
**Name:** **Jonathan Mazenge**

**Reg. Number:** **R206679P**

**Course:** **Information Security**

# Assignment 2

1 a) State and explain the properties of Hash Functions [9]

Properties of Hash Functions
In order to be an effective cryptographic tool, the hash function is desired to possess following properties −

Pre-Image Resistance

This property means that it should be computationally hard to reverse a hash function.

In other words, if a hash function h produced a hash value z, then it should be a difficult process to find any input value x that hashes to z.

This property protects against an attacker who only has a hash value and is trying to find the input.

Second Pre-Image Resistance

This property means given an input and its hash, it should be hard to find a different input with the same hash.

In other words, if a hash function h for an input x produces hash value h(x), then it should be difficult to find any other input value y such that h(y) = h(x).

This property of hash function protects against an attacker who has an input value and its hash, and wants to substitute different value as legitimate value in place of original input value.

Collision Resistance

This property means it should be hard to find two different inputs of any length that result in the same hash. This property is also referred to as collision free hash function.

In other words, for a hash function h, it is hard to find any two different inputs x and y such that h(x) = h(y).

Since, hash function is compressing function with fixed hash length, it is impossible for a hash function not to have collisions. This property of collision free only confirms that these collisions should be hard to find.

This property makes it very difficult for an attacker to find two input values with the same hash.

Also, if a hash function is collision-resistant then it is second pre-image resistant.

b) Difference between Cyber Security and Information Security [6]

The NIST defines cybersecurity as protecting, preventing damage to and restoring electronic communications services and systems. This includes the information stored in these systems, which cybersecurity professionals work to protect.
According to the NIST, infosec involves the protection of information and information systems against unauthorized use. The field aims to provide availability, integrity and confidentiality. Information security is an overarching term for creating and maintaining systems and policies to protect any information—digital, physical or intellectual, not just data in cyberspace.

An information security expert may develop the means of data access by authorized individuals or establish security measures to keep information safe. Cybersecurity, on the other hand, focuses on protecting information from cyberattacks such as ransomware and spyware.

c) State and describe three security services provided by a digital signature [9]

Message authentication − When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.

Data Integrity − In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.

Non-repudiation − Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

d) Briefly explain the following
i)Differential Cryptanalysis [3]

Differential cryptanalysis is a branch of study in cryptography that compares the way differences in input relate to the differences in encrypted output. It is used primarily in the study of block ciphers to determine if changes in plaintext result in any non-random results in the encrypted ciphertext. This process is important because non-random changes to the ciphertext may signify a weakness in the encryption scheme. An unauthorized third-party may gain information about what was encrypted or how it was encrypted by monitoring data changes.

ii) Linear Cryptanalysis [3]

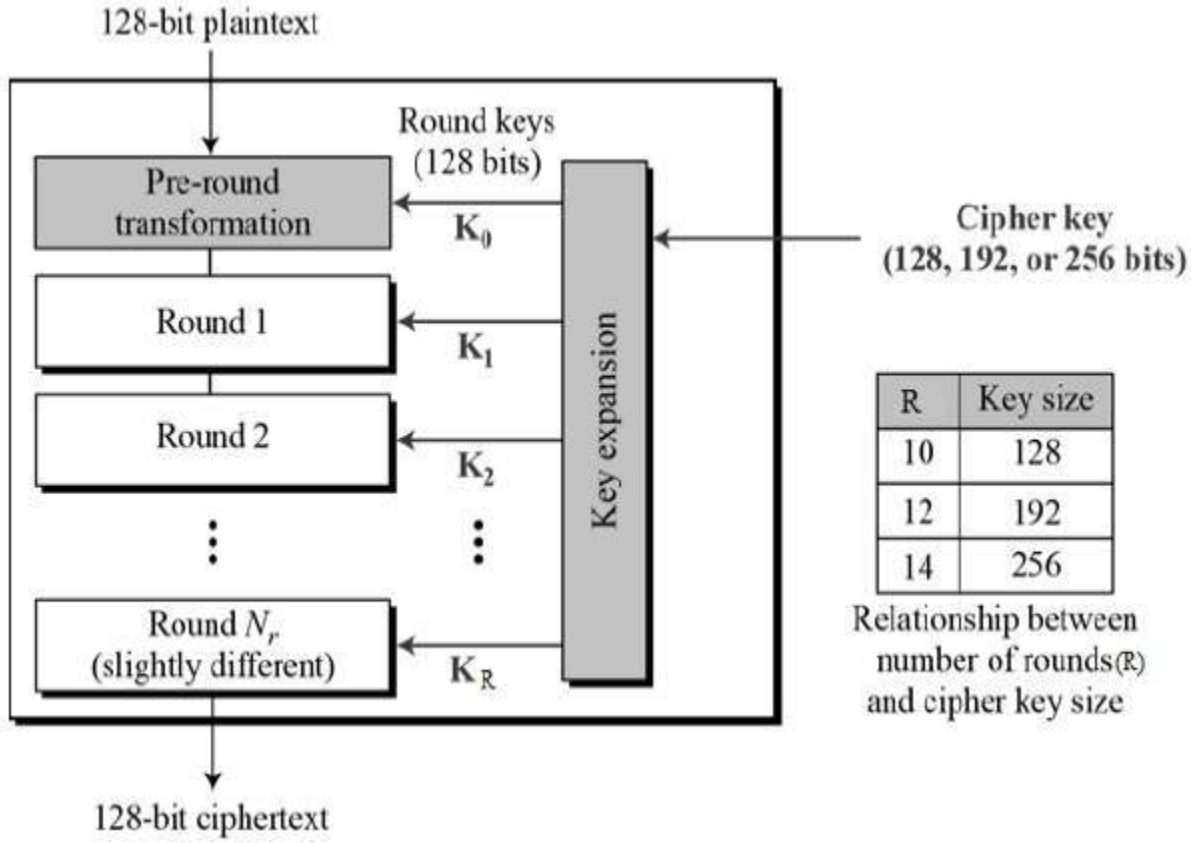
Linear cryptanalysis is a known plaintext attack in which the attacker studies probabilistic linear relations (called linear approximations) between parity bits of the plaintext, the ciphertext, and the secret key. Given an approximation with high probability, the attacker obtains an estimate for the parity bit of the secret key by analyzing the parity bits of the known plaintexts and ciphertexts. Using auxiliary techniques, he or she can usually extend the attack to find more bits of the secret key.

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration −




| R | Key size |
|---|---|
| 10 | 128 |
| 12 | 192 |
| 14 | 256 |

Relationship between number of rounds (R) and cipher key size

AES Structure

b) The AES (Advanced Encryption Standard) algorithm was developed to replace the DES (Data Encryption Standard) Algorithm, state and describe the criteria that were used by NIST to select the best AES [6]

One of the original requirements from the National Institute of Standards and Technology (NIST) for the DES replacement algorithm was that it had to be efficient both in software and hardware implementations. (DES was originally practical only in hardware implementations.) Java and C reference implementations were used to do performance analysis of the algorithms. AES was chosen through an open competition with 15 candidates from as many research teams around the world, and the total amount of resources allocated to that process was tremendous.

Finally, in October 2000, a NIST press release announced the selection of Rijndael as the proposed Advanced Encryption Standard (AES).

| | DES | AES |
|---|---|---|
| Developed | 1977 | 2000 |
| Key Length | 56 bits | 128, 192, or 256 bits |
| Cipher Type | Symmetric block cipher | Symmetric block cipher |
| Block Size | 64 bits | 128 bits |
| Security | Proven inadequate | Considered secure |

c) Explain the properties that satisfy Message Authentication Code (MAC) [6]

MAC stands for Message Authentication Code. Here in MAC, sender and receiver share same key where sender generates a fixed size output called Cryptographic checksum or Message Authentication code and appends it to the original message. On receiver's side, receiver also generates the code and compares it with what he/she received thus ensuring the originality of the message. These are components:

Message
Key
MAC algorithm
MAC value

d) Explain the following security threats and indicate which security goal is it a threat to:
i) Snooping
ii) Masquerading
iii) Repudiation
iv) Replaying

Snooping attacks involve an intruder listening to traffic between two machines on your network. If traffic includes passing unencrypted passwords, an unauthorized individual can potentially access your network and read confidential data.

A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack.

A repudiation attack happens when an application or system does not adopt controls to properly track and log users' actions, thus permitting malicious manipulation or forging the identification of new actions

Replay Attack is a type of security attack to the data sent over a network. In this attack, the hacker or any person with unauthorized access, captures the traffic and sends communication to its original destination, acting as the original sender. The receiver feels that it is an authenticated message but it is actually the message sent by the attacker. The main feature of the Replay Attack is that the client would receive the message twice, hence the name, Replay Attack.