# Asymmetric data cryptography and asymmetric data cryptography: the meaning and ap...

Science, Computer Science

There are two common types of data cryptography that are commonly used, symmetric data cryptography and asymmetric data cryptography. When it comes to symmetric key cryptography, both the receiver and the sender share common information or secrets. The mutually shared information or shared secrets is what is used for decryption and encryption. On the hand, in asymmetric cryptography, two different keys that form a single pair are made use of. One of the keys is private whereas the other one is public. The public one is normally used for the encryption of messages from its user end and the other user can also decrypt the messages by the use of a private key. In the event that organizations intend to utilize symmetric key cryptography, there can be an arrangement where the secret key can be shared offline in order to be used for decryption and encryption. Similarly, if an organization intends to used asymmetric cryptography, then it means that the cryptography in this case is public and pairs of can be chosen and shared to the public. This paper carries out a brief study on the advantages and disadvantages of both keys and then proposes a solution for the given case study. Basing arguments on the advantages of the two keys, this essay proposes asymmetric key as the solution that ABC research institute should make use of in ensuring the security of the top secret information that it has.

## Advantages of Using Symmetric Keys

The chief advantage of using symmetric keys is that they significantly prevent messages from landing on parties that are unauthorized. In other words, they are highly secure. They are easier and faster to implement when compared to their asymmetric counterparts (B sasi, 2014). Installing symmetric keys does not consume time. Additionally, implementing them for

use in the systems of organizations is relatively easier. Another advantage of symmetric keys is that they have a relatively lower overhead costs on the system resources.

## Advantages of Asymmetric Keys

The chief advantage of using asymmetric key is relatively easy to administer and quite scalable. Asymmetric key also has a friendly user interface which makes it ideal for the users to use it (Fujisaki & Okamoto, 2014). Another advantage of this key is that it is easy to detect that someone has tries to compromise whatever it is concealing. Information encrypted with asymmetric key is highly safe and secure.

## Solution for the Case Study

In the case study, this essay proposes the use of asymmetric key as the solution. ABC institute of Research should opt for opt for asymmetric encryption since their main objective is to ensure safety of information. With the use of asymmetric key encryption, the implication is that information is entirely private therefore no third party will have access to it. One of the main advantages of using asymmetric encryption is the manner in which it is capable of establishing a highly secure channel even in instances where it is operating on mediums that are not secure. This is possible because in asymmetric encryption, there is exchange of public keys that are used in the encryption of the data. The private key that complements the public key is never shared and this is the key that is used for decryption.

## Conclusion

In the long run, both systems of data encryption have the good and bad sides. In choosing the type of encryption to be used, the specific needs and context for that encryption should be defined as that is what gives the direction on the type of encryption to be made use of. As for the case study, it is evident that asymmetric encryption is very efficient in conveying top secret information and therefore ABC research should definitely make use of it.