Online Activity #1

Ahsan Syed

[Aksyed2@myseneca.ca](mailto:Aksyed2@myseneca.ca)

Monday – 3rd July 2017

**Describe how to use Symmetric and Asymmetric keys to secure a message**

**Symmetric Keys** secure a message with a same key to encrypt and decrypt information. With symmetric encryption, strenght and secrecy of the key is really important. One key is used in the encryption and decryption process; the key is dstribued to all the parties that will need to

encrypt or decrypt the data.

In simple words, with symmetric encryption only one secret key is used which I shared with different groups/users. Symmetric keys are more efficient and faster, as they have fixed key length. But if the key is lost, modification and disclosure of data is possible.



**Asymmetric key** is also widely known as public key encryption. It was originally concieved to tackle some of the weak points of symmetric keys: key distribution, nonrepudiation, and generation. This encryption involves two different keys(public key and private key), unlike symmetric keys. Anyone who has access to the public key can encrypt data but only the private key holder can decrypt data. Asemmetric encryption problems usually invovle ones that are relatively easy to solve one way, but difficult to solve the other way.

In simple words, with asymmetric encryption a paid of keys are used in which one is public and the other is private. Depending on the algorithms, it has variable key lenghts, which makes it slower and less efficient. If data is lost, both key datas can be modified, but disclosed from only the private key.



Joe wants to send a secure message to Bob. You need to make this process both secure and efficient by applying Symmetric and Asymmetric Keys.

Please describe the detailed steps in your process.

Knowing the advantages and disadvantages of both, symmetric and asymmetric keys, the most ideal path for Joe would be to use the advantages of both the keys. Thus, that way Joe will get a good mix of performance and security combining the two. Asymmetric keys could be used to exchange the keys and symmetric keys could be used to encrypt the data.

Joe should start off by encrypting the message with symmetric keys so the process is in its most efficient form. Joe then should send the message through asymmetric encryption so that it’s secure and only the private key can unveil it. If symmetric key is used, the message can easily be hacked by a third-party. The principle is that a strong algorithm with a large key should be used to encrypt the key. Another encryption algorithm (symmetric key) can be used now with a smaller key so that the data can be transferred faster. And while doing so, using asymmetric encryption with symmetric keys to protect the symmetric keys will keep the data secure. Once Bob receives the data, he will have the keys to decrypt it. This way the message will be secure and efficient!