SRI VIDYA COLLEGE OF ENGINEERING & TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

QUESTION BANK

Year / Dept / Sem: IV / CSE / 07 Subject code: CS6551

Staff Name : M.Mohana SubjectName: Cryptography and Network Security

UNIT-II

PART-A (2 MARKS)

1. **What is message authentication?**

It is a procedure that verifies whether the received message comes from assigned source has not been altered. It uses message authentication codes, hash algorithms to authenticate the message.

2. **Define the classes of message authentication function.**

Message encryption: The entire cipher text would be used for authentication.

Message Authentication Code: It is a function of message and secret key produce a fixed length value.

Hash function: Some function that map a message of any length to fixed length which serves as authentication.

3. What are the requirements for message authentication?

The requirements for message authentication are

i. Disclosure: Release of message contents to any person or process not processing the appropriate cryptographic key

ii. Traffic Analysis: Discovery of the pattern of traffic between parties. In a connection oriented application, the frequency and duration of connections could be determined. In either a connection oriented or connectionless environment, the number and length of messages between parties could be determined.

iii. Masquerade: Insertion of messages into the network from a fraudulent source. This includes the creation of messages by an opponent that are purported to come from an authorized entity. Also included are fraudulent acknowledgements of message receipt or no receipt by someone other than the message recipient.

iv. Content modification: Changes to the contents of a message , including insertion, deletion, transposition, and modification.

v. Sequence modification: Any modification to a sequence of messages between parties, including insertion, deletion, and modification.

vi. Timing modification: Delay or replay of messages. In a connection oriented application, an entire session or sequence of messages could be a replay of

some previous valid session, or individual messages in the sequence could be delayed or replayed. In connectionless application, an individual message could be delayed or replayed.

vii. Source repudiation: Denial of transmission of message by source.

viii. Destination repudiation: Denial of receipt of message by destination.

4. What you meant by hash function?

Hash function accept a variable size message M as input and produces a fixed size hash code H(M) called as message digest as output. It is the variation on the message authentication code.

5. **Differentiate MAC and Hash function?**

MAC:

In Message Authentication Code, 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.

6. Any three hash algorithm.

- MD5 (Message Digest version 5) algorithm.
- SHA_1 (Secure Hash Algorithm).
- RIPEMD_160 algorithm.

7. What are the requirements of the hash function?

- H can be applied to a block of data of any size.
- H produces a fixed length output.
- H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.

8. What you meant by MAC?

MAC is Message Authentication Code. It is a function of message and secret key which produce a fixed length value called as MAC. MAC = $C_k(M)$

Where M = variable length message

K = secret key shared by sender and receiver.

$C_K(M)$ = fixed length authenticator.

9. **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.

10. **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.

11. **What is the role of compression function in 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 value of the chaining variable is the hash value usually b>n; hence the term compression.

12. **What is the difference between weak and strong collision resistance?**

Weak collision resistance	Strong resistance collision
For any given block x, it is computationally infeasible to fine $y \neq x$ wit $H(y)=H(x)$. It is proportional to 2^n	It is computationally infeasible to find any pair (x,y) such that $H(x)=H(y)$. It is proportional to $2^{n/2}$

13**. 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 constants used	64	4	9
Endianess	Little endian	Big endian	Little endian

14. 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.

15. 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.

16. 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.

PART-B

1. Explain the classification of authentication function in detail.
2. Describe MD5 algorithm in detail. Compare its performance with SHA-1.
3. Describe SHA-1 algorithm in detail. Compare its performance with MD5 and RIPEMD-160 and discuss its advantages.
4. Describe RIPEMD-160 algorithm in detail. Compare its performance with
5. Describe HMAC algorithm in detail.
6. Write and explain the Digital Signature Algorithm.
7. Briefly explain Deffie Hellman key exchange with an example. (16)
8. Write and explain the digital signature algorithm. (8) (ii) Explain in detail Hash Functions. (8)
9. Compare the Features of SHA-1 and MD5 algorithm. (8)
10. Discuss about the objectives of HMAC and it security features. (8)
11. How man in middle attack can be performed in Diffie Hellman algorithm.(4)
12. Explain in detail EIGamal Public key cryptosystem. (8)
13. Discuss clearly Secure Hash Algorithm(SHA) (8)
14. Describe the MD5 message digest algorithm with necessary block diagrams. (16)