UNIT 3 -2 MARKS

1. **What is a hash in cryptography?**
   A **hash function** H accepts a variable-length block of data M as input and produces a fixed-size hash value h= H(M) called as message digest as output. It is the variation on the message authentication code
2. **What is the role of a compression function in a hash function?**
   The hash algorithm involves repeated use of a compression function f, that takes two inputs and produce a n-bit output. At the start of hashing the chaining variable has an initial value that is specified as part of the algorithm. The final values of the chaining variable is the hash value usually b>n; hence the term compression
3. **What is cryptography hash function?**
   The kind of hash function needed for security applications is referred to as a **cryptographic hash function**. A cryptographic hash function is an algorithm for which it is computationally infeasible (because no attack is significantly more efficient than brute force) to find either (a) a data object that maps to a pre-specified hash result (the one-way property) or (b) two data objects that map to the same hash result (the collision-free property). Because of these characteristics, hash functions are often used to determine whether or not data has changed.
4. **What are the applications of cryptographic hash function?**
   - Message Authentication
   - Digital Signatures
   - pseudorandom function (PRF) or a pseudorandom number generator (PRNG).
5. **What are the requirements for message authentication?**
   - Disclosure
   - Traffic analysis
   - Masquerade
   - Content modification
   - Sequence modification
   - Timing modification
   - Source repudiation
   - Destination repudiation
6. **What is collision resistant attack or birthday paradox?**
   For a collision resistant attack, an adversary wishes to find two messages or data blocks, *x* and , that yield the same hash function:H(x)= H(y). This turns out to require considerably less effort than a preimage or second preimage attack. The effort required is explained by a mathematical result referred to as the **birthday paradox**. In essence, if we choose random variables from a uniform distribution in the range 0 through N-1, then the probability that a repeated element is encountered exceeds 0.5 after root(N) choices have been made. Thus, for an m -bit hash value, if we pick data blocks at random, we can expect to find two data blocks with the same hash value within root(2^m) = $2^{m/2}$ attempts
7. **List the processing logic of SHA-512**
   1. Append padding bits
   2. Append padding length
   3. Initialize hash buffer
   4. Process message in 1024 bits(128-words) blocks
   5. Output
8. **What are the security requirement for cryptography hash function?**

Table 11.1 Requirements for a Cryptographic Hash Function H

Requirement	Description
Variable input size	H can be applied to a block of data of any size.
Fixed output size	H produces a fixed-length output.
Efficiency	$H(x)$ is relatively easy to compute for any given x, making both hardware and software implementations practical.
Preimage resistant (one-way property)	For any given hash value h, it is computationally infeasible to find y such that $H(y) = h$.
Second preimage resistant (weak collision resistant)	For any given block x, it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$.
Collision resistant (strong collision resistant)	It is computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$.
Pseudorandomness	Output of H meets standard tests for pseudorandomness.

9. List down the comparison of SHA parameters

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Message Digest Size	160	224	256	384	512
Message Size	$< 2^{64}$	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Block Size	512	512	512	1024	1024
Word Size	32	32	32	64	64
Number of Steps	80	64	64	80	80

Note: All sizes are measured in bits.

10. Mention the various ways of producing authenticator or define the classes of message authentication function

• **Hash function:** A function that maps a message of any length into a fixed length hash value, which serves as the authenticator

• **Message encryption:** The ciphertext of the entire message serves as its authenticator

• **Message authentication code (MAC):** A function of the message and a secret key that produces a fixed-length value that serves as the authenticator

11. What do you meant by MAC?

It involves the use of a secret key to generate a small fixed-size block of data, known as a **cryptographic checksum** or MAC, that is appended to the message. This technique assumes that two communicating parties, say A and B, share a common secret key .When A has a message to send to B, it calculates the MAC as a function of the message and the key: **MAC = MAC(*K, M*)**

where

M = input message

C = MAC function

K = shared secret key

MAC = message authentication code

12. Differentiate MAC and Hash function?

MAC: In MAC , the secret key shared by sender and receiver. The MAC is appended to the message at the source at a time which the message is assumed or known to be correct.

Hash Function: The hash value is appended to the message at the source at time when the message is assumed or known to be correct. The hash function itself not considered to be secret.

13. List any three hash algorithm.

- MD5(message Digest version 5) algorithm
- SHA_1 (Secure Hash algorithm)
- RIPEMD_160 algorithm

14. What is the difference between weak and strong collisions resistance?

Weak collisions resistance: for any given block x, it is computationally infeasible to find y * x with H(y) = H(x). it is proportional to 2^n .

Strong collision resistance: it is computationally infeasible to find any pair (x,y) such that H(x)= H(y). it is proportional to $2^{n/2}$

15. Differentiate internal and external error control.

Internal error control:

In internal error control, an error detecting code also known as frame check sequence or checksum.

External error control:

In external error control, error detecting codes are appended after encryption.

16. What is the meet in the middle attack?

This is the cryptanalytic attack that attempts to find the value in each of the range and domain of the composition of two functions such that the forward mapping of one through the first function is the same as the inverse image of the other through the second function-quite literally meeting in the middle of the composed function.

17. Compare MD5, SHA1 and RIPEMD-160 algorithm.

	MD5	SHA-1	RIPEMD160
Digest length	128 bits	160 bits	160 bits
Basic unit of processing	512 bits	512 bits	512 bits
No.of steps	64(4 rounds of 16)	80(4 rounds of 20)	160(5 pairs rounds of 16)
Maximum message size	infinity	2^{64}-1 bits	2^{64}-1 bits
Primitive logical function	4	4	5
Additive constant used	64	4	9
Endianess	Little endian	Big endian	Little endian

18. Distinguish between direct and arbitrated digital signature?

Direct digital signature	Arbitrated Digital Signature
1.The direct digital signature involves only the communicating parties. 2.This may be formed by encrypting the entire message with the sender's private key.	1.The arbiter plays a sensitive and crucial role in this digital signature. 2. Every signed message from a sender x to a receiver y goes first to an arbiter A, who subjects the message and its signature to a number of tests to check its origin and content.

19. What are the properties a digital signature should have?

- It must verify the author and the data and time of signature.
- It must authenticate the contents at the time of signature.
- It must be verifiable by third parties to resolve disputes.

20. What requirements should a digital signature scheme should satisfy?

- The signature must be bit pattern that depends on the message being signed.
- The signature must use some information unique to the sender, to prevent both forgery and denial.
- It must be relatively easy to produce the digital signature.
- It must be relatively easy to recognize and verify the digital signature.
- It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message.
- It must be practical to retain a copy of the digital signature in storage.

21. What is digital signature?

A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. Typically the signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message.

22. What is dual signature? What it is purpose?

The purpose of dual signature is to link two messages that intended for two different recipients. To avoid misplacement of orders.

15 MARKS

1. **Describe Secure hash Algorithm in detail. (16)**
2. **Describe the MD5 message digest algorithm with necessary block diagrams. (16)**
3. **(i)Summarize CMAC algorithm and its usage.(8)**
   (ii)Describe any one method of efficient implementation of HMAC. (8)
4. **Describe digital signature algorithm and show how signing and verification is done using DSS. (16)**
5. **Explain in detail ElGamal Digital Signature scheme with an example. (16)**
6. **Explain in detail about different ways of distribution of public keys**
7. **Consider prime field q=19, it has primitive roots { 2,3,10,13,14,15}, if suppose α=10. Then write key generation by she choose X_A=16. And also sign with hash value m=14 and alice choose secret no K=5. Verify the signature using Elgamal digital Signature Scheme**