed. The firing was to the extent that the barrels became red hot and the guns began jamming.

Some of the jamming guns would actually "buck like a bucking bronco" and literally fall back onto the gunners in the firing pits! The officers and noncoms on hand began issuing orders to exit the firing pits for fear of the weapons exploding and injuring or killing the men in the pits. Jacques did as he was told, and got out of the firing pit, and began to run, falling into a large hole. He recalls being dazed, stunned and appeared to have fallen into a large "black hole" in which he had to climb out. (bomb crater?)

3) Rabin cryptosystem:
   1) Result:

a)

```
C:\Users\liebe\Downloads\cryptography\hw2\solution2>javac rabinprog3.java

C:\Users\liebe\Downloads\cryptography\hw2\solution2>java rabinprog3
 ------ Rabin cryptosystem ------
 SELECT Encryption method
 1. ek(x)=x^2 mod n
 2. ek(x) = x(x+B) mod n
 3. exit
 Enter the choice: 1

    p:199

    q:211

   Method selected ek(x)=x^2 mod n
      1.Encryption
      2.Decryption
      Enter the choice: 1
Encryption selected
plain:
32767
n :41989
encrypted plain: 17559
```

b)

```
 ------ Rabin cryptosystem ------
 SELECT Encryption method
 1. ek(x)=x^2 mod n
 2. ek(x) = x(x+B) mod n
 3. exit
 Enter the choice: 1

    p:199

    q:211

   Method selected ek(x)=x^2 mod n
      1.Encryption
      2.Decryption
```

```
      Enter the choice: 2
Decryption selected
cipher:
17559
n :41989
sqrt(17559) mod 199 (positive) :131
sqrt(17559) mod 199 (negetive) :68
sqrt(17559) mod 211 (positive) :62
sqrt(17559) mod 211 (negetive) :149
b1 :83
b2 :-88
plain1 :32767
plain2 :20827
plain3 :21162
plain4 :9222
 ------ Rabin cryptosystem ------
 SELECT Encryption method
 1. ek(x)=x^2 mod n
 2. ek(x) = x(x+B) mod n
 3. exit
 Enter the choice: 3
```

2) Result:

a)

```
C:\Users\liebe\Downloads\cryptography\hw2\solution2>java rabinprog3
 ------ Rabin cryptosystem ------
 SELECT Encryption method
 1. ek(x)=x^2 mod n
 2. ek(x) = x(x+B) mod n
 3. exit
 Enter the choice: 2

    p:199

    q:211
   Method selected ek(x) = x(x+B) mod n
    1.Encryption
    2.Decryption
    Enter the choice: 1
Encryption selected
plain:
32767
```

n :41989
encrypted plain: 16027

b)

------ Rabin cryptosystem ------
SELECT Encryption method
1. ek(x)=x^2 mod n
2. ek(x) = x(x+B) mod n
3. exit
Enter the choice: 2

p:199

q:211
Method selected ek(x) = x(x+B) mod n
1.Encryption
2.Decryption
Enter the choice: 2
Decryption selected
cipher:
16027
n :41989
intermediate y val :4013
sqrt(4013) mod 199 (positive) :86
sqrt(4013) mod 199 (negetive) :113
sqrt(4013) mod 211 (positive) :209
sqrt(4013) mod 211 (negetive) :2
b1 :83
b2 :-88
xi_1 :29538
xi_2 :1479
xi_3 :40510
xi_4 :12451
plain1 :7865
plain2 :21795
plain3 :18837
plain4 :32767
------ Rabin cryptosystem ------
SELECT Encryption method
1. ek(x)=x^2 mod n
2. ek(x) = x(x+B) mod n
3. exit
Enter the choice: 3

3) Rabin cryptosystem:-

1) a) $e_k(x) \equiv x^2 \bmod n$

y = x.modPow(new BigInteger("2"), n)

b) $d_k(y) = ?$

$y = \sqrt{x} \bmod n$

we have p and q, $n = p \times q$

$\sqrt{x} \bmod p \equiv \pm y^{(p+1)/4} \bmod p$

$\sqrt{x} \bmod q \equiv \pm y^{(q+1)/4} \bmod q$

$\Rightarrow x_{p1}, x_{p2}, x_{q1}, x_{q2}$

we will get 4 values, By using p and q ~~them~~ we calculate ~~result~~ ~~res~~.

~~result = q *~~ b1 and b2 through extended euclidean algorithm.

So, four possible result's are as fallow's.

~~res = q * b1 *~~

$res1 = (q \times b \times x_{p1} + p \times b2 \times x_{q1}) \bmod n$

$res2 = (q \times b \times x_{p1} + p \times b2 \times x_{q2}) \bmod n$

$res3 = (q \times b \times x_{p2} + p \times b2 \times x_{q1}) \bmod n$

$res4 = (q \times b \times x_{p2} + p \times b2 \times x_{q2}) \bmod n$

2) a) $e_k(x) = x(x+B) \bmod n$

B value = 1357

$y = x(x+1357) \bmod n$

b)

$y = x(x+B) \bmod n$

$y = x^2 + xB \bmod n$

Add $(B/2)^2$ on both sides

$y + (B/2)^2 = x^2 + xB + (B/2)^2 \bmod n$

$y + (B/2)^2 = (x + B/2)^2 \bmod n$

So, we calculate manually 2^{-1}, i.e $2^{-1} = 20995$.

$y + (B/2)^2 = y + (B \times 20995)^2 \bmod n$

$= y + (1357 \times 20995)^2 \bmod n$

we got y of ~~1002~~

$\bar{y} = y + (1357 \times 20995)^2 \bmod n$

So,

$x + B/2 = \sqrt{\bar{y}} \bmod n$

we will use previous method's to find 4 possible values.

~~$x = B \times 2^{-1}$~~

$$x = \left(\sqrt{y} \bmod n\right) - B \times 2^{-1}$$

$$x = \left(\sqrt{y} \bmod n\right) - 21673.$$