CS4331/CS5342 Network Security
Homework 1

Submitted By:
Ashlesha Malla
R#: R11904228

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**
  Instead of 48 bits, 56 bits are used, and the rest are parity bits.

2. 4 keys does the Triple DES algorithm use?

- **False**
  Triple DES uses three keys, not four C = 3(K_3, D($K_{2,}$ E(K_1, P)))

3. Like DES, AES also uses Feistel Structure.

- **False**
  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.

- **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.

- **False**
  It usually refers to an asymmetric or public-key encryption system rather than a conventional cipher system.

6. Symmetric Block Cypher provides authentication and confidentiality.

   - **False**
     AES is one such example. It aids in the protection of critical information.

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

   - **False**
     Ciphertext is the data after encryption is performed, not plain text.

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

   - **True**
     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.

   - **True**
     In addition to ensuring that the 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 **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 key**.

6. AES's advantage is that most operations can be combined into **XOR** and **table lookups**.

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 requirements form the foundation of information security and are referred to as the CIA triad, representing Confidentiality, Integrity, and Availability.

a. **Confidentiality**
   Confidentiality in information security assures that information is accessible only by authorized individuals. It involves the actions of an organization to ensure data is kept confidential or private.

b. **Integrity**
   Integrity guarantees that data is correct and undamaged while being stored, processed, or transmitted. It guards against tampering or unauthorized modifications.

c. **Availability**
   Availability indicates that networks, systems, and applications are up and operating. It assures that authorized users have timely, trustworthy access to resources when they are required.

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

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

The five ingredients of symmetric encryption are:

a. **Plaintext**: This is the original message or data that is fed into the algorithm as input.
b. **Encryption algorithm**: The encryption algorithm performs various substitutions and transformations on the plaintext.
c. **Secret key**: The secret key is also input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.
d. **Ciphertext**: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.
e. **Decryption algorithm**: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

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

a. **Unconditional security**
   A level of security that is theoretically flawless is known as unconditional security, commonly referred to as information-theoretic security. Regardless of the adversary's computing power, a system is said to be unconditionally secure if the encrypted data doesn't contain any information that could help them crack the encryption. In other words, despite having infinite computational capacity, communication cannot be decrypted by an enemy.
   One Time Pad (OTP) is the only example of unconditional security.

b. **Computational security**
   The foundation of computational security, also referred to as computational complexity security, is the idea that some mathematical problems are computationally challenging even for strong attackers. The encryption may theoretically be broken, but doing so would require an impractical amount of time or processing power. In computational security, it is assumed that adversaries have limited computational resources.
   Most modern cryptographic systems, like AES and RSA, are designed with computational security in mind.

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

Shannon's Diffusion

Diffusion means that changing one bit in the plaintext changes approximately half the bits in the ciphertext, and similarly changing one bit in the ciphertext changes approximately half the bits in the plaintext. In a cipher with good diffusion, if one bit of the plaintext is changed, then the ciphertext should change completely, in an unpredictable or pseudorandom manner. For example, diffusion ensures that any patterns in the plaintext, such as redundant bits, are not apparent in the ciphertext.
Shannon's Diffusion is achieved through Transposition or Permutation algorithm.
In transposition, the positions of elements within a block are shuffled according to a specific pattern or key. This rearrangement does not change the actual values of the elements, but it alters their positions, which can significantly obscure the original information.

Shannon's Confusion

Confusion means that each binary digit (bit) in the ciphertext depends on some part of the key, obscuring the connection between the two. The chaos property hides the relationship between the ciphertext and the key. This property makes it difficult to find the key from the

ciphertext, and if one bit of the key is changed, the computation of most or all bits of the ciphertext is affected.
Shannon's Confusion is achieved through Substitution algorithm.
In the field of cryptography, a substitution algorithm is a method for encrypting data by swapping out characters or bits for other elements in accordance with a predetermined rule or key. This procedure is an essential part of many encryption techniques, particularly those based on symmetric key cryptography.

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

The criteria to evaluate a cipher, such as AES are:

a. General security
b. Software implementation
c. Restricted space environments
d. Hardware implementations
e. Attacks on implementations
f. Encryption versus decryption
g. Key agility
h. Other versatility and flexibility
i. Potential for instruction-level parallelism

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

The properties of true random numbers are:

a. **Unpredictability**: Genuine random numbers are impossible to predict. Knowing one random number should not make it feasible to forecast the next.

b. **No Correlation**: Successive values of true random numbers should show no correlation. In other words, knowledge of one number should not offer any insights into the next.

c. **Independence**: Each generated random number should be entirely independent of preceding and subsequent numbers.

d. **Uniformity**: In a series of true random numbers, every potential value should have an equal likelihood of appearing. This guarantees an even spread across the entire range.

e. **No Algorithmic Generation**: Genuine random numbers cannot be produced by any algorithm, regardless of its complexity.

f. **Unbiasedness**: True random numbers should not display any inclination towards specific values or patterns.

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

Pseudorandom Number Generator is a mechanism for generating random numbers on a computer that are indistinguishable from truly random numbers.
It is pseudo random because it is not possible to generate truly random numbers from deterministic things like a computer.

The properties of Pseudorandom Number Generator are:

a. **Correctness:** the pseudorandom number generator should be able to generate the random numbers deterministically.
b. **Efficiency:** The algorithm should be efficient enough to generate the bits in the pseudorandom number.
c. **Security:** The algorithm should not be predictable by attackers even if the initial state or seed value is known.
d. **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 using a 128-bit key. Encryption is defined as

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

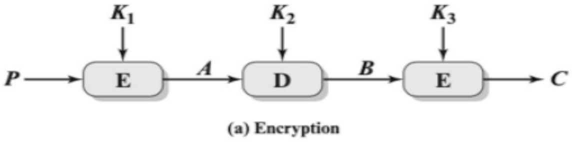
Where C = ciphertext, K = secret key, K0 = leftmost 64 bits of K, K1 = rightmost 64 bits of K, $\oplus$ = bitwise exclusive OR, and $\boxplus$ is addition mod 2^{64}, Show the decryption equation. That is show the equation for P as a function of C, K0 and K1. (7 points)

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

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

In the above equation first, we decrypt the leftmost 64 bits using the bitwise exclusive or operation and the 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.

We start by decrypting the ciphertext C using key K_3. Then, encrypting the resulting output with key K_2 and finally decrypting it using key K_1.

$$P = D(K_{1,} E(K_2, D(K_3, C)))$$

(2) Write encryption equation.

We start by encrypting the plaintext using key K_1. Next, decrypting the resulting ciphertext with key K_2, and finally, encrypting it once more using key K_3.

$$C = E(K_{3,} D(K_2, E(K_1, P)))$$