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 48 bits are used for the encryption procedure; the rest are parity bits.

Ans: False, The remaining 8 bits are parity bits, so 56 bits are used.

2. 4 keys does the Triple DES algorithm use?

Ans: False, in triple DES, we use three different keys .

3. Like DES, AES also uses Feistel Structure.

Ans: False, AES does not use a Feistel structure.

Instead, each full round consists of four separate functions:

- Byte substitution
- Permutation: shift rows (permute bytes row by row)
- Mix Operation: mix columns (alter each byte in a column as a function of all the bytes in the column)
- XOR with a key

4. There is an addition of round key before the start of the AES round algorithms.

Ans: True, the final round of AES round algorithms consists of three transformations, the first of which is the single transformation known as “Add round key” before the first round.

5. If the sender and receiver use different keys, the system is referred to as conventional cipher system.

Ans: False, Asymmetric, two-key, or public-key cipher systems are examples of such systems.

6. Symmetric Block Cypher provides authentication and confidentiality.

Ans: True, AES is one such example. It aids in the protection of critical information.

7. Plain text is the data after encryption is performed.

Ans: False, the algorithm used in encryption is known as cipher. The data following encryption is known as ciphertext.

8. X.800 architecture was developed as an international standard and focuses on security in the context of networks and communications.

Ans: True, The X.800 architecture was created as an international standard to address network and communication security.

9. Data integrity assures that information and programs are changed only in a specified and authorized manner.

Ans: True, In addition to ensuring that data is accurate, consistent, and dependable, data integrity is essential for maintaining data's dependability and trustworthiness.

Q.2. Short Answer Questions (21 points)

1. Release of message contents and traffic analysis are two types of ___ attacks.

Answer: Passive

2. Replay, masquerade, modification of messages, and denial of service are examples of ___ attacks.

Answer: Active

3. A ___ processes the plaintext input in fixed-size blocks and produces a block of ciphertext of equal size for each plaintext block.

Answer: Block Cipher

4. A ___ processes the input elements continuously, producing one element at a time.

Answer: Stream Cipher

5. With the use of symmetric encryption, the principal security problem is to maintain the secrecy of ___.

Answer: Key

6. AES's advantage is that most operations can be combined into ___ and ___.

Answer: XOR and table lookups

7. What is the entropy of a uniform random distribution over 16 values?

Answer: 4 bits

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

- Confidentiality: Ensures that any data is not accessible to unauthorized users.
- Integrity: Maintains that data is accurate and has not been altered.
- Availability: Ensures that systems are available for authorized users.

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

Symmetric Encryption: A type of encryption where the same key is used for both encryption and decryption.

The five ingredients:

1. Plaintext: The actual data to be encrypted.
2. Secret Key: Input to the encryption algorithm.
3. Encryption Algorithm: Performs transformations on plaintext.
4. Ciphertext: The encrypted output.
5. Decryption Algorithm: Reverses the encryption to produce plaintext.

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

- Unconditional Security: The cipher cannot be broken even with unlimited computational power.
- Computational Security: Breaking the cipher would require more resources than the value of the information.

Q.6. What are Shannon's Diffusion and Confusion? (6 points)

- Confusion: Ensures that a change in the key affects the ciphertext significantly.
- Diffusion: Ensures that changing one plaintext bit affects the ciphertext widely.

Q.7. What are the criteria to evaluate a cipher, such as AES? (5 points)

- General security
- Software implementations
- Restricted space environments
- Hardware implementations
- Attacks on implementations
- Encryption vs decryption
- Key agility
- Instruction-level parallelism

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

1. Randomness
   - Uniformity: Bits should be uniformly distributed.
   - Independence: No subsequence can infer others.
2. Unpredictability
   - Satisfies the “next-bit test.”

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

1. Correctness: Produces random numbers deterministically.
2. Efficiency: Generates bits quickly.
3. Security: Not predictable by attackers.
4. Rollback Resistance: Previous bits cannot be inferred.

Q.10. Decryption equation for simple symmetric block encryption (7 points)

Decryption Equation:

OBJ.

Q.11. Triple DES encryption process (7 points)

1. Decryption Equation:

OBJ.

2. Encryption Equation:

OBJ.