Question no.1

In a public-key scheme using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e=5, N=35. What is the plaintext M?

⇨ Given,

Ciphertext (C) =10

Encrypted key (e) =5

N =35

Plaintext (M) =?

Now,

The factor of the N =35 = 1 ,5 ,7,35

Prime number p = 5 , and q =7

Then,

T = (p – 1) (q – 1) = (5 – 1) (7 – 1) = 4 * 6 =24

Again,

e*d = T *n +1

if n =1, then,

or, 5d = 24 +1

or, d =25/5

therefore, d = 5

checking,

e*d mod T =1

or, 5 *5 mod T =1

therefore, 1 = 1

Finally, we have:

Public key (e ,N) = (5 , 35)

Private key (d ,N) = (5 ,35)

At last,

Plaintext (M) = $C^d$ mod N

$= 10^5 \bmod 35$

$= 5.$

Question no.2

In a public-key scheme using RSA, the public key of a given user is e=31, N=3599. What is the private key of this user? Please show the steps of how you get your answer.

⇨ Given,

Encrypted key (e) =31

N =3599

The private key(d, N) =?

Now,

The factor of the N =3599 = 1 ,59 ,61,35

Prime number p = 59 , and q = 61

Then,

T = (p – 1) (q – 1) = (59 – 1) (61 – 1) = 58* 60 = 3480

Therefore Z=58*60=3480

e*d= Z*n + 1 -> 31*d = 3480*n + 1

if n=1, 31 != 3481, it is not a solution.

After calculating one by one, we can deduce that n=27, 31*d=93961 -> d=3031

So the private key is (3031, 3599).

Question.3

Perform encryption and decryption using the RSA algorithm.

You need to describe the detailed procedure, including using exponentiation modular arithmetic to compute x^y mod z

| Question | P | Q | e | d | plaintext | ciphertext |
|---|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| A | 7 | 17 | | 5 | 19 | |
| B | 3 | 11 | 7 | | 5 | |
| C | 5 | 11 | | 3 | 9 | |
| D | 7 | 11 | | 17 | 8 | |
| E | 11 | 13 | | 11 | 7 | |
| F | 17 | 21 | | 7 | 2 | |

a) The answer of A:

⇨ Given,

A prime number (p) = 7

A prime number (q) = 17

Ciphertext (C) =?

Encrypted key (e) =?

Decrypted key (d) = 5

Plaintext (M) = 19

Now,

The value of the N = p * q = 7 * 17 =119

Then,

T = (p – 1) (q – 1) = (7 – 1) (17 – 1) = 6* 16 = 96

Again,

e*d = T *n +1

if n =1, then,

or, 5e = 96 +1

or, e =95/5

therefore, e = 19

checking,

e*d mod T =1

or, 19 *5 mod 96 =1

therefore, 95 = 1
is not equal so we will continue.
Again, if n= 2 ,
e = 193 / 5 = 38.6 which is also not equal
again, if n =3,
e = 288 / 5 = 57.8 which is also not equal
again, if n = 4,
e = 385 /5 =77 which is equal to the mod T = 1
Finally, we have:
The public key (e , N) = (77 , 119)
Private key (d ,N) = (5 ,119)
At last,
Ciphertext = M^e mod N = $19^{77}$ mod 119 = 66

b) The answer of B

⇨ Given,
A prime number (p) = 3
A prime number (q) = 11
Ciphertext (C) =?
Encrypted key (e) = 7
Decrypted key (d) = ?
Plaintext (M) = 5
Now,
The value of the N = p * q = 3 * 11 = 33
Then,
T = (p – 1) (q – 1) = (3 – 1) (11 – 1) = 2 * 10 = 20
Again,
e*d = T *n +1

if n =1, then,
or, 7d = 20 +1
or, d = 21/7
therefore, d = 3
checking,
e*d mod T =1
or, 7 * 3 mod 20 =1
therefore, 1 = 1 which is equal to the mod T = 1
Finally, we have:
The public key (e, N) = ( 7, 33)
Private key (d ,N) = (3, 33)
At last,
Ciphertext = M ^e mod N = $5^7$ mod 33 = 14

c) The answer for C

⇨ Given,
A prime number (p) = 5
A prime number (q) = 11
Ciphertext (C) =?
Encrypted key (e) =?
Decrypted key (d) = 3
Plaintext (M) = 9
Now,
The value of the N = p * q = 5 * 11 = 55
Then,
T = (p – 1) (q – 1) = (5 – 1) (11 – 1) = 4 * 10 = 40
Again,
e*d = T *n +1

if n =1, then,
or, 3e = 40 +1
or, 3e = 41
therefore, 41 is a prime so it is not possible to have the value of e.
Again, if n= 2 ,
3e = 80 +1
e = 81 / 3
therefore e = 27
checking,
e*d mod T =1
or, 81 mod 40 =1
therefore, 1 = 1, which is equal to the mod T = 1
Finally, we have:
The public key (e, N) = (27, 40)
Private key (d ,N) = (3 ,40)
At last,
Ciphertext = M^e mod N = $9^{27}$ mod 55 = 4

d) The answer for D

⇨ Given,
A prime number (p) = 7
A prime number (q) = 11
Ciphertext (C) =?
Encrypted key (e) =?
Decrypted key (d) = 17
Plaintext (M) = 8
Now,

The value of the N = p * q = 7 * 11 = 77
Then,
T = (p – 1) (q – 1) = (7 – 1) (11 – 1) = 6* 10 = 60
Again,
e*d = T *n +1
if n =1, then,
or, 17e = 60 +1
or, 17e = 61
therefore, 61 is a prime number which is not possible to have the value for e,
Again, if n= 2 ,
17e = 120+1
e = 121 / 17 = 7.11
checking,
e*d mod T =1
or, 7.11 * 17 mod 77 = 43.87
therefore, 43.87 = 1
is not equal so we will continue.
again, if n =3,
17e = 181 which is also a prime.
again, if n = 4,
17e = 241 which is also a prime.
Again, if n= 15,
17 e = 900 +1
e = 901 /17 = 53 which is equal to the mod T = 1
Finally, we have:
The public key (e , N) = ( 53 , 77)
Private key (d ,N) = (17 , 77)
At last,

Ciphertext = M^e mod N = $8^{53}$ mod 77 = 50

e) The answer for E

⇨ Given,

A prime number (p) = 11

A prime number (q) = 13

Ciphertext (C) =?

Encrypted key (e) =?

Decrypted key (d) = 11

Plaintext (M) = 7

Now,

The value of the N = p * q = 11 * 13 = 120

Then,

T = (p – 1) (q – 1) = (11 – 1) (13 – 1) = 10 * 12 = 120

Again,

e*d = T *n +1

if n =1, then,

or, 11e = 120 +1

or, e =121/11

therefore, e = 11

checking,

e*d mod T =1

or, 11 * 11 mod 120 =1

therefore, 1 = 1 which is equal to the mod T = 1

Finally, we have:

The public key (e , N) = (11, 143)

Private key (d ,N) = (11 ,143)

At last,

Ciphertext = M^e mod N = $7^{11}$ mod 143 = 50

f) The answer for F

⇨ Given,

A prime number (p) = 17

A prime number (q) = 21

Ciphertext (C) =?

Encrypted key (e) =?

Decrypted key (d) = 7

Plaintext (M) = 2

Now,

The value of the N = p * q =17 * 21 = 357

Then,

T = (p – 1) (q – 1) = (17 – 1) (21 – 1) = 16* 10 = 320

Again,

e*d = T *n +1

if n =1, then,

or, 7e = 320+1

or, e =321/ 7

therefore, e = 45.85

checking,

e*d mod T =1

or, 45.85 * 7 mod 320 =1

therefore, 1.0003 = 1

is not equal so we will continue.

Again, if n= 2 ,

7e = 641 which is also a prime.

again, if n =3,

e = 961/ 7 = 137.285 which is also not equal

again, if n = 18,

e = 5761 / 7 = 823 which is equal to the mod T = 1
Finally, we have:
The public key (e , N) = (823, 357)
Private key (d,N) = (7 , 357)
At last,
Ciphertext = M^e mod N = $2^{823}$ mod 357 = 128