Question no.1
Discussion Board

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?
  - ⇨ Speed is a concern as it uses a single key for encryption and decryption, making the process faster compared to asymmetric key cryptography. Large amounts of data need to be encrypted as it is more efficient for bulk encryption. The number of participants is limited and trusted as the same key is used for both encryption and decryption.

    Overall, symmetric key cryptography is preferred when speed and simplicity are important, and the number of participants is limited and trusted.

- Under what conditions, asymmetric key cryptography is better?
  - ⇨ Security is a concern as it uses a pair of public and private keys for encryption and decryption, making it more secure compared to symmetric key cryptography. The number of participants is large and not fully trusted as each participant has their own unique pair of keys, ensuring the confidentiality and authenticity of the communication. Digital signatures and authentication are required as the

public key can be used for encrypting messages, while the private key is used for decryption.

Overall, asymmetric key cryptography is preferred when security and confidentiality are important, and the number of participants is large and not fully trusted.

- Under what conditions, they are tied?
  - ⇨ Both symmetric and asymmetric key cryptography can be used in different scenarios depending on the specific requirements of the system. In some cases, a combination of both can also be used to achieve a balance between security and efficiency.

    Therefore, there is no strict condition where one is better than the other and they can be considered tied in terms of when they are appropriate to use. The choice between the two ultimately depends on the specific requirements and trade-offs of the system in question.

What you need to find out are

- The range of the number of users when symmetric key cryptography is better than asymmetric key cryptography.
  - ⇨ $N < 26$, if the key size i.e N is smaller then it is better than the symmetric key.
- The range of the number of users when symmetric key cryptography is worse than asymmetric key cryptography.

- ⇨ N >26, if the key size i.e N is greater then it is better than the asymmetric key

- The range of the number of users when symmetric key cryptography is as good as asymmetric key cryptography N= 26, if the key size i.e N is equal then it is as good as an asymmetric key.

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 the 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)

- ⇨ For symmetric key cryptography, the number of keys f(n)=N(N-1)/2......(1)

  For asymmetric key cryptography, number of keys f(n)=2N......(2)

  solving both equations 1 and 2 we get n=6,0; that means when the number of users is 6 both symmetric and asymmetric key cryptography need the same number of keys. When the user number, is n=6,
  for symmetric key cryptography number of keys=6(6-1)/2=15, and for asymmetric key cryptography number of keys is N=2n=2*6=12, So,

when the user number is 5 both symmetric and asymmetric cryptography is on a tie. Checking with lesser or higher numbers,
let's consider user n=4, Symmetric keys=4*3/2=6, asymmetric keys=2*4=8; considering n=6, symmetric keys=5*4/2=10, asymmetric keys=2*5=10; from this, we can conclude that, when the number of users is less than 5 symmetric key cryptography requires less number of keys than asymmetric keys. Similarly, the number of users increases from 5, and the number of symmetric keys is higher than asymmetric keys.

With respect to the number of keys, for n number of users,

if n=6 asymmetric key cryptography is as good as symmetric key cryptography.
n>6 asymmetric key cryptography is better

n<6 symmetric key cryptography is better

Thus,

4. How many keys are required for N number of users if symmetric key cryptography is used?
   - ⇨ The number of keys needed for the user, if they are symmetric key cryptography then it is (n^2 -n)/2.

5. How many keys are required for N number of users if asymmetric key cryptography is used?
   - ⇨ When using asymmetric key cryptography, each user needs a set of public and private keys, for a total of two keys. Therefore, N * 2 keys are needed for N users.

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

- ⇨ Comparing the formulas of asymmetric and symmetric key cryptography does not necessarily which is better as the appropriate choice between the two ultimately depends on the specific requirements and trade-offs of the system in question.

  In general, symmetric key cryptography can be faster and more efficient than asymmetric key cryptography, as it uses a single key for both encryption and decryption. However, symmetric key cryptography may be less secure, as the same key must be shared among all participants, increasing the risk of key compromise.

  Asymmetric key cryptography, on the other hand, uses two separate keys (a public key and a private key) for encryption and decryption, offering a higher level of security. However, asymmetric key cryptography can be slower and less efficient than symmetric key cryptography, as it requires more complex mathematical computations and the use of two separate keys.

  The specific formulas used in each type of cryptography can vary widely depending on the algorithm and the requirements of the system. Some common algorithms used in asymmetric key cryptography include RSA, Elliptic Curve Cryptography (ECC), and Diffie-Hellman, while some common algorithms used in symmetric key cryptography include AES, DES, and Blowfish.

In conclusion, comparing the formulas of asymmetric and symmetric key cryptography can provide insights into the strengths and weaknesses of each approach, but the appropriate choice between the two ultimately depends on the specific requirements and trade-offs of the system in question.