Week 3 Essay Questions

Student’s Name:

Institutional Affiliation:

**Week 3 Essay Questions**

**Question 1**

The advantages of the symmetric cryptosystem include being faster, it uses password identification for proving the identity of the receiver, and it has the secret key for decrypting a message (Fujisaki & Okamoto, 2014). The disadvantage of symmetric cryptosystem is that it has a problem of critical transportation and it cannot provide the digital signatures that cannot be retracted. One use of the asymmetric cryptosystem is that it is used in payment applications like card transactions.

The advantage of the asymmetric cryptosystem is that there is no needed for the exchanging keys hence eliminating the problem of key distribution, it has increased security and can give the digital signatures which can be retracted. The disadvantage of the asymmetric cryptosystems is a bit slower compared to another public key encryption method. An asymmetric cryptosystem is used for encrypting messages to provide confidentiality.

**Question 2**

Cryptanalysis involves the learning of analyzing the IS (information systems) to learn the features of the systems. It is utilized to breach the cryptographic structures of security and attain admission to the encrypted messages subjects (Biham & Shamir, 2014).

The commonly used cryptanalytic techniques in attacks are:

 The chosen plaintext attack- the analysts, has access to the device or knows the encryption algorithm utilized during encryption (Biham & Shamir, 2014). The analyst can encrypt the selected plaintext with the algorithm targeted to attain the information concerning the key.

The differential cryptanalysis attack- it is the type of the selected plaintext attack on the block ciphers which analyses plaintext pairs instead of the single plaintexts. Hence the analyst can establish how the directed algorithm is working when it meets various types of information.

**Question 3**

CPTED is the agenda for manipulation of the stable environment to establish safer neighborhoods. It is an aesthetic alternative to the classic target of hardening approaches. The strategies compromise of the natural surveillance that increases the risk perceived of the attempting wrong actions through improvement of the visibility of the probable offenders to the public (Cozens et al., 2015). The natural access control strategy limits the chances of crime happening by taking steps to differentiate between private space and public space. Through selective placement of exits, entrances, landscape, lightning, and fence to limit the control flow and access, the natural access control happens.

 References

Biham, E., & Shamir, A. (2014). Differential cryptanalysis of DES-like cryptosystems. *Journal of CRYPTOLOGY*, *4*(1), 3-72.

Cozens, P. M., Saville, G., & Hillier, D. (2015). Crime prevention through environmental design (CPTED): a review and modern bibliography. *Property management*, *23*(5), 328-356.

Fujisaki, E., & Okamoto, T. (2014. August). Secure integration of asymmetric and symmetric encryption schemes. In *Annual International Cryptology Conference* (pp. 537-554). Springer, Berlin, Heidelberg.