**CSC-407 INFORMATION SECURITY**

BSCS 8-C – Fall 2021

**ASSIGNMENT 1**



**STUDENT NAME:** SAIF-UR-REHMAN

**STUDENT ENROLLMENT:** 02-134181-005

**INSTRUCTOR:** SIR NOMAN KHALID

**DEPARTMENT OF COMPUTER SCIENCE**

**BAHRIA UNIVERSITY, KARACHI CAMPUS**

**CLASSIFICATION OF ENCRYPTION TECHNIQUE:**

The basic purpose of the encryption is to convert the plain text into cipher text so that it can be protected from any sort of security breach and all the CIA traits are met. Now encryption is of two types Symmetric Encryption and Asymmetric Encryption. In symmetric encryption there is one key which is used for both encryption and decryption and in Asymmetric encryption there are two keys public and private keys one for encryption and other for decryption it is also called public key cryptography.

Now the technique which I think will be most suitable for a company like adventure club will be Asymmetric encryption that is because the sender and receiver will have different keys, sender will use one key for encryption and receiver will use other key to decrypt it. In it the data encrypted with public key can only be decrypted with private key and vice versa. Transport layer security is the security layer that makes https possible and it is also based upon Asymmetric encryption. A user or client will take public key from websites transport layer security and then he will use it for secure communication. Website owners keep private key secret.

**EXPLANATION OF ENCRYPTION FRAMEWORK:**

If we talk about Asymmetric encryption, Asymmetric encryption itself is a broad term there are many type of Asymmetric encryption as discussed above one of the most basic feature or different feature which Asymmetric encryption is the number of keys it have two keys public and private keys. One key is used for encryption and other is used for decryption and usually most important protocol for website is https and it is provided by transport layer security and it comes under the umbrella of asymmetric encryption, TLS provides public key for secure communication over network and private key is with website owner In general terms HTTPS(Hyper Text Transfer Protocol Secure) is a protocol that protects the integrity and confidentiality of data packets between the user and the computer. If we talk about protocol it is simply set of rules for transmitting data between devices. Data while using the HTTPS is protected by transport layer security protocol which ensures that CIA traits are ensured and maintained.

**ARGUMENTS FOR & AGAINST THE ENCRYPTION OPTION:**

If we talk about symmetric encryption the most key feature that we can say is compromised is security because in it we only use one key for encryption and decryption so in case if we have large number of users then the security might be compromised due to key distribution and single key but in case if we are using asymmetric encryption we have both public and private keys for encryption and decryption and the end user have either public or private key so the chances of security breach are less. Asymmetric encryption also provides the facility of digital signatures in which there is hash value protected by the senders private key and is decrypted by the receiver with senders public key this thing ensure the integrity of the data. RSA and DSA are the most commonly used digital signature algorithms.

**SORT OF PROJECTS WHICH BENEFIT & NOT BENEFIT:**

The projects in which the security is the major concern and speed isnt then asymmetric encryption is most suitable but incase if the speed is more major concern as comapre to the security thdn we can say symmetric encryption can be used. In case if we are working on the project which is being designed for banking then symmetric encryption will be more suitable that is because symmetric cryptography is more suitable for bulk encryption of large amounts of data like for payment applications which includes card based transactions. Symmetric encryption is also suitable for the data at rest and its most common example is bitlocker based encryption due to which if the drive which is encrypted with bitlocker is placed in any other system it requires bitlocker dec ryption key for usage. Now if we talk about asymmetric encryption it can be used for projects like chatting apps which uses end to end encryption for the protection and to maintain confedentiality aysmmetric encryption can also be used for web application because most of the websites are protected by HTTPS which is based on TLS.

**EXPLAINATION OF TWO ASPECTS OF ENCRYPTION TECHNIQUES:**

There are two basic techniques of encryption Asymmetric and Symmetric as discussed above the major difference between these two is Asymmetric have two different keys for encryption and decryption which are public and private keys on the other hand the symmetric encryption only have one key which is used for both encryption and decryption. Both of these methodologies have their own advantages and disadvantages like incase if our major priority is security then we use asymmetric encryption but if our priority is speed then symmetric encryption is more suitable the most common types or example of symmetric encryption are Des, Triple Des, Blow fish, RC4, RC5, RC6 and AES. If we talk about asymmetric encryption then its most common example are end to end encryption, digital signatures, RSA, diffie-hellman and others. There are many case scenarios in which symmetric and asymmetric encryption are used together for better services. Some of the major features that both of them provide like security and speed are incorporated together for better services. HTTPS connection between the client and server uses both of the encryption techniques like for many websites first asymmetric encryption is used to establish a connection then for duration or continuation of the connection symmetric encryption is used. There is a session key which is one time use symmetric key which is used for encryption and decryption. These session keys are randomly generated, the approach in which both techniques are used together is called hybrid approach. As discussed above it is used by TLS/SSL which forms the basics for https it is also used by mobile chat systems which uses asymmetric encryption for the verification of identity of participant at the conversation start and then symmetric encryption for the ongoing contents of the conversation because symmetric encryption is useful and fast for bulk encryption.Whatsapp we can say is an example of hybrid approach which uses the combination of both symmetric and asymmetric encryption.