**BAHRIA UNIVERSITY**

**Karachi Campus**

**Department of Computer Science**

**Information Security (CSC-407)**

**Fall 2020**

**Assignment Title : Encryption Techniques and Email standards**

**Name:** Muhammad Uzair **Enrollement:** 02-134171-061

Assignment # 1  **S**core **: 10** Due Date: 29/10/2020

**Instructions :** Follow these instructions carefully otherwise marks will be deducted.

**•**Deadlines are to be strictly observed; no late submissions will be accepted under any circumstances.

•Submit handwritten assignment (**preferably in your own words**)

•Submit assignment as a SINGLE file in either PDF or word format using same template on LMS-- no other file formats will be accepted.

•This is individual assignment; no copying is allowed . Any form of plagiarism will result in receiving zero in the assignment.

**Instructor:** Imran Memon

**Office:** Faculty 9 near lab-6 ,Iqbal block,Bahria university, karachi

**Telephone:** 9240002, ext. 392

**E-mail:** imranmemon.bukc@bahria.edu.pk

**Website:** https://sites.google.com/site/imranmemoncourses1

**Office Hours:** 8:00 am to 4:30 PM

What is a link-layer frame? A network layer datagram? A transport-

layer segment? an application-layer message?

What is a link-layer frame? A network layer datagram? A transport-

layer segment? an application-layer message?

What is a link-layer frame? A network layer datagram? A transport-

layer segment? an application-layer message?

What is a link-layer frame? A network layer datagram? A transport-

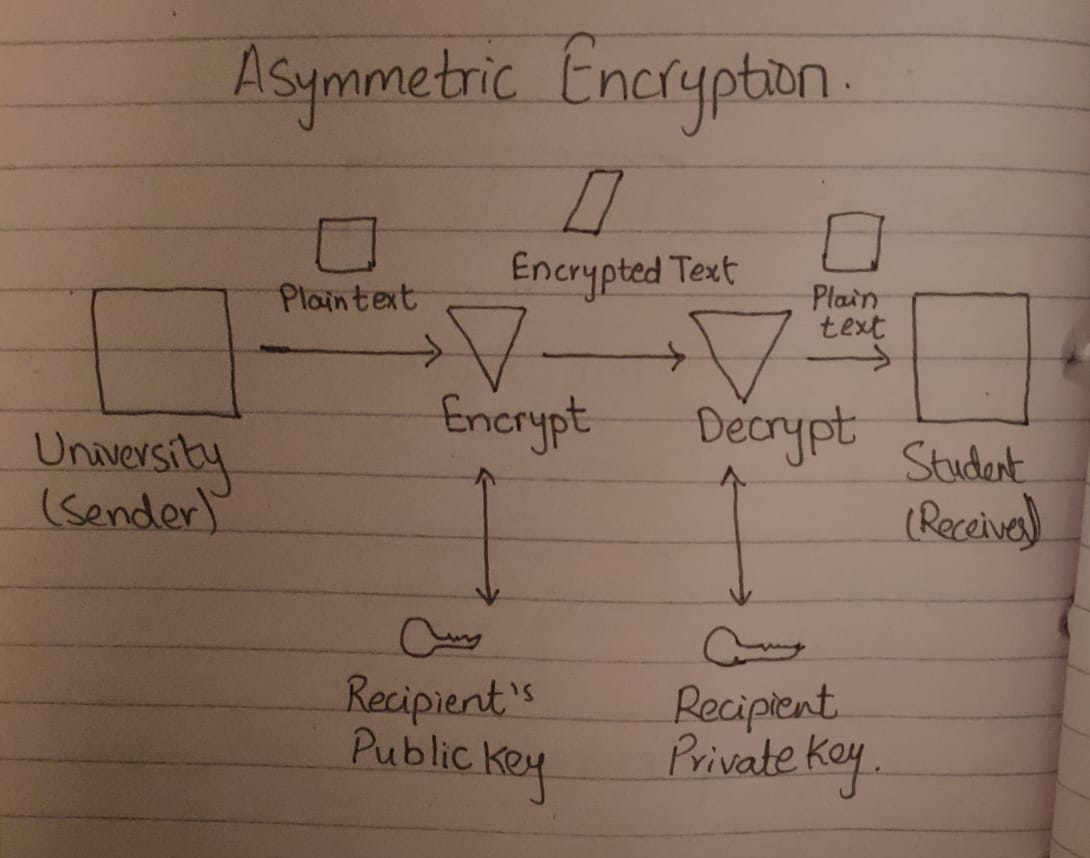
layer segment? an application-layer message?

1. Consider bahria university has no experience in encryption teahniques from Information security Engineer point of view ,explain encryption algorithm methodology also trying to argue the case to adopt the encryption methodology for internal system security and contracted (procured) system development. you will need to provide detailed arguments?

* An overview of encryption technique

Asymmetric encryption methodology would be adopted for this case. Encryption is a way of jumbling data so that only authorized or consented parties can be able understand the information. In methodological term, encryption is the procedure of altering plaintext to ciphertext. In easy term, it takes readable information and changes it so that it just seems random.

* An explanation of the encryption framework



Univeristy has send a message to a student in which public key can be known to everyone but private keymust be identified and used only by the university (owner). In this case, public keys will be listed in register and record of e-mail so that they are accessible to any student whoever wants to utilize these keys for encryption or decryption of data when communicating with the university.

* Arguments for and against the adoption of Encryption. You will need to reference authoritative sources to convince your management
* Asymmetric data is more secure than symmetric encryption because it uses different keys for the encryption and decryption process.
* Asymmetric systems provides for simplier and more convenient key sharing than symmetric systems and asymmetric system also do not have the scalability concerns unlike symmetric systems.
* Asymmetric encryption also allows authentication and non-repudiation unlike symmetric systems.
* Clearly identify what sorts of projects would benefit and what sorts of projects will not benefit. This can be part of your point 3 arguments.

Projects that would be benefit:

Everyday communication over the internet, Asymmetric encryption method is used and Client-server model which is based on digital certificates, Asymmetric encryption method is preferred. Asymmetric will assure that data is more secure because it uses different keys for the encryption and decryption process.

Projects that would not be benefit:

When there is transmitting of data in bulk, which means encrypting files and communication path, for such purpose asymmetric encryption is not preferred technique because it is more complex and executes slower.

* An explanation of two aspects of Encryption methodologies (Encryption, secure or other processes) that could be adopted across the organisation, even if some systems were not appropriate for Encryption. Explain why this is a good idea. (minimum 1000 words)

Symmetric encryption, there is only one key, which is used for encryption and decryption. It is then significant that a protected method is believed to transfer the key among sender and recipient. Symmetric encryption is faster than asymmetric encryption because of it`s simple logic.

Asymmetric encryption, there are two keys: one key is used for encryption, and a different key is used for decryption. One of the keys is known as the private key and the other is known as the public key. The private key is kept by the owner, while public key is shared publicly for anyone to use.

**(3 marks)**

1. Suppose you are security engineer and your job to develop cryptographic application is larger and more complex ,project focus on customer requirements have been thoroughly secure wihin budget.Explain in detail cryptographic scheme (s) would you choose and why?

Asymmetric encryption methodology would be adopted because project`s the key requirement is to develop cryptographic application is larger and more complex, project focus on customer requirements have been thoroughly secure wihin budget. Asymmetric encryption, there are two keys: one key is used for encryption, and a different key is used for decryption. One of the keys is known as the private key and the other is known as the public key. The private key is kept by the owner, while public key is shared publicly for anyone to use.

(**2 marks)**

1. How can security technique improvement plan including applicable protect any information security project? Discuss appropriate tools and processes chosen to coordinate various aspects of Infromation security tasks?

Let take an example of LMS (Learning Management System), It is an application for the management, certification, trailing, reportng, computerization and liberation of learning courses, educational programs or training and development programs. The LMS concept come out directly from e-Learning. Some of the tool services of LMS are managing users, courses, roles, and generating reports, making a course calendar, messaging and notifications, assessments that can handle pre/post testing, certification and display employees' score and transcripts, instructor-led course management and administration.

(**2 marks)**

1. In the email system ,there are many viruses / trojan horses propagate via email. The messages in question carry forged “From” addresses, to improve the likelihood that the recipient will activate the attachment, explain the technique reduce the risk and losses also, improvement the email security?

Secure MIME (S/MIME)is used for providing secure data/message transmissions. S/MIME is a standard for digitally and encrypting signing e-mails. S/MIME is the extends of the MIME standard which allows for the encryption of electronic mail and attachments. The hashing algorithms and encryption can be specified by the sender of the message.

If someone has interfered with the email or digital signature, S/MIME immediately alerts the recipients regarding the risk.

(**1 mark)**

1. Give one example for each, example should be explained in your own words ,it is recommended if possible the example should be any of your’s/friend’s past experience / Real World Scenario.
2. Link Encryption

**Secure Group website** is an example of link encryption.

Secure Group website utilizes link encryption through SSL. Whenever the visitors come and they use it to log into our systems for registered users. Traffic between them and us is encrypted, even if they want it or not. This is referred to as traffic-flow security.

1. End to End Encryption

**Voice calls, video calls, chats and file sharing** are good examples of End to End Encryption. These apps that use end-to-end encryption to encrypt messages between the sender and recipient. This allows secure transfer of information where data is encrypted and decrypted only at the end points.

.

1. PGP (Pretty Good Privacy)

**Apple Mail** is an example of PGP (Pretty Good Privacy).

PGP generates and manages your public and private keys which integrates with Apple Mail. Once the keys are generated, the message will be encrypted with the public key. After sending the mail to a friend. Your friend will not be able to see the content of the mail until he decrypts it using the private key.

1. S/MIME

**E-mails** are the good example of S/MIME.

S/MIME is based on asymmetric cryptography which uses pair of mathematically related keys that operate a public key and private key. When an email received contains an audio clip, graphic, or some other type of multimedia component, this will send the file with a header that describes the file type. For example, the header might be indicating that MIME type is Image and that subtype will be jpeg.

1. PEM (Privacy Enhanced Mail)

**E-mail** is an example of Privacy-Enhanced Mail (PEM).

It allows confidentiality, sender authentication, and message integrity.

Confidentiality allows a message to be keep the message secret from everyone. Sender authentication allows user to authorized that message have been actually send by author. Message integrity allows user to ensure that a message has not been modified or altered during transportation.

(**2 marks)**