CS4331/CS5342 Network Security
Homework 1_Solution

Q.1. False (F) or True (T) and justify the answer (36points)

1 An encryption scheme is unconditionally secure if the ciphertext generated does not contain enough information to determine uniquely the corresponding plaintext, no matter how much cipher text is available.

Ans: **True**, The definition of unconditionally secure cipher systems can be found in the statement above.

2 In the DES algorithm, although the key size is 64 bits only 48bits 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.

3 In the DES algorithm the 64-bit key input is shortened to 56 bits by ignoring every 4th bit.

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

4 The "A" in the CIA triad stands for "Authenticity".

Ans: **False**, A model used to represent three fundamental principles is the CIA triad.

5 4 keys does the Triple DES algorithm use?

Ans: **False**, For Triple DES algorithm we can use 2 or 3 keys.
Using 2 keys: c = Ek1(Dk2(Ek1(m)))
Using 3 keys: c = Ek3(Ek2(Ek1(m)))

6 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
- arithmetic operations over a finite field, and
- XOR with a key

7 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, which is called "Round 0."

8 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

9 Network Security provides authentication and access control for resources.

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

10 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.

11 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.

12 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 (16 points)

1. Release of message contents and traffic analysis are two types of _____ attacks.
2. Replay, masquerade, modification of messages, and denial of service are example of _____ attacks.
3. A _____ processes the plaintext input in fixed-size blocks and produces a block of ciphertext of equal size for each plaintext block.

4. A_____ processes the input elements continuously, producing output one element at a time?
5. A_____ stream is one that is unpredictable without knowledge of the input key and which has an apparently random character.
6. The _____ is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption.
7. With the use of symmetric encryption, the principal security problem is to maintain the secrecy of_____
8. AES's advantage is that all operations can be combined into _____ and_____.

Answer:

1. Passive
2. Active
3. Block cipher
4. Stream Cipher
5. Pseudorandom
6. Public and Private Key
7. Key
8. XOR and table lookups

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

Ans: The three main basic security requirements are Confidentiality, Integrity, and Availability.

Confidentiality: This requirement makes sure that any data that is private is not accessible to any unauthorized users.

Integrity: Integrity makes sure that the data in transmission between send and receiver is not prone to any modification or alteration. In general, there are two types of integrity namely, data integrity and system integrity.

Availability: This makes sure that the systems are always available to respond to a user's request who are authorized.

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

Ans: **Symmetric encryption**: Symmetric encryption is a type of encryption where the same key(also referred to as public key) is used to encrypt as well as decrypt the plain text given.

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 the differences between unconditional security and computational security? (5 points)

Ans:

	Unconditional Security	**Computational Security**
Definition	It is made sure that system is secure against all possible attacks	it is made sure that the system is secure against only feasible attacks
Achievability	It is theoretically achievable but practically not	Practical to implement
Complexity	Complex and difficult to implement	It is simple and used widely
Limitations	It is limited by mathematical models and may not be applicable to all types of data /applications	It is adaptive and optimized for a wide range of applications and data types.

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

Ans: Confusion refers to making the relationship between the ciphertext and the symmetric key as complex and involved as possible; Diffusion refers to dissipating the statistical structure of plaintext over the bulk of ciphertext.

Shannon's Diffusion:

1. In this the bits in the plain text are reorganized about the string to create cryptic plain texts.
2. It is achievable with the help of transposition algorithms.
3. Only block cipher uses diffusion.
4.

Shannon's Confusion:

1. In this the bits in the plain text are replaced by other bits thus causing confusion about the plain text.
2. It is achievable with the help of substitution algorithms.
3. Both stream and block ciphers use confusion.

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

Ans:

- 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? (5 points)

Ans:

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)

Ans:

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** **(6 points)**

$$C = (P \oplus K_0) \boxplus K_1$$

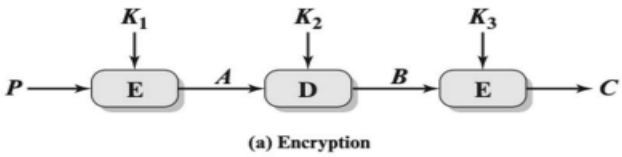
Where C = ciphertext, K = secret key, K_0 = leftmost 64 bits of K, K_1 = rightmost 64 bits of K, $\oplus$ = bitwise exclusive OR, and $\boxplus$ is addition mod 2^{64}, Show the decryption equation. That is show the equation for P as a function of C, K_0 and K_1. (6 points)

Ans: The decryption equation for the above given scenario could be formed as follows:

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

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.** **(6 points)**



(a) Encryption

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

Ans: Let the following be notations used to write the statements:

E(K,X) = encryption of X using key K

D(K,Y) = decryption of Y using key K

1. The decryption equation would be:

   P = D(K1, E(K2, D(K3, C)))

2. The encryption equation would be:

   C = E(K3, D(K2, E(K1, P)))