1. Simple Product Cipher

- Please use the following simple Product Cipher to send the plaintext "coronavirus pandemic". Caesar Cipher is used for Confusion, Transposition Cipher is used for Diffusion.
    - A. Encrypt the plaintetxt to create ciphertext
        1. Encrypt the message using Caesar Cipher with key=3
        2. Encrypte the previous result using Transposition Cipher with the key="covid"
    - B. Decrypt the ciphertext to create plaintext
        1. Decrypt the ciphertext using Transposition Cipher with the key="covid"
        2. Decrypt the previous result using Caesar Cipher with key=3

2. If you compare the advantages and disadvantages of symmetric key cryptography and asymmetric key cryptography based only on the number of keys each mechanism needs to create. The less the better.

- Under what condition, symmetric key cryptography is better?
- Under what condition, asymmetric key cryptography is better?
- Under what condition, they are tie?

What you need to find out are

1. The range of the number of users when symmetric key cryptography is better than asymmetric key cryptography.
2. The range of the number of users when symmetric key cryptography is worse than asymmetric key cryptography.
3. The range of the number of users when symmetric key cryptography is as good as asymmetric key cryptography .

Your answer will looks like this

200 < N < 300 symmetric key cryptography is as good as asym
N <=200 symmetric key cryptography is better
300 <= N asymmetric key cryptography is better

Note: - N represents number of users.
- This answer is an example, it is not the correct answer,

You can figure out the answers by first figuring out the formulas for

Number_of_keys=f(N)

Thus,

1. How many keys are required for N number of users if symmetric key cryptography is used?
2. How many keys are required for N number of users if asymmetric key cryptography is used?

Comparing the formulas, you will be able to figure out the answers.

Ans:

1.

A.

1)

With the key = 3, we get abcdefghijklmnopqrstuvwxyz to defghijklmnopqrstuvwxyzabc

Then, encrypt the message (***coronavirus pandemic***) using Caesar Cipher, we get

‘frurqdyluxv sdqghplf’

2)

Encrypte the previous result using Transposition Cipher with the key="covid", we get (alphabetical sort the key)

c	o	v	i	d
1	4	5	3	2
f	r	u	r	q
d	y	l	u	x
y	s	d	q	g
h	p	l	f	a

Then output in the order, we get “fdynqxgaruqfryspuldl”

B.

1)

The length of cipher is 20 and the length of the key is 5

So numbers of rows = 20 /5 = 4

fdyn qxga ruqf rysp uldl

Then mark the key’s sequence:

c	o	v	i	d
1	4	5	3	2
f	r	u	r	q
d	y	l	u	x
y	s	d	q	g
h	p	l	f	a

The plaintext we get is “frurqdyluxvsdqghplfa”

2)

Decrypt the previous result using Caesar Cipher with key=3, and we have “frurqdyluxvsdqghplfa”,
When key = 3 we get, defghijklmnopqrstuvwxyzabc
Then compare to get the sequence, thus go find in the abcdefghijklmnopqrstuvwxyz
For example, f is 3rd and in original one 3rd is c.
We will get “coronaviruspandemicx”

2.

Under what condition, symmetric key cryptography is better?

When transfer keys, and n < 5

Under what condition, asymmetric key cryptography is better?

When encrypt and decrypt the message, and n > 5

Under what condition, they are tie?

When contacting objects equal to 5, they are tie, because asymmetric is 2n, symmetric key is n(n-1)/2, when n = 5, 2 * 5 = 10 = 5 *(5 - 1)/2

When there are n number of users, we need n(n-1)/2 symmetric keys, because every two users have a key
When there are n number of users, we need 2n asymmetric keys, because each users have public key and private key, two keys.