CS4331/CS5342 Network Security
Homework 1

Q.1. False (F) or True (T) and justify the answer (27 points)

a) In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure; the rest are parity bits.
b) 4 keys does the Triple DES algorithm use?
c) Like DES, AES also uses Feistel Structure.
d) There is an addition of a round key before the start of the AES round algorithms.
e) If the sender and receiver use different keys, the system is referred to as a conventional cipher system.
f) Symmetric Block Cipher provides authentication and confidentiality.
g) Plain text is the data after encryption is performed.
h) X.800 architecture was developed as an international standard and focuses on security in the context of networks and communications.
i) Data integrity assures that information and programs are changed only in a specified and authorized manner.

Q.2. Short answer Questions (21 points)

a) Release of message contents and traffic analysis are two types of _____attacks.
b) Replay, masquerade, modification of messages, and denial of service are examples of _____ attacks.
c) A _____ processes the plaintext input in fixed-size blocks and produces a block of ciphertext of equal size for each plaintext block.
d) A _____ processes the input elements continuously, producing output one element at a time.
e) With the use of symmetric encryption, the principal security problem is to maintain the secrecy of the encryption _____.
f) AES's advantage is that most operations can be combined into _____ and _____.
g) What is the entropy of a uniform random distribution over 16 values _____ bits.

Q.3. List and briefly define the three main basic security requirements (5 points)

Q.4. What is symmetric encryption? What are the five ingredients? (5 points)

Q.5. What are unconditional security and computational security? (5 points)

Q.6. What are Shannon's Diffusion and Confusion, and corresponding methods to achieve them? (5 points)

Q.7. What are the criteria to evaluate a cipher, such as AES? (6 points)

Q.8. What are the properties of true random numbers? (6 points)

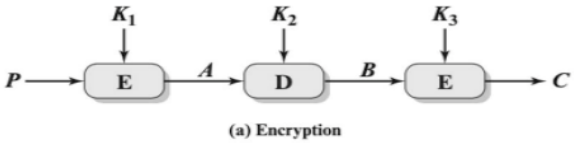
Q.9. What are Pseudorandom Number Generator's (PRNG) properties? (6 points)

Q.10. Consider a very simple symmetric block encryption algorithm in which 64-bit blocks of plaintext are encrypted using a 128-bit key. Encryption is defined as

$$C = (P \oplus K0) \boxplus K1$$

Where C = ciphertext, K = secret key, K0 = leftmost 64 bits of K, K1 = rightmost 64 bits of K, $\oplus$ = bitwise exclusive OR, and $\boxplus$ is addition mod 2^{64}, Show the decryption equation. That shows the equation for P as a function of C, K0, and K1. (7 points)

Q.11. The Figure shows the Triple DES encryption process. P is plaintext. C is ciphertext. (7 points)



(a) Encryption

a. Write the decryption equation.
b. Write the encryption equation.