Week 3 Assignment

[Name of the Writer]

[Name of the Institution]

Week 3 Assignment

Symmetric key cryptography algorithms use the same keys for both encryption and decryption. Some of the advantages of symmetric key cryptography are that it is faster, the encrypted data can be sent on the link that can intercept the data because the decryption key is not sent with the data so the data remains safe. It uses password authentication and the system that has the decryption key can open the message. The disadvantages are that to decode a message, a key must be sent to the receiver before the transmission of the actual message. However, no electronic medium of communication is safe so a third party might intercept. Also, it does not have digital signatures that cannot be rejected. It can be used for several payment applications such as credit card transactions (Tripathi & Agrawal, 2014).

  The asymmetric cryptography uses two keys that are a public and private key. The public key is distributed openly. In this type of cryptography, the encryption of messages can be done by any person using the public key of the receiver however the message can only be decrypted by the private key. The advantage is that there is no need for a key exchange like in symmetric cryptography. It also has digital signatures and is very secure. The disadvantage of the asymmetric key is speed.

The study of information systems that are ciphertext, ciphers, and cipher systems is called cryptanalysis. Several types of cryptanalysis attacks, as well as techniques, are known however it depends upon the information of the ciphertext provided to the analyst (Simmons, 1993). Some of the techniques are as follow:

* Ciphertext only attacks: Hacker can only access a few encrypted messages but does not know about the plain text and the encryption algorithm being used.
* Known plain text attack: Attacker has some information regarding plain text and only needs a key to decrypt a message. Once a key is discovered all the messages can be decrypted.
* Chosen plain text attack: Either the encryption algorithm or the device that was used for the encryption is known by the attacker.
* Side-channel attack: This attack focuses on the power consumed by the system that performed encryption. As during the process, electromagnetic radiations are emitted that can be used by the hacker.
* Man-in-the-middle attack: Attackers try to intercept the communication between two parties that are about to share keys. The attacker impersonates one of the party and performs the key exchange process with the other party.
* Brute force attack: These attacks refers to the attacks in which the attacker try all possible combinations of key until the right one is identified. It is very costly and time-consuming.

  CPTED stands for crime prevention through environmental design. It is a design to build an environment safe that will improve the quality of life and reduce fear and threat of any crime occurrence. The three concepts that are used in CPTED are natural access control that involves the reduction in the opportunities for crime by reducing the access to crime targets. The other is natural surveillance that promotes the visibility of people so that intruders can be easily observed and identified. The third one is natural territorial reinforcement is to create a sphere of influence that discourages criminal intentions. CPTED design is based on anticipating the thought process of an offender by creating an environment that discourages the follow-through. CPTED has increased not only the sense of security among the employees as well as the wellbeing of the employees. After the implementation of CPTED, the environment surrounding the organization will discourage any criminal behavior while encouraging honest employees. Thus the basic purpose of CPTED is to prevent certain crimes in a controlled environment (Cozens & Hillier, 2005).

**References**

Cozens, P. M., Saville, G., & Hillier, D. (2005). Crime prevention through environmental design (CPTED): a review and modern bibliography. *Property management*, *23*(5), 328-356.

Simmons, G. J. (1993, December). Cryptanalysis and protocol failures. In *Proceedings of the 1st ACM conference on Computer and communications security* (pp. 213-214). ACM.

Tripathi, R., & Agrawal, S. (2014). Comparative study of symmetric and asymmetric cryptography techniques. *International Journal of Advance Foundation and Research in Computer (IJAFRC)*, *1*(6), 68-76.