CS4331/CS5342 Network Security
Homework 1

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

1. In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits.
   False. DES uses 56 bits for encryption, not 48 bits. The remaining 8 bits are parity bits, which are used to check for errors in the key.
2. 4 keys does the Triple DES algorithm use?
   False. Triple DES uses three DES keys, not four.
3. Like DES, AES also uses Feistel Structure.
   False. AES uses a substitution-permutation network (SPN) structure, not a Feistel structure.
4. There is an addition of round key before the start of the AES round algorithms.
   True. A round key is added before the start of each AES round algorithm.
5. If the sender and receiver use different keys, the system is referred to as conventional cipher system.
   False. A conventional cipher system uses the same key for encryption and decryption. If the sender and receiver use different keys, the system is referred to as an asymmetric cipher system, or public key encryption.
6. Symmetric Block Cypher provides authentication and confidentiality.
   True, AES is one such example. It aids in the protection of critical information.
7. Plain text is the data after encryption is performed.
   False. Plaintext is the data before encryption is performed. Ciphertext is the data after encryption is performed.
8. X.800 architecture was developed as an international standard and focuses on security in the context of networks and communications.
   True. X.800 is an international standard for security in networks and communications.
9. Data integrity assures that information and programs are changed only in a specified and authorized manner.
   True. Data integrity assures that information and programs are changed only in a specified and authorized manner.

Q.2. Short answer Questions (21 points)

1.Release of message contents and traffic analysis are two types of **passive** attacks.
2.Replay, masquerade, modification of messages, and denial of service are examples of **active** attacks.
3.A **block cipher** processes the plaintext input in fixed-size blocks and produces a block of ciphertext of equal size for each plaintext block.
4.A **stream cipher** processes the input elements continuously, producing output one element at a time.
5.With the use of symmetric encryption, the principal security problem is to maintain the secrecy of the encryption **key.**

6.AES's advantage is that most operations can be combined into **XOR** and **substitution**.
7.What is the entropy of a uniform random distribution over 16 values **4 bits**.

Q.3. List and briefly define the three main basic security requirements (5 points)
The three main basic security requirements are:
Confidentiality: Confidentiality ensures that data is only accessible to authorized individuals.
Integrity: Integrity ensures that data is accurate and complete, and that it has not been altered without authorization.
Availability: Availability ensures that data and systems are accessible to authorized individuals when they need them.

Q.4. What is symmetric encryption? What are the five ingredients? (5 points)
Symmetric encryption is a type of encryption where the same key is used to encrypt and decrypt data. The five ingredients of symmetric encryption are:

The five ingredients in symmetric encryption are:
1. Plaintext: This is the actual data or message the user is intending to send to the receiver.
2. Secret Key: This is a key that is fed as an input to the algorithm and the output ciphertext is generated based on the secret key.
3. Encryption algorithm: This is an algorithm that refers to various substitutions and transformations on the plaintext.
4. Ciphertext: This is the encrypted message that is generated as an output upon applying the encryption algorithm on the plaintext along with the secret key.
5. Decryption algorithm: This algorithm is a reverse of the actual encryption algorithm, generates the plain text as output by using secret key as an input on the cipher text.

Q.5. What are unconditional security and computational security? (5 points)
Unconditional security is a type of security where it is impossible for an attacker to break the encryption, even with infinite resources.
Computational security is a type of security where it is impractical for an attacker to break the encryption with the resources that are currently available.

Q.6. What are Shannon's Diffusion and Confusion and corresponding methods to achieve them? (5 points)
Diffusion and confusion are two fundamental concepts in cryptography. Diffusion spreads the influence of each bit of the plaintext over many bits of the ciphertext. Confusion makes it difficult to determine the relationship between the plaintext and ciphertext.
Some corresponding methods to achieve diffusion are:
Block ciphers: Block ciphers divide the plaintext into blocks of a fixed size and encrypt each block independently. This helps to spread the influence of each bit of the plaintext over many bits of the ciphertext.
Stream ciphers: Stream ciphers encrypt the plaintext one bit at a time. This helps to make it difficult to determine the relationship between the plaintext and ciphertext.
Some corresponding methods to achieve confusion are:
Substitution: Substitution ciphers replace each byte of the plaintext with a different byte. This helps to make the relationship between the plaintext and ciphertext more difficult to determine.
Permutation: Permutation ciphers rearrange the order of the bits in the plaintext. This also helps to make the relationship between the plaintext and ciphertext more difficult to determine.

Q.7. What are the criteria to evaluate a cipher, such as AES? (6 points)
General security
Software implementations
Restricted-space environments
Hardware implementations
Attacks on implementations
Encryption versus decryption
Key agility
Other versatility and flexibility
Potential for instruction-level parallelism

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

1. Randomness

- **a. Uniformity**
  - **i. distribution of bits in the sequence should be uniform.**
- **b. Independence**
  - **i. no one subsequence in the sequence can be inferred from the others.**

2. Unpredictable

- **a. satisfies the "next-bit test"**

Q.9.What are Pseudorandom Number Generator's (PRNG) properties? (6 points)
The properties of pseudorandom number generators are as follows:
1. **Correctness:** the pseudorandom number generator should be able to generate the random numbers deterministically.
2. Efficiency: The algorithm should be efficient enough to generate the bits in the pseudorandom
number.
3. Security: The algorithm should not be predictable by attackers even if the initial state or seed
value is known.
4. Rollback resistance: The bits generated should not deduce anything about any previously generated bits.

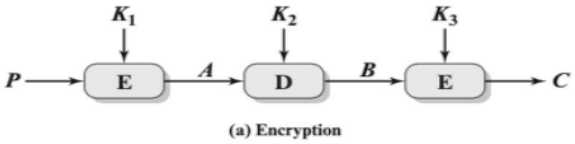
Q.10. Consider a very simple symmetric block encryption algorithm in which 64-bits blocks of plaintext are encrypted suing a 128-bit key. Encryption is defined as

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

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 264, Show the decryption equation. That is show the equation for P as a function of C, K0 and K1. (7 points)

The decryption equation for the given symmetric block encryption algorithm is:
$P = (C \boxplus K1) \oplus K0$
In the above equation first, we decrypt the leftmost 64 bits using the bitwise exclusive or operation and then decrypt the rightmost 64 bits using the addition mod 2^{64}.

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



(a) Encryption

(1) Write decryption equation.
(2) Write encryption equation.

Decryption equation for the Triple DES encryption process:
P = D(K1, E(K2, D(K3, C)))
Encryption equation for the Triple DES encryption process:
C = E(K3, D(K2, E(K1, P)))
where:

- P is the plaintext
- C is the ciphertext
- K1, K2, and K3 are the three DES keys

The decryption equation is simply the reverse of the encryption equation.