SESSION: 24

CRYPTOGRAPHIC HASH FUNCTIONS

24.1 Aim

Understand the basic concepts of Hash Functions and Applications of Hash Functions.

24.2 Instructional Objectives

The objective of this session is to introduce the basic concepts of Hash Functions. It provides the necessary theoretical background and demonstrates the applications of Hash Functions.

24.3 Learning Outcomes

At the end of this session, you should be able to:

1. Define Hash Functions
2. List Properties of Hash Functions

24.4 Module Description

This module defines Hash function. Applications of Hash algorithms are also discussed in this module. Secure Hash Algorithm (SHA 512) algorithms are demonstrated. Calculating Hash value using two simple hash functions is also discussed. Similarly MD5 is also discussed. Message Authentication Code (MAC) algorithms are also discussed.

24.5 Session Introduction

This session describes the concepts of Hash functions, Message Authentication Codes (MAC) and applications of hash functions.

24.6 Session Description

24.6.1 Hash Functions

Hash function accepts a variable length message and produces a fied length hash value. Hash value is otherwise called as message digest Hash values are used to check integrity of messages. The following figure illustrates hash function –The equation for hash function are h=H(M)

Where M –Variable length message

H-Hash Function

h –Hash value

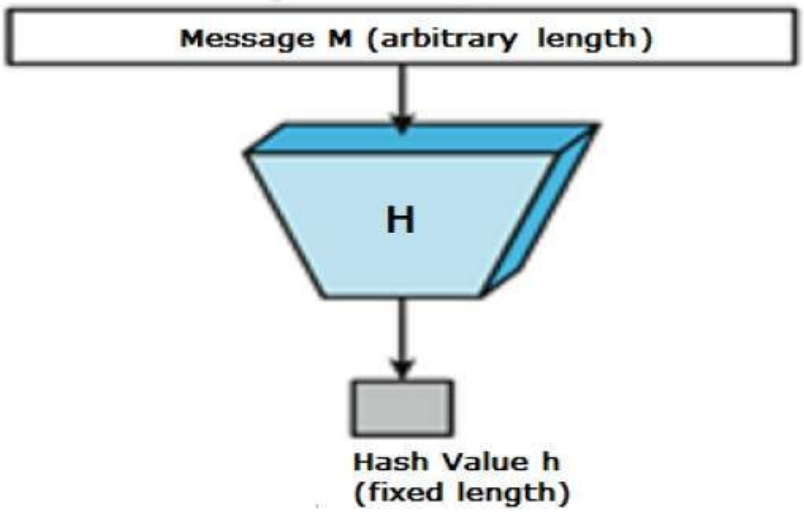


Figure: 24.1 Hash Function
Note: Copyrights of this figure are reserved with original author.

24.6.2 Properties of Hash Functions

Table 24.1 Properties of Hash Functions

Note: Copyrights of this figure are reserved with original author.

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.

24.7 Activities: NA

24.8 Examples: NA

24.9 Table Numbering

Table 24.1 Properties of Hash Functions

24.10 Figures with Captions

Figure 24.1 Hash Function

24.11 Self-Assessment Questions

1. What does a hash function's main function entail?

a) To encrypt data

b) To compress data

c) To generate a unique identifier for data

d) To sort data

2. Which characteristics need to a good hash function have?

a) Preimage resistance

b) Second preimage resistance

c) Collision resistance

d) All of the above

3. Defining collision resistance as:

a) The ability to find two different inputs that produce the same hash output

b) The ability to generate a hash output that is difficult to reverse-engineer

c) The ability to compute the hash of a given input quickly

d) The ability to prevent unauthorized modifications to the data

4. Which of the following claims regarding the hash function avalanche effect is true?

a) A small change in the input should produce a significant change in the output.

b) A small change in the input should produce no change in the output.

c) A small change in the input should produce a moderate change in the output.

d) A small change in the input should result in a collision.

5. The hash output's length is denoted by:

a) Salt b) Digest c) Key d) Block size

6. Which of the subsequent attacks looks for two inputs that result in the same hash output?

a) Preimage attack b) Collision attack c) Birthday attack d) Brute force attack

7. In hash functions, the idea of a "birthday attack" relates to:

a) Finding the original input from a given hash output

b) Finding two different inputs that produce the same hash output

c) Finding a collision by randomly trying inputs

d) Finding a preimage for a given hash output

8. Which of the following is NOT a standard hash function in cryptography?

a) MD5 b) SHA-1 c) SHA-256 d) AES

9. When a hash function consistently produces the same hash result for a given input, it is said to be:

a) Deterministic b) Non-deterministic c) Collision-resistant d) Preimage-resistant

10. Which of the following is an illustration of a hash function that is not cryptographic?

a) MD5 b) SHA-256 c) CRC32 d) HMAC

Answers:

c) To generate a unique identifier for data

d) All of the above

a) The ability to find two different inputs that produce the same hash output

a) A small change in the input should produce a significant change in the output.

b) Digest

b) Collision attack

b) Finding two different inputs that produce the same hash output

d) AES

a) Deterministic

c) CRC32

24.12 Summary

It should be emphasized that cryptographic hash functions undergo continuous scrutiny and evaluation to identify any potential vulnerabilities. Ongoing research and development efforts focus on creating newer hash functions that incorporate advanced security features. The objective is to meet the ever-changing demands of cryptography and ensure robust data protection.

24.13 Terminal Questions

1. Define Hash function

2. List the properties of Hash functions

3. Represent Hash functions in equation form.

4. Illustrate the hash function with a neat diagram.

5. Define One way property of hash function.

24.14 Answer Key

1. Hash function accepts a variable length message and produces a fixed length hash value. Hash value is otherwise called as message digest Hash values are used to check integrity of messages.

2. One way Property

   Weak Collision Resistance

   Strong Collision Resistance

   Psuedorandomness

   Efficiency

   Variable size input

   Fixed size output

3. Hash function accepts a variable length message and produces a fixed length hash value. Hash value is otherwise called as message digest Hash values are used to check integrity of messages. The following figure illustrates hash

function –The equation for hash function are h=H(M)

Where M –Variable length message

H-Hash Function

h –Hash value

4. Hash function accepts a variable length message and produces a fixed length hash value. Hash value is otherwise called as message digest Hash values are used to check integrity of messages. The following figure illustrates hash function –The equation for hash function are h=H(M)

   Where M –Variable length message
   H-Hash Function
   h –Hash value

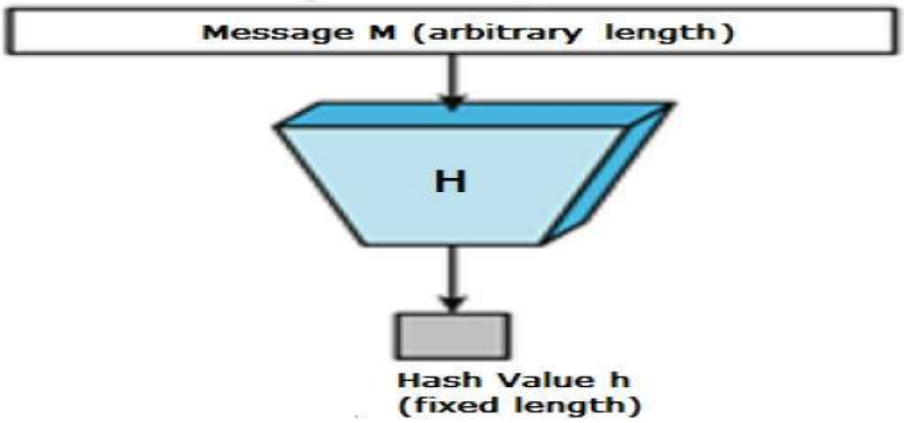


Figure: Hash Function
Note: Copyrights of this figure are reserved with original author.

5. For any given hash value h, it is computationally infeasible to find y such that H(y)=h.

24.15 Case studies: NA

24.16 Glossary

MAC - Message Authentication Code

24.17 References

1. Cryptography and Network Security Principles and Practice, by William stallings, Pearson, 5th edition.

2.Applied Cryptography: Protocols, Algorthms, and Source Code in C , by Bruce Schneier, Second Edition , John Wiley & Sons, Inc., 2015.

3.Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, by Hamid R. Nemati and Li Yang, IGI Global, 2011

4.Forouzon B, “Cryptography and Network Security,” Indian Edition, TMH (2010).

24.18 Keywords

Hash Value-Hash Function, Encryption, Digital Signatures

SESSION: 25

APPLICATIONS OF CRYPTOGRAPHIC HASH FUNCTIONS

25.1 Aim

Understand the basic concepts of Hash Functions and Applications of Hash Functions.

25.2 Instructional Objectives

The objective of this session is to introduce the basic concepts of Hash Functions. It provides the necessary theoretical background and demonstrates the applications of Hash Functions.

25.3 Learning Outcomes

At the end of this session, you should be able to:

Define Hash Functions
List applications of Hash Functions

25.4 Module Description

This module defines Hash function. Applications of Hash algorithms are also discussed in this module. Secure Hash Algorithm (SHA 512) algorithms are demonstrated. Calculating Hash value using two simple hash functions is also discussed. Similarly MD5 is also discussed. Message Authentication Code (MAC) algorithms are also discussed.

25.5 Session Introduction

This session describes the concepts of Hash functions and applications of hash functions.

25.6 Session Description

25.6.1 Applications of Hash Functions

- ***Message Authentication***

(a) Source calculates hash value of a message and appends it to the message. Message together with hash value is encrypted using secret key and any symmetric encryption algorithm and sent to the destination. Destination decrypts the message and hash value with the same secret key and computes hash value for the received message and compares with the hash value calculated by the source. If the hash value sent by the source and hash value computed by the destination for the received message are same it means that message is received at the destination without modification so that the integrity of the message is preserved.

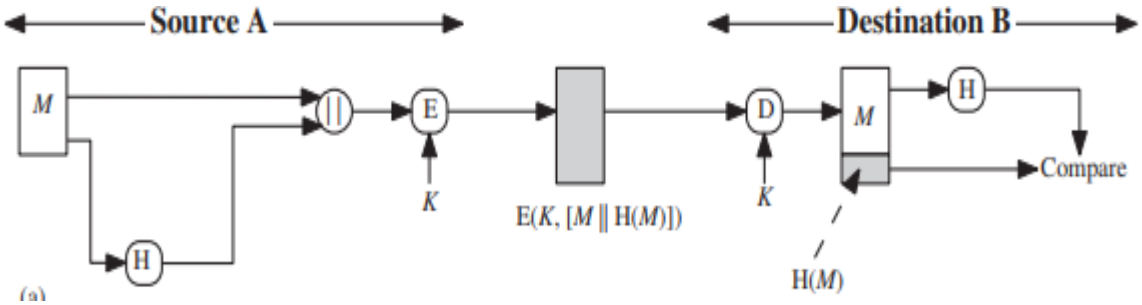


Figure 25.1 Usage of Hash Function in Message Authentication: Symmetric Encryption

Note: Copyrights of this diagram are reserved for original author

(b) Source calculates hash value of a message and appends it to the message. Only hash value is encrypted using secret key and any symmetric encryption algorithm and sent to the destination. Destination decrypts the hash value with the same secret key and computes hash value for the received message and compares with the hash value calculated by the source. If the hash value sent by the source and hash value computed by the destination for the received message are same it means that message is received at the destination without modification so that the integrity of the message is preserved.

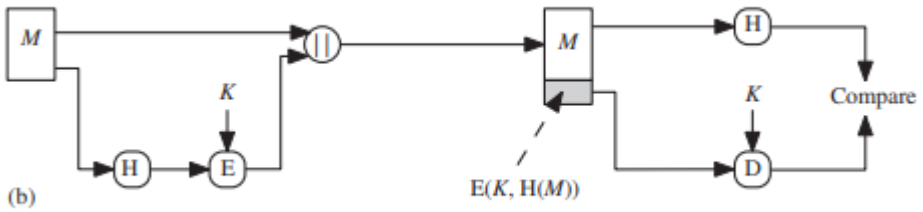


Figure 25.2 Usage of Hash Function in Message Authentication: Symmetric Encryption

Note: Copyrights of this diagram are reserved for original author

(c) Source appends a random number (s) to the message and calculates hash value of a message and appends it to the message. Message appended with hash value is received at the destination. Destination also appends the same random number used by the source to the message and computes hash value. If the hash value sent by the source and hash value computed by the destination for the received message are same it means that message is received at the destination without modification so that the integrity of the message is preserved.

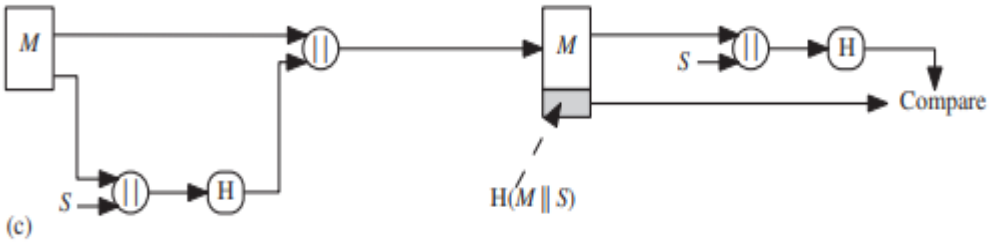


Figure 25.3 Usage of Hash Function in Message Authentication: Appending Random Number

Note: Copyrights of this diagram are reserved for original author

(d) Source appends a random number (s) to the message and calculates hash value of a message and appends it to the message. Message appended with the hash value is encrypted using secret key and any symmetric encryption algorithm. Encrypted message is received at the destination. Destination decrypts the received message using same secret key and symmetric encryption algorithm used by the source Destination also appends the same random number used by the source to the message and computes hash value of the received message. If the hash value sent by the source and hash value computed by the destination for the received message are same it means that message is received at the

destination without modification so that the integrity of the message is preserved.

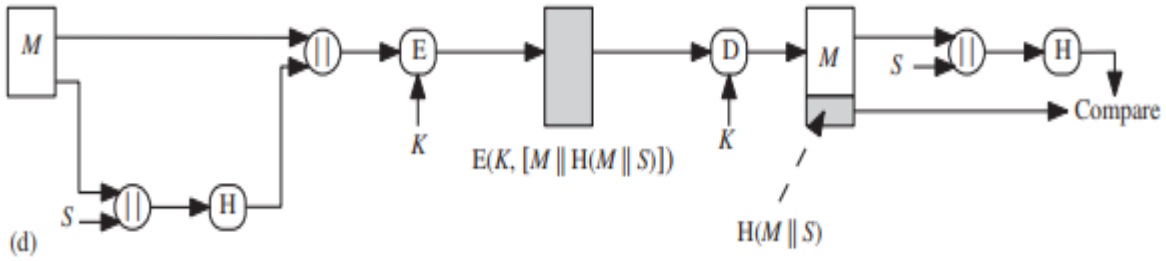


Figure 25.4 Usage of Hash Function in Message Authentication: Appending Random Number & Symmetric Encryption

Note: Copyrights of this diagram are reserved for original author

- ***Digital Signature***

Encrypting the hash vaue or MAC value of the message with Private Key of source (PR_a) and decrypting with public key (PU_a) of source is called Digital Signature.

(a) Source calculates hash value of a message and encrypts it with private key of source (PR_a) using asymmetric encryption algorithm, appends encrypted hash value to the message and sends to the destination. Destination decrypts the encrypted hash value with the public key of source (PU_a) and computes hash value for the received message and compares with the hash value calculated by the source. If the hash value sent by the source and hash value computed by the destination for the received message are same it means that message is received at the destination without modification so that the integrity of the message is preserved.

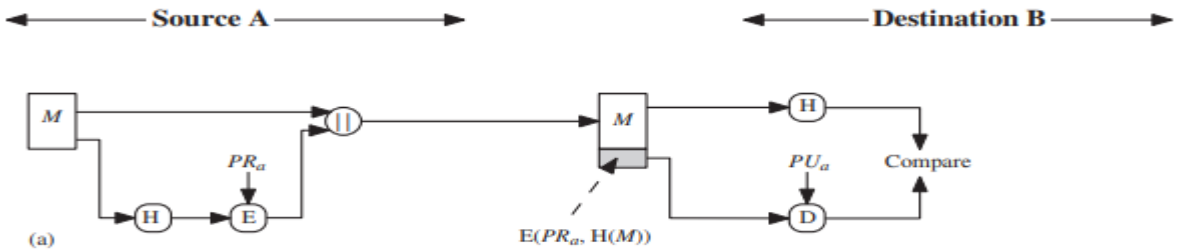


Figure 25.5 Sample 1 of Digital Signature

Note: Copyrights of this diagram are reserved for original author

(b) Source calculates hash value of a message and encrypts it with private key of source (PR_a) using asymmetric encryption algorithm, appends encrypted hash value to the

message and re-encrypts message and encrypted hash value with secret key (K) using symmetric encryption algorithm and sends to the destination. Destination decrypts the message using same secret key (K) used by the source and decrypts encrypted hash value with the public key of source (PU_a) and computes hash value for the received message and compares with the hash value calculated by the source. If the hash value sent by the source and hash value computed by the destination for the received message are same it means that message is received at the destination without modification so that the integrity of the message is preserved.

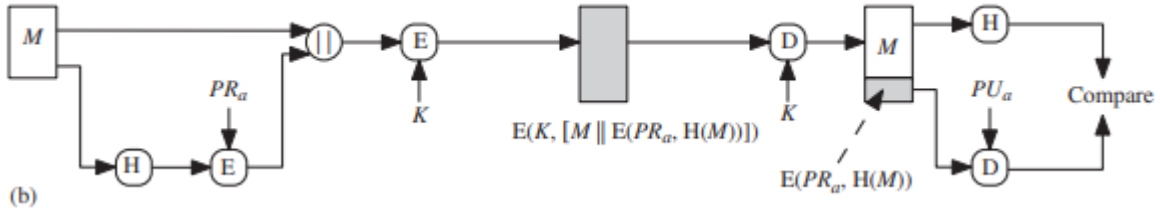


Figure 25

25.6 Sample 2 of Digital Signature

- ***Other Applications***
  - To create a one-way password file.
  - Used in intrusion detection and virus detection
  - Used to construct a pseudorandom function (PRF) or a pseudorandom number generator (PRNG

25.7 Activities: NA

25.8 Examples: NA

25.9 Table Numbering: NA

25.10 Figures with Captions

Figure 25.1 Usage of Hash Function in Message Authentication: Symmetric Encryption

Figure 25.2 Usage of Hash Function in Message Authentication: Symmetric Encryption

Figure 25.3 Usage of Hash Function in Message Authentication: Appending Random Number

Figure 25.4 Usage of Hash Function in Message Authentication: Appending Random Number & Symmetric Encryption

Figure 25.5 Sample 1 of Digital Signature

Figure 25.6 Sample 2 of Digital Signature

25.11 Self-Assessment Questions

1. Identify hash function applications among the following.

a) Data encryption b) Data compression c) Data deduplication d) All of the above

2. Identify the primary use of Hash Function in preserving integrity of data.

a) Ensuring data confidentiality

b) Detecting unauthorized access

c) Verifying data integrity

d) Encrypting data during transmission

3. When storing passwords, hash functions are frequently used to:

a) Encrypt passwords for added security

b) Store passwords in plain text format

c) Generate random passwords

d) Create hash values of passwords for verification

4. Hash functions are frequently used in blockchain technology for

a) Storing sensitive data securely

b) Achieving consensus in distributed systems

c) Performing mathematical calculations

d) Conducting financial transactions

5. Which of the following instances of digital signatures uses hash functions?

a) Verifying the authenticity of digital documents

b) Encrypting sensitive information

c) Storing private keys securely

d) Creating digital certificates

6. Hash functions are used for content addressing in distributed file systems to:

a) Encrypt files for secure storage

b) Compress files to reduce storage space

c) Identify and retrieve files based on their content

d) Authenticate users accessing the file system

7. Applications for hash functions in data deduplication include:

a) Encrypting redundant data

b) Compressing data to reduce storage space

c) Identifying and eliminating duplicate data chunks

d) Storing data in distributed storage systems

8. Hash functions are used to calculate checksums, which are frequently employed in network protocols:

a) Detect errors during data transmission

b) Encrypt sensitive information

c) Authenticate network devices

d) Prioritize network traffic

9. Hash functions are important in digital forensics because they help:

a) Decrypting encrypted data

b) Detecting file tampering and manipulation

c) Recovering lost or deleted files

d) Analyzing network traffic patterns

10. Hash functions are used for content-based routing in distributed systems to:

a) Securely authenticate messages

b) Encrypt sensitive data during transmission

c) Determine the destination of messages based on their content

d) Optimize network bandwidth

Answers:

d) All of the above

c) Verifying data integrity

d) Create hash values of passwords for verification

b) Achieving consensus in distributed systems

a) Verifying the authenticity of digital documents

c) Identify and retrieve files based on their content

c) Identifying and eliminating duplicate data chunks

a) Detect errors during data transmission

b) Detecting file tampering and manipulation

c) Determine the destination of messages based on their content

25.12 Summary

It should be emphasized that cryptographic hash functions undergo continuous scrutiny and evaluation to identify any potential vulnerabilities. Ongoing research and development efforts focus on creating newer hash functions that incorporate advanced security features. The objective is to meet the ever-changing demands of cryptography and ensure robust data protection.

25.13. Terminal Questions

1. List the applications of Hash function

2. Define Digital signature

3. Demonstrate Message Authentication with neat diagrams

4. Illustrate Digital signature with neat diagrams

5. List other applications of Hash functions.

25.14 Answer Key

1. Message authentication

Digital signatures

To create a one-way password file.

Used in intrusion detection and virus detection

Used to construct a pseudorandom function (PRF) or a pseudorandom number generator (PRNG0.

2. Encrypting the hash vaue or MAC value of the message with Private Key of source (PR_a) and decrypting with public key (PU_a) of source is called Digital Signature.

3. (a) Source calculates hash value of a message and appends it to the message. Message together with hash value is encrypted using secret key and any symmetric encryption algorithm and sent to the destination. Destination decrypts the message and hash value with the same secret key and computes hash value for the received message and compares with the hash value calculated by the source. If the hash value sent by the source and hash value computed by the destination for the received message are same it means that message is received at the destination without modification so that the integrity of the message is preserved.

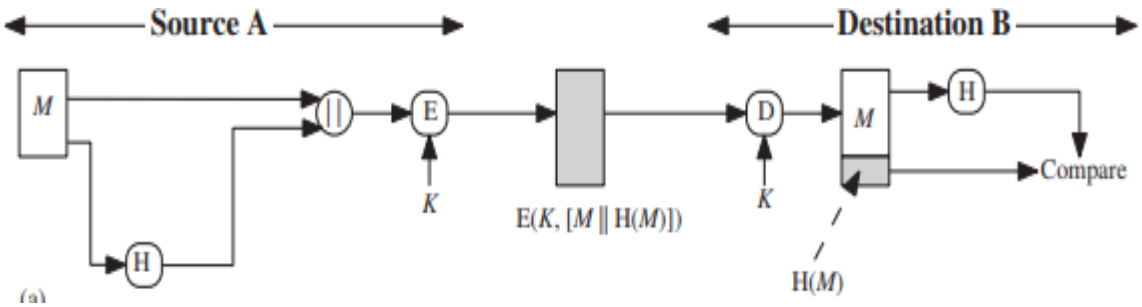


Figure Usage of Hash Function in Message Authentication: Symmetric Encryption

Note: Copyrights of this diagram are reserved for original author

(b) Source calculates hash value of a message and appends it to the message. Only hash value is encrypted using secret key and any symmetric encryption algorithm and sent to the destination. Destination decrypts the hash value with the same secret key and computes hash value for the received message and compares with the hash value calculated by the source. If the hash value sent by the source and hash value computed by the destination for the received message are same it means that message is received at the destination without modification so that the integrity of the message is preserved.

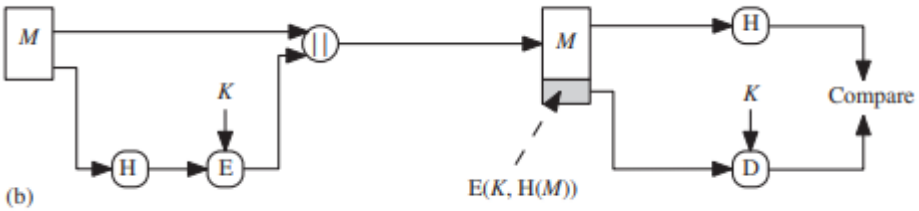


Figure Usage of Hash Function in Message Authentication: Symmetric Encryption

Note: Copyrights of this diagram are reserved for original author

(c) Source appends a random number (s) to the message and calculates hash value of a message and appends it to the message. Message appended with hash value is received at the destination. Destination also appends the same random number used by the source to the message and computes hash value. If the hash value sent by the source and hash value computed by the destination for the received message are same it means that message is received at the destination without modification so that the integrity of the message is preserved.

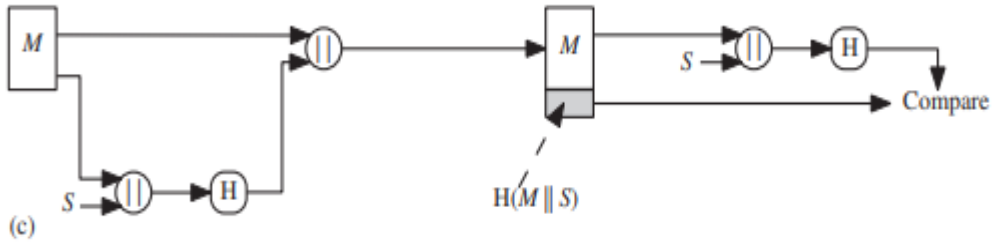


Figure Usage of Hash Function in Message Authentication: Appending Random Number

Note: Copyrights of this diagram are reserved for original author

(c) Source appends a random number (s) to the message and calculates hash value of a message and appends it to the message. Message appended with the hash value is encrypted using secret key and any symmetric encryption algorithm. Encrypted message is received at the destination. Destination decrypts the received message using same secret key and symmetric encryption algorithm used by the source Destination also appends the same random number used by the source to the message and computes hash value of the received message. If the hash value sent by the source and hash value computed by the destination for the received message are same it means that message is received at the destination without modification so that the integrity of the message is preserved.

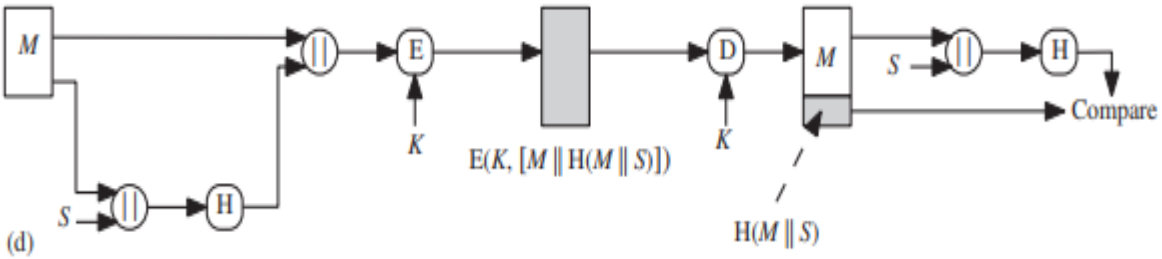


Figure Usage of Hash Function in Message Authentication: Appending Random Number & Symmetric Encryption

Note: Copyrights of this diagram are reserved for original author

4. Digital Signature

Encrypting the hash vaue or MAC value of the message with Private Key of source (PR_a) and decrypting with public key (PU_a) of source is called Digital Signature.

(a) Source calculates hash value of a message and encrypts it with private key of source (PR_a) using asymmetric encryption algorithm, appends encrypted hash value to the message and sends to the destination. Destination decrypts the encrypted hash value with the public key of source (PU_a) and computes hash value for the received message and compares with the hash value calculated by the source. If the hash value sent by the source and hash value computed by the destination for the received message are same it means that message is received at the destination without modification so that the integrity of the message is preserved.

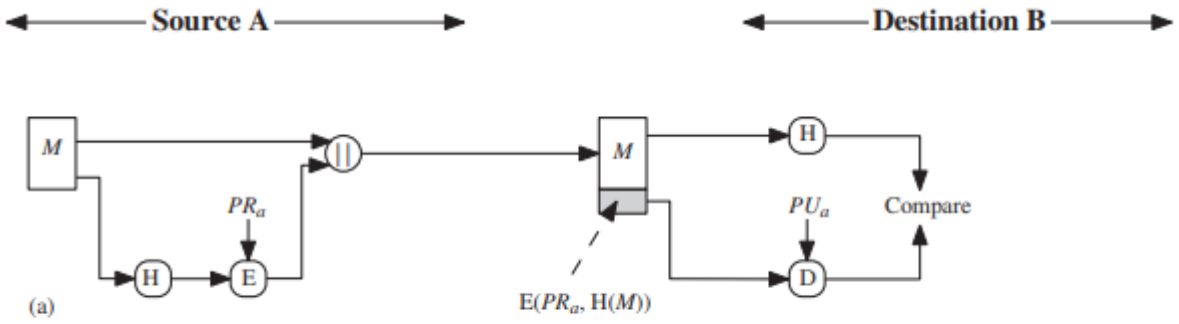


Figure Sample 1 of Digital Signature

Note: Copyrights of this diagram are reserved for original author

(b) Source calculates hash value of a message and encrypts it with private key of source (PR_a) using asymmetric encryption algorithm, appends encrypted hash value to the message and re-encrypts message and encrypted hash value with secret key (K) using symmetric encryption algorithm and sends to the destination. Destination decrypts the message using same secret key (K) used by the source and decrypts encrypted hash value with the public key of source (PU_a) and computes hash value for the received message and compares with the hash value calculated by the source. If the hash value sent by the source and hash value computed by the destination for the received message are same it means that message is received at the destination without modification so that the integrity of the message is preserved.

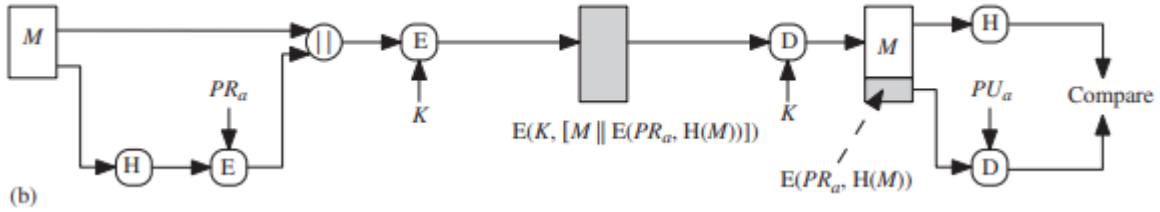


Figure Sample 2 of Digital Signature

5. Other Applications

- To create a one-way password file.
- Used in intrusion detection and virus detection
- Used to construct a pseudorandom function (PRF) or a pseudorandom number generator (PRNG).

25.15 Case studies: NA

25.16 Glossary

PRF- Pseudorandom Function

PRNG - Pseudorandom number generator.

25.17 References

1. Cryptography and Network Security Principles and Practice, by William stallings, Pearson, 5th edition.

2.Applied Cryptography: Protocols, Algorthms, and Source Code in C , by Bruce Schneier, Second Edition , John Wiley & Sons, Inc., 2015.

3.Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, by Hamid R. Nemati and Li Yang, IGI Global, 2011

4.Forouzon B, “Cryptography and Network Security,” Indian Edition, TMH (2010).

25.18 Keywords

Hash Value-Hash Function, Encryption, Digital Signatures

SESSION: 26

TWO SIMPLE HASH FUNCTIONS

26.1 Aim

Understand the basic concepts of Hash Functions and simple Hash Functions.

26.2 Instructional Objectives

The objective of this session is to introduce the basic concepts of Hash Functions. It provides the necessary theoretical background and demonstrates simple Hash Functions.

26.3 Learning Outcomes

At the end of this session, you should be able to:

Apply simple Hash Functions

26.4 Module Description

This module defines Hash function. Applications of Hash algorithms are also discussed in this module. Secure Hash Algorithm (SHA 512) algorithms are demonstrated. Calculating Hash value using two simple hash functions is also discussed. Similarly MD5 is also discussed. Message Authentication Code (MAC) algorithms are also discussed.

26.5 Session Introduction

This session describes the concepts of Hash functions and applications of hash functions.

26.6 Session Description

26.6.1 Hash Function 1 (Bit-by-Bit XOR Operation)

The input is seen as a series of n-bit blocks, including messages, files, etc. An n-bit hash function is created by iteratively processing each block of the input. The bit-by-bit exclusive-OR (XOR) of each block is one of the most basic hash functions. This can be said to be

$C_i = b_{il}$ XOR b_{i2} XOR…….b_{im}

$C_i = i^{th}$ bit of hash code

m= no. of n-bit blocks in the input

$i^{th} = i^{th}$ bit in the j^{th} block

26.6.2 Hash Function 2

The simplest method to make things better is to rotate or shift the hash value by one bit after each block is processed. The following is a summary of the process.

1. Start off by setting the n-bit hash value to 0.

2. Execute the subsequent instructions on each n-bit block of data:

a. Rotate the current hash value one bit to the left.

b. XOR the block with the hash number.

26.6.3 Hash Function Based on Cipher Block Chaining (CBC) Mode

Divide a message into fixed-size blocks M_1,M_2,……..M_N and use a symmetric encryption system such as DES to compute the hash code as

H_0= Initial Value

H_i= E(M_i, H_i-1)

G=H_N

26.7 Activities: NA

26.8 Examples:

1. Consider the message 10111011000011111010111. Divide the message into 3 blocks and compute the hash value uing bit-by-bit XOR Operation.

2. Consider the message 10111011000011111010111. Divide the message into 3 blocks and compute the hash value using the following equations

H_0= Initial Value

$H_i = E(M_i, H_i\text{-}1)$

$G=H_N$

26.9 Table Numbering: NA

26.10 Figures with Captions

Figure 26.1 Usage of Hash Function in Message Authentication: Symmetric Encryption

Figure 26.2 Usage of Hash Function in Message Authentication: Symmetric Encryption

Figure 26.3 Usage of Hash Function in Message Authentication: Appending Random Number

Figure 26.4 Usage of Hash Function in Message Authentication: Appending Random Number & Symmetric Encryption

Figure 26.5 Sample 1 of Digital Signature

Figure 26.6 Sample 2 of Digital Signature

26.11 Self-Assessment Questions

1. Which of the following statements best sums up a basic hash function?

a) A hash function with a fixed output size

b) A hash function that uses basic arithmetic operations

c) A hash function designed for basic data integrity checks

d) A hash function without collision resistance

2. What is the main function of a simple hash function?

a) Generating unique hash values for data

b) Encrypting sensitive information

c) Compressing data to reduce storage space

d) Performing complex mathematical calculations

3. Which of the following claims regarding the output size of a simple hash function is true?

a) It is smaller than the input size

b) It is larger than the input size

c) It is the same as the input size

d) It can vary based on the input size

4. Which characteristic of cryptographic hash functions does the simple hash function lack?

a) Deterministic output b) Preimage resistance c) Collision resistance d) Avalanche effect

5. Which one of the following is a simple hash function example?

a) MD5 b) SHA-1 c) CRC32 d) HMAC

6. Which of the following uses simple hash functions frequently?

a) Data encryption for secure communication

b) Secure password storage

c) Digital signatures for authentication

d) Basic data integrity checks

7. What could go wrong if you use a straightforward hash function without collision resistance?

a) Increased computational complexity

b) Increased risk of data corruption

c) Weaker security against malicious attacks d

d) Slower data processing speed

8. Which of the subsequent processes is frequently used in basic hash functions?

a) Bitwise XOR b) Modular arithmetic c) Bit shifting d) All of the above

9. The hash value is frequently used as a/an in stimple hash functions:

a) Encryption key

b) Data compression algorithm

c) Identifier or index for data storage

d) Authentication token

10. A simple hash function's design is more concerned with:

a) Computational efficiency

b) Cryptographic security

c) Data compression ratio

d) Input flexibility and versatility

Answers:

b) A hash function that uses basic arithmetic operations

a) Generating unique hash values for data

a) It is smaller than the input size

c) Collision resistance

c) CRC32

d) Basic data integrity checks

c) Weaker security against malicious attacks

d) All of the above

c) Identifier or index for data storage

a) Computational efficiency

26.12 Summary

Basic algorithms known as simple hash functions create a fixed-size hash value or digest from an input. They are frequently used for indexing and simple data integrity checks. These hash functions frequently make use of modular arithmetic, bitwise operations, and fundamental arithmetic operations. They lack the sophisticated security characteristics seen in cryptographic hash functions, such as preimage and collision resistance. Simple hash functions typically provide outputs that are smaller than their inputs.

26.13. Terminal Questions

1. Summarize bit-by-bit XOR operation of hash function.

2. Enumerate Simple Hash functions

3. Consider the message 01000101111100001011011. Divide the message into 3 blocks and compute the hash value uing bit-by-bit XOR Operation.

4. Consider the message 01000101111100001011011. Divide the message into 3 blocks and compute the hash value using the following equations

H_0= Initial Value

$H_i = E(M_i, H_i\text{-}1)$

$G=H_N$

5. Summarize hash function using CBC Mode of operation.

26.14 Answer Key:

1.

The input is seen as a series of n-bit blocks, including messages, files, etc. An n-bit hash function is created by iteratively processing each block of the input. The bit-by-bit exclusive-OR (XOR) of each block is one of the most basic hash functions. This can be said to be

$C_i = b_{il}$ XOR b_{i2} XOR…….b_{im}

$C_i = i^{th}$ bit of hash code

m= no. of n-bit blocks in the input

$i^{th} = i^{th}$ bit in the j^{th} block

2.

a. The input is seen as a series of n-bit blocks, including messages, files, etc. An n-bit hash function is created by iteratively processing each block of the input. The bit-by-bit exclusive-OR (XOR) of each block is one of the most basic hash functions. This can be said to be

$C_i = b_{il}$ XOR b_{i2} XOR…….b_{im}

$C_i = i^{th}$ bit of hash code

m= no. of n-bit blocks in the input

$i^{th} = i^{th}$ bit in the j^{th} block

b. The simplest method to make things better is to rotate or shift the hash value by one bit after each block is processed. The following is a summary of the process.

1. Start off by setting the n-bit hash value to 0.

2. Execute the subsequent instructions on each n-bit block of data:

a. Rotate the current hash value one bit to the left.

b. XOR the block with the hash number.

c. Divide a message into fixed-size blocks M_1,M_2,……..M_N and use a symmetric encryption system such as DES to compute the hash code as

H_0= Initial Value

H_i= E(M_i, H_i-1)

G=H_N

3.

Message: 010001011111000010110011

Block 1: 01000101 Block 2: 11110000 Block 3: 10110011

To compute the hash value using bit-by-bit XOR operation, we perform XOR operation between corresponding bits of each block.

Step 1: Block 1 XOR Block 2: 01000101 XOR 11110000

10110101

Step 2: (Previous result) XOR Block 3: 10110101 XOR 10110011

00000110

The final hash value computed using bit-by-bit XOR operation for the given message is 00000110.

4.

Given message: 010001011111000010110011

Block 1: 01000101 Block 2: 11110000 Block 3: 10110011

Let's assume the initial value, H0, is 00000000.

Using the XOR operation for E(Mi, Hi-1):

H1 = E(Block 1, H0) = Block 1 XOR H0 = 01000101 XOR 00000000 = 01000101 = 0x45

H2 = E(Block 2, H1) = Block 2 XOR H1 = 11110000 XOR 01000101 = 10110101 = 0xB5

H3 = E(Block 3, H2) = Block 3 XOR H2 = 10110011 XOR 10110101 = 00000110 = 0x06

Finally, G = H3 = 0x06

The hash value computed using the provided equations for the given message is 0x06 (hexadecimal) or 00000110 (binary).

5.

Divide a message into fixed-size blocks M_1,M_2,……..M_N and use a symmetric encryption system such as DES to compute the hash code as

H_0= Initial Value

H_i= E(M_i, H_i-1)

G=H_N

26.15 Case studies: NA

26.16 Glossary: NA

26.17 References

1. Cryptography and Network Security Principles and Practice, by William stallings, Pearson, 5th edition.

2.Applied Cryptography: Protocols, Algorthms, and Source Code in C , by Bruce Schneier, Second Edition , John Wiley & Sons, Inc., 2015.

3.Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, by Hamid R. Nemati and Li Yang, IGI Global, 2011

4.Forouzon B, “Cryptography and Network Security,” Indian Edition, TMH (2010).

26.18 Keywords

Simple Hash Function, bit-by-bit XOR,CBC

CRYPTANALYSIS & CYBER DEFENSE

21CS3041RA

Course Description: This course provides an introduction to the core principles of cryptography and its relevance in the field of network security. Students will gain a comprehensive understanding of cryptographic methods used to ensure secure communication in potentially insecure environments. Topics covered include techniques for verifying message source authenticity, ensuring message integrity during transmission across unsecured channels, and establishing unique message origin identification. The course also addresses cryptanalysis attacks on cryptographic techniques, as well as various attack models.

SESSION: 27

Cryptanalysis of Hash Functions

27.1 Aim

Understand the basic concepts of Hash Functions and simple Hash Functions.

27.2 Instructional Objectives

The objective of this session is to introduce the basic concepts of Hash Functions. It provides the necessary theoretical background and demonstrates attacks on hash functions.

27.3 Learning Outcomes

At the end of this session, you should be able to:

6. Summarize cryptanalysis of hash functions

27.4 Module Description

This module defines Hash function. Applications of Hash algorithms are also discussed in this module. Secure Hash Algorithm (SHA 512) algorithms are demonstrated. Calculating Hash value using two simple hash functions is also discussed. Similarly MD5 is also discussed. Message Authentication Code (MAC) algorithms are also discussed.

27.5 Session Introduction

This session describes the concepts of cryptanalysis of hash functions

27.6 Session Description

27.6.1 Brute Force Attack

A brute-force attack on a hash function is not contingent upon the particular algorithm employed but rather on the length of the hash value in bits. In such an attack, the assailant systematically attempts all feasible input values in order to discover a corresponding hash value. The complexity of a brute-force attack grows exponentially with the bit length of the hash value. Consequently, hash functions featuring longer hash values are generally deemed more impervious to brute-force attacks.

27.6.2 Birthday Paradox

1. The birthday paradox draws attention to the likelihood that two or more people in a group will have the same birthday.
2. The paradox results from the fact that birthdays do not occur at random times throughout the year but rather tend to concentrate around particular dates.
3. The paradox calls into question the belief that a sizable group is necessary to have a high likelihood of sharing birthdays. In actuality, as the group size expands, the probability rises sharply.
4. The precise likelihood varies depending on the number of participants, although surprisingly little number of persons can achieve a 50% or higher chance.
5. The birthday paradox is useful in the world of cryptography since it highlights the flaw in using only birthdays as random numbers.

27.6.3 Birthday Attack

A cryptographic attack known as a "birthday attack" uses the birthday paradox to find collisions in hash functions or weaken particular encryption techniques. The phrase "birthday attack" comes from the birthday paradox, which shows that in a reasonably small group, it is more likely than not that two people will share the same birthday.

A collision, also known as two distinct inputs that produce the same hash value, is what a birthday attack aims to find. The birthday paradox increases the likelihood of collisions, which an attacker might exploit by producing multiple random inputs and comparing the resulting hash values.

A birthday attack's potency is based on the size of the hash value or the quantity of possible inputs. The likelihood of a collision increasing along with the amount of potential inputs. Therefore, using hash algorithms with longer hash values or increasing the input space aids in reducing the probability of successful birthday attacks.

Birthday attacks significantly affect the safety of cryptographic systems. They stress the value of using hash algorithms with sufficient bit lengths to reduce collision hazards. Additionally, they emphasize how carefully thought-out design and in-depth research of encryption systems are required to ensure resilience against birthday attacks.

27.6.4 Meet-in-the-Middle Attack

An attack known as a "meet-in-the-middle" makes use of the trade-off between time and space complexity in specific encryption algorithms or schemes. By locating a collision or more quickly recovering the encryption key than with an exhaustive search, it seeks to decrypt the data.

A meet-in-the-middle attack takes use of the fact that the same key can be used to encrypt and decrypt data. Using a forward encryption phase and a backward decryption phase, the attack splits the encryption process into two pieces. A subset of possible keys are precomputed for encryption and decryption by the attacker, and the intermediate results are stored in memory.

The attacker then conducts a thorough search on the remaining key candidates while encrypting the plaintext and contrasting the intermediate outcomes of the precomputation. A match suggests a potential key that might be used to decrypt the ciphertext if it is discovered.

When the encryption method or scheme makes it simple to separate the encryption and decryption processes, as well as when the number of potential keys is sufficient for the attacker to efficiently do precomputations and exhaustive searches, the meet-in-the-middle attack is effective.

Cryptographic systems can include countermeasures such using bigger key sizes, more secure encryption algorithms, or adding more rounds of encryption to defend against meet-in-the-middle attacks.

27.7 Activities: NA

27.8 Examples: NA

27.9 Table Numbering: NA

27.10 Figures with Captions: NA

27.11 Self-Assessment Questions

1. What is a hash function brute force attack?

a) A method to crack passwords by trying all possible combinations.

b) An attack where the attacker tries to find two different inputs that produce the same hash output.

c) A technique to exploit weak key generation in symmetric encryption.

d) A method to intercept communication between two parties.

2. The Birthday Paradox states that in a group of 23 people, there is approximately a 50% chance that:

a) Two people share the same birthday.

b) Two people share the same birth year.
c) Two people have birthdays on consecutive days.
d) No two people share the same birthday.

3. What is a Birthday Attack in cryptography?
a) A type of attack on a person's identity based on their birth date.
b) An attack where the attacker impersonates someone else in a cryptographic system.
c) An attack that exploits the probability of finding two different inputs with the same hash output.
d) A method to bypass authentication using someone's birthday as the password.

4. The Birthday Paradox is relevant to cryptography because it helps to understand:
a) How to generate secure passwords.
b) How to predict someone's birth date based on their name.
c) The likelihood of finding collisions in hash functions.
d) The probability of two people sharing the same cryptographic key.

5. What is a collision in the context of hash functions?
a) A situation where the hash function output is longer than the input.
b) A scenario where two different inputs produce the same hash output.
c) An attack where an unauthorized person gains access to a system.
d) A method to generate secure cryptographic keys.

6. Which cryptographic attack exploits the birthday paradox to find collisions in a hash function?
a) Birthday Attack.
b) Meet-in-the-Middle Attack.
c) Brute Force Attack.
d) Differential Cryptanalysis.

7. The birthday attack complexity for finding a collision in an ideal hash function with a hash size of n bits is approximately:
a) O(2^n)
b) O(2^(n/2))

c) O(n^2)

d) O(n)

8. In a Meet-in-the-Middle Attack, the attacker:

a) Intercepts communication between two parties.

b) Tries all possible combinations of characters to crack a password.

c) Exploits the process of encrypting and decrypting data simultaneously.

d) Uses precomputed tables to speed up a cryptographic attack.

9. Which of the following statements is true about the Meet-in-the-Middle Attack?

a) It is applicable only to asymmetric encryption schemes.

b) It works by searching for a collision in the hash function.

c) It is a generic attack that can be used against any cryptographic system.

d) It relies on the attacker being in the middle of a communication channel.

10. The Meet-in-the-Middle Attack is commonly associated with which encryption technique?

a) RSA (Rivest-Shamir-Adleman)

b) AES (Advanced Encryption Standard)

c) DES (Data Encryption Standard)

d) ECC (Elliptic Curve Cryptography)

11. How does the Meet-in-the-Middle Attack work?

a) It uses a large number of computers to simultaneously try all possible keys.

b) It attempts to find a collision in the hash function by searching for two identical outputs.

c) It divides the cryptographic algorithm into two parts and precomputes possible combinations for each part.

d) It exploits the weak key generation process in the encryption algorithm.

12. Which attack can be mitigated by using a salt in password hashing?

a) Brute Force Attack.

b) Birthday Attack.

c) Meet-in-the-Middle Attack.

d) Differential Cryptanalysis.

13. The Birthday Paradox is based on the principle of:
a) Probability theory.
b) Cryptographic keys.
c) Hash collisions.
d) Prime number generation.

14. What is the purpose of using a salt in password hashing?
a) To add flavor to the password for better memorization.
b) To protect against brute force attacks.
c) To prevent birthday attacks.
d) To increase the length of the password.

15. In the context of cryptographic attacks, what does "narrowing the search space" mean?
a) Reducing the size of the encrypted data.
b) Limiting the number of possible solutions an attacker needs to try.
c) Making the encryption algorithm more complex.
d) Restricting access to the cryptographic keys.

16. Which of the following attacks is NOT related to hash functions?
a) Brute Force Attack.
b) Meet-in-the-Middle Attack.
c) Side-Channel Attack.
d) Birthday Attack.

17. The probability of a collision occurring in a hash function increases as the number of possible hash outputs:
a) Increases.
b) Decreases.
c) Remains constant.
d) None of the above.

18. A hash function that produces a fixed-size output, regardless of the input size, is considered:
a) Ideal for password hashing.
b) Vulnerable to birthday attacks.
c) Secure against all types of attacks.
d) Prone to collisions.

19. Which cryptographic attack exploits a weakness in a double encryption process?
a) Birthday Attack.
b) Differential Cryptanalysis.
c) Meet-in-the-Middle Attack.
d) Brute Force Attack.

20. The security of a hash function is based on its ability to resist which of the following attacks?
a) Brute Force Attack.
b) Birthday Attack.
c) Meet-in-the-Middle Attack.
d) All of the above.

27.12 Summary

Overall, the birthday paradox serves as a fascinating example of how intuition can sometimes lead us astray in probabilistic reasoning and highlights the importance of understanding probability concepts and their applications. In order to decrypt data, a meet-in-the-middle attack takes advantage of the trade-off between time and space complexity. The attacker attempts to more effectively locate a collision or recover the encryption key by precalculating intermediate results and running a thorough search. Increased key sizes and the use of stronger encryption methods can reduce the danger of meet-in-the-middle attacks.

27.13. Terminal Questions

1. Summarize birthday paradox.

2. Enumerate birthday attack

3. Analyze attacks possible on hash functions

4. List attacks possible on hash functions

5. Define brute force attack

27.14 Answer Key:

Self- Assessment -Question – Answers

Answers:

1. a A method to crack passwords by trying all possible combinations.

2. a Two people share the same birthday.

3. c An attack that exploits the probability of finding two different inputs with the same hash output.
4. c The likelihood of finding collisions in hash functions.

5. b A scenario where two different inputs produce the same hash output.

6. a Birthday Attack.

7. b O(2^(n/2))

8. d Uses precomputed tables to speed up a cryptographic attack.

9. c It is a generic attack that can be used against any cryptographic system.

10. c DES (Data Encryption Standard)

11. c It divides the cryptographic algorithm into two parts and precomputes possible combinations for each part.

12. a Brute Force Attack.

13. a Probability theory.

14. b To protect against brute force attacks.

15. b Limiting the number of possible solutions an attacker needs to try.

16. c Side-Channel Attack.

17. a Increases.

18. d Prone to collisions.

19. c Meet-in-the-Middle Attack.

20. d All of the above.

1.

1. The birthday paradox draws attention to the likelihood that two or more people in a group will have the same birthday.
2. The paradox results from the fact that birthdays do not occur at random times throughout the year but rather tend to concentrate around particular dates.
3. The paradox calls into question the belief that a sizable group is necessary to have a high likelihood of sharing birthdays. In actuality, as the group size expands, the probability rises sharply.
4. The precise likelihood varies depending on the number of participants, although surprisingly little number of persons can achieve a 50% or higher chance.
5. The birthday paradox is useful in the world of cryptography since it highlights the flaw in using only birthdays as random numbers.

2.

A cryptographic attack known as a "birthday attack" uses the birthday paradox to find collisions in hash functions or weaken particular encryption techniques. The phrase "birthday attack" comes from the birthday paradox, which shows that in a reasonably small group, it is more likely than not that two people will share the same birthday.

A collision, also known as two distinct inputs that produce the same hash value, is what a birthday attack aims to find. The birthday paradox increases the likelihood of collisions, which an attacker might exploit by producing multiple random inputs and comparing the resulting hash values.

A birthday attack's potency is based on the size of the hash value or the quantity of possible inputs. The likelihood of a collision increasing along with the amount of potential inputs. Therefore, using hash algorithms with longer hash values or increasing the input space aids in reducing the probability of successful birthday attacks.

Birthday attacks significantly affect the safety of cryptographic systems. They stress the value of using hash algorithms with sufficient bit lengths to reduce collision hazards. Additionally, they emphasize how carefully thought-out design and in-depth research of encryption systems are required to ensure resilience against birthday attacks.

3.

- ***Brute Force Attack***

A brute-force attack on a hash function is not contingent upon the particular algorithm employed but rather on the length of the hash value in bits. In such an attack, the assailant

systematically attempts all feasible input values in order to discover a corresponding hash value. The complexity of a brute-force attack grows exponentially with the bit length of the hash value. Consequently, hash functions featuring longer hash values are generally deemed more impervious to brute-force attacks.

- ***Birthday Paradox***

  1. The birthday paradox draws attention to the likelihood that two or more people in a group will have the same birthday.

  2. The paradox results from the fact that birthdays do not occur at random times throughout the year but rather tend to concentrate around particular dates.

  3. The paradox calls into question the belief that a sizable group is necessary to have a high likelihood of sharing birthdays. In actuality, as the group size expands, the probability rises sharply.

  4. The precise likelihood varies depending on the number of participants, although surprisingly little number of persons can achieve a 50% or higher chance.

  5. The birthday paradox is useful in the world of cryptography since it highlights the flaw in using only birthdays as random numbers.

- ***Birthday Attack***

  A cryptographic attack known as a "birthday attack" uses the birthday paradox to find collisions in hash functions or weaken particular encryption techniques. The phrase "birthday attack" comes from the birthday paradox, which shows that in a reasonably small group, it is more likely than not that two people will share the same birthday.

  A collision, also known as two distinct inputs that produce the same hash value, is what a birthday attack aims to find. The birthday paradox increases the likelihood of collisions, which an attacker might exploit by producing multiple random inputs and comparing the resulting hash values.

  A birthday attack's potency is based on the size of the hash value or the quantity of possible inputs. The likelihood of a collision increasing along with the amount of potential inputs. Therefore, using hash algorithms with longer hash values or increasing the input space aids in reducing the probability of successful birthday attacks.

  Birthday attacks significantly affect the safety of cryptographic systems. They stress the value of using hash algorithms with sufficient bit lengths to reduce collision hazards. Additionally, they emphasize how carefully thought-out design and in-depth research of encryption

systems are required to ensure resilience against birthday attacks.

- ***Meet-in-the-Middle Attack***

  An attack known as a "meet-in-the-middle" makes use of the trade-off between time and space complexity in specific encryption algorithms or schemes. By locating a collision or more quickly recovering the encryption key than with an exhaustive search, it seeks to decrypt the data.

  A meet-in-the-middle attack takes use of the fact that the same key can be used to encrypt and decrypt data. Using a forward encryption phase and a backward decryption phase, the attack splits the encryption process into two pieces. A subset of possible keys are precomputed for encryption and decryption by the attacker, and the intermediate results are stored in memory.

  The attacker then conducts a thorough search on the remaining key candidates while encrypting the plaintext and contrasting the intermediate outcomes of the precomputation. A match suggests a potential key that might be used to decrypt the ciphertext if it is discovered. When the encryption method or scheme makes it simple to separate the encryption and decryption processes, as well as when the number of potential keys is sufficient for the attacker to efficiently do precomputations and exhaustive searches, the meet-in-the-middle attack is effective.

  Cryptographic systems can include countermeasures such using bigger key sizes, more secure encryption algorithms, or adding more rounds of encryption to defend against meet-in-the-middle attacks.

4.

Brute force attack

Birthday attack

Meet-in-the-middle attack

5.

A brute-force attack on a hash function is not contingent upon the particular algorithm employed but rather on the length of the hash value in bits. In such an attack, the assailant systematically attempts all feasible input values in order to discover a corresponding hash value. The complexity of a brute-force attack grows exponentially with the bit length of the hash value. Consequently, hash functions featuring longer hash values are generally deemed more impervious to brute-force attacks.

27.15 Case studies: NA

27.16 Glossary: NA

27.17 References

1. Cryptography and Network Security Principles and Practice, by William stallings, Pearson, 5th edition.

2.Applied Cryptography: Protocols, Algorthms, and Source Code in C , by Bruce Schneier, Second Edition , John Wiley & Sons, Inc., 2015.

3.Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, by Hamid R. Nemati and Li Yang, IGI Global, 2011

4. Forouzon B, “Cryptography and Network Security,” Indian Edition, TMH (2010).

27.18 Keywords

Simple Hash Function, bit-by-bit XOR,CBC

CRYPTANALYSIS & CYBER DEFENSE

21CS3041RA

Course Description: This course provides an introduction to the core principles of cryptography and its relevance in the field of network security. Students will gain a comprehensive understanding of cryptographic methods used to ensure secure communication in potentially insecure environments. Topics covered include techniques for verifying message source authenticity, ensuring message integrity during transmission across unsecured channels, and establishing unique message origin identification. The course also addresses cryptanalysis attacks on cryptographic techniques, as well as various attack models.

SESSION: 28

Secure Hash Algorithm (SHA-512)

28.1 Aim

Demonstrate hash algorithm like Secure Hash Algorithm (SHA-512).

28.2 Instructional Objectives

The objective of this session is to introduce the basic concepts of Hash Functions. It provides the necessary theoretical background and demonstrates attacks on hash functions.

28.3 Learning Outcomes

At the end of this session, you should be able to:

7. Demonstrate SHA-512 hash algorithm.

28.4 Module Description

This module defines Hash function. Applications of Hash algorithms are also discussed in this module. Secure Hash Algorithm (SHA 512) algorithms are demonstrated. Calculating Hash value using two simple hash functions is also discussed. Similarly MD5 is also discussed. Message Authentication Code (MAC) algorithms are also discussed.

28.5 Session Introduction

This session starts with the introduction of SHA-512. It illustrates block diagram of SHA-512 and the operations being carried in a single round of SHA-512 in detail.

28.6 Session Description

28.6.1 Secure Hash Algorithm (SHA-512)

The algorithm outputs a 512-bit message digest from an input message with a maximum length of less than 2^{128} bits. 1024-bit blocks of the input are processed at once.

a. ***Append Padding Bits:*** The message is padded to make it exactly 896 modulo 1024 in length. Even if the message is of the desired length, padding is always applied. The range of padding bits is therefore from 1 to 1024. A single 1 bit precedes the necessary amount of 0 bits in the padding.

b. ***Append Length:*** The message has a block of 128 bits added to it.The most significant byte is placed first in this block, which is interpreted as an unsigned 128-bit integer and contains the length of the original message (before padding).

   The result of the first two stages is a message with a length that is an integer multiple of 1024 bits.

c. **Initialize hash buffer**. The hash function's intermediate and final results are stored in a 512-bit buffer.Eight 64-bit registers (designated as a, b, c, d, e, f, g, and h) can be used to represent the buffer. The following 64-bit numbers (represented in hexadecimal values) are used as the registers' initial values:. Big-endian format, which places the most important byte of a word at the low-address (leftmost) byte position, is how these values are stored.

d. **Process message in 1024-bit (128-word) blocks:** The heart of the algorithm is a module that consists of 80 rounds.

e. **Output.** After all 1024-bit blocks have been processed, the output from the th stage is the 512-bit message digest.

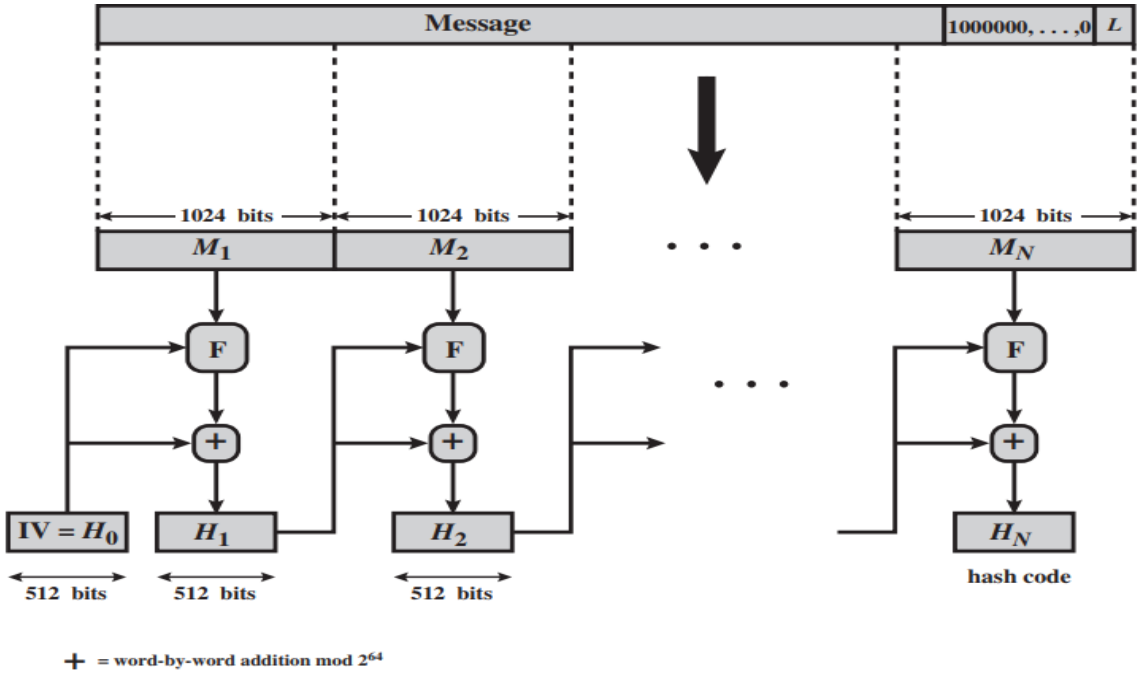


Figure 28.1 SHA-512 Block Diagram

Note: Copyrights of this diagram are reserved for original author

Each round updates the contents of the buffer using the 512-bit buffer value abcdefgh as input. The intermediate hash value H_{i-1} is present in the buffer at the start of the first round. Each round t uses a 64-bit value W_t that is taken from the 1024-bit block that is currently being processed. These values are obtained using the message scheduling that is detailed below. Additionally, an additive constant K_t is utilized for each of the 80 rounds. The first 64 bits of the cube roots of the first 80 prime numbers are represented by these words. A "randomized" set of 64-bit patterns are provided by the constants, which should get rid of any regularities in the input data. The result is created by adding the input from the first round H_{i-1} to the output of the eighty-first round. Using addition modulo 2^{64}, each of the eighth words in the buffer is separately added to each of the corresponding words in H_{i-1}.

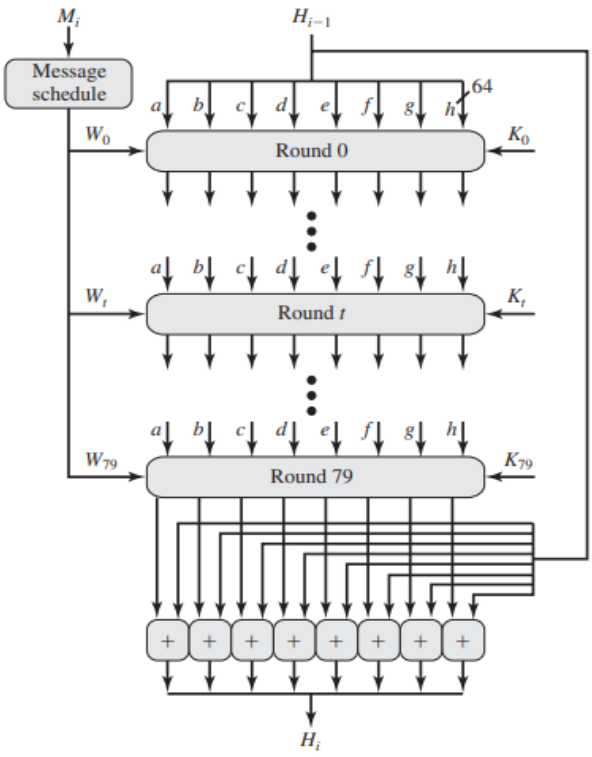


Figure 28.2 SHA-512 Processing of a Single 1024 Bit Block

Note: Copyrights of this diagram are reserved for original author

where

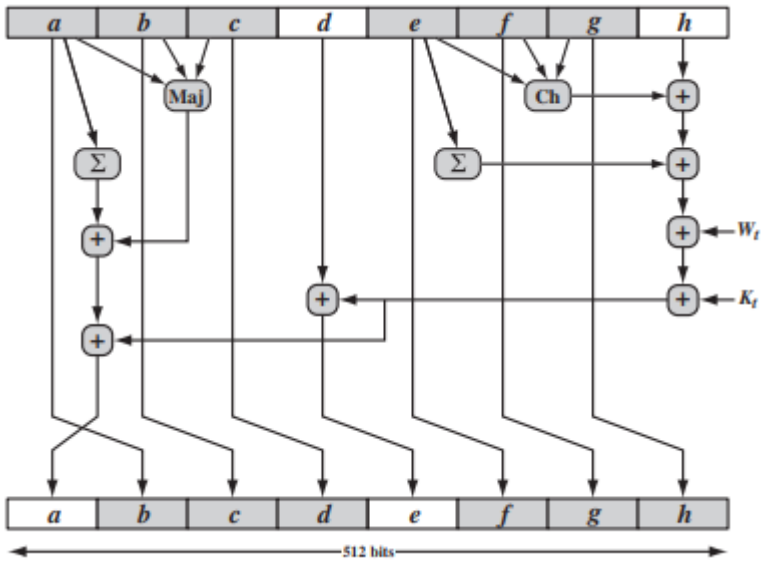
IV = initial value of the abcdefgh buffer, defined in step 3

$abcdefgh_i$ = the output of the last round of processing of the ith message block

N = the number of blocks in the message (including padding and length fields)

SUM_{64} = addition modulo 2^{64} performed separately on each word of the pair of inputs

MD = final message digest value



$$T_1 = h + \text{Ch}(e, f, g) + \left(\sum_1^{512} e\right) + W_t + K_t$$

$$T_2 = \left(\sum_0^{512} a\right) + \text{Maj}(a, b, c)$$

$$h = g$$

$$g = f$$

$$f = e$$

$$e = d + T_1$$

$$d = c$$

$$c = b$$

$$b = a$$

$$a = T_1 + T_2$$

where

t = step number; $0 \leq t \leq 79$

$\text{Ch}(e, f, g) = (e \text{ AND } f) \oplus (\text{NOT } e \text{ AND } g)$
the conditional function: If e then f else g

$$\begin{aligned}
\text{Maj}(a, b, c) &= (a \text{ AND } b) \oplus (a \text{ AND } c) \oplus (b \text{ AND } c) \\
&\quad \textit{the function is true only of the majority (two or three) of the arguments are true} \\
\left(\sum_0^{512} a\right) &= \text{ROTR}^{28}(a) \oplus \text{ROTR}^{34}(a) \oplus \text{ROTR}^{39}(a) \\
\left(\sum_1^{512} e\right) &= \text{ROTR}^{14}(e) \oplus \text{ROTR}^{18}(e) \oplus \text{ROTR}^{41}(e) \\
\text{ROTR}^n(x) &= \text{circular right shift (rotation) of the 64-bit argument } x \text{ by } n \text{ bits} \\
W_t &= \text{a 64-bit word derived from the current 512-bit input block} \\
K_t &= \text{a 64-bit additive constant} \\
+ &= \text{addition modulo } 2^{64}
\end{aligned}$$

$$W_t = \sigma_1^{512}(W_{t-2}) + W_{t-7} + \sigma_0^{512}(W_{t-15}) + W_{t-16}$$

where

$$\begin{aligned}
\sigma_0^{512}(x) &= \text{ROTR}^1(x) \oplus \text{ROTR}^8(x) \oplus \text{SHR}^7(x) \\
\sigma_1^{512}(x) &= \text{ROTR}^{19}(x) \oplus \text{ROTR}^{61}(x) \oplus \text{SHR}^6(x) \\
\text{ROTR}^n(x) &= \text{circular right shift (rotation) of the 64-bit argument } x \text{ by } n \text{ bits} \\
\text{SHR}^n(x) &= \text{left shift of the 64-bit argument } x \text{ by } n \text{ bits with padding by zeros on the right} \\
+ &= \text{addition modulo } 2^{64}
\end{aligned}$$

Figure 28.3 Single Round Processing of SHA-512

28.7 Activities (One Minute Paper):

1. State the value of the padding field in SHA-512 if the length of the message is

a. 1919 bits

b. 1920 bits

c. 1921 bits

2. State the value of the length field in SHA-512 if the length of the message is

a. 1919 bits

b. 1920 bits

c. 1921 bits

28.8 Examples: NA

28.9 Table Numbering: NA

28.10 Figures with Captions:

Figure 25.1 SHA-512 Block Diagram

Figure 25.2 SHA-512 Processing of a Single 1024 Bit Block

Figure 25.3 Single Round Processing of SHA-512

28.11 Self-Assessment Questions

1. What does "SHA" stand for in SHA-512?

a) Secure Hash Algorithm

b) Secret Hash Algorithm

c) Strong Hash Algorithm

d) Structured Hash Algorithm

2. SHA-512 produces a hash value of what size in bits?

a) 64 bits

b) 128 bits

c) 256 bits

d) 512 bits

3. Which of the following is true about SHA-512?

a) It is a symmetric encryption algorithm.

b) It is used for digital signatures.

c) It is a key exchange algorithm.

d) It is a cryptographic hash function.

4. The input block size of SHA-512 is:

a) 128 bits

b) 256 bits

c) 512 bits

d) 1024 bits

5. SHA-512 belongs to which family of hash functions?

a) MD5

b) SHA-1

c) SHA-2

d) SHA-3

6. How many rounds does SHA-512 use in its compression function?

a) 48

b) 64

c) 80

d) 128

7. Which of the following is a potential use case for SHA-512?

a) Encrypting data for secure transmission

b) Generating random numbers

c) Creating a digital signature for a document

d) Performing a Diffie-Hellman key exchange

8. What is the collision resistance property of SHA-512?

a) It is infeasible to find two different inputs that produce the same hash output.

b) It is infeasible to reverse the hash to obtain the original input.

c) It guarantees the uniqueness of the hash output for any input.

d) It ensures the security of the key used in the algorithm.

9. In SHA-512, the message is processed in blocks of how many bytes?

a) 32 bytes

b) 64 bytes

c) 128 bytes

d) 256 bytes

10. Which of the following attacks is SHA-512 vulnerable to?

a) Birthday attack

b) Differential cryptanalysis

c) Brute-force attack

d) Meet-in-the-middle attack

11. The Merkle-Damgård construction is used in SHA-512 to:

a) Encrypt the data

b) Decrypt the data

c) Create the padding for the input message

d) Generate the final hash output

12. Which of the following statements about the security of SHA-512 is true?

a) It is considered broken and insecure.

b) It is secure against pre-image attacks.

c) It is immune to all known cryptographic attacks.

d) It is susceptible to collision attacks.

13. The initial hash values used in SHA-512 are derived from:

a) The value of π (pi)

b) The square root of 2

c) The golden ratio (φ)

d) The first 64 bits of the fractional parts of the square roots of the first 8 prime numbers

14. How does SHA-512 handle input messages longer than the block size?

a) It truncates the message to fit the block size.

b) It pads the message to a multiple of the block size.

c) It discards the excess data.

d) It encrypts the message in multiple passes.

15. Which of the following is an advantage of SHA-512 over its predecessors like SHA-1?

a) Faster computation speed

b) Shorter hash output size

c) Higher collision resistance

d) Better support for key exchange

16. Which of the following is a drawback of using SHA-512?

a) It is not widely supported in cryptographic libraries.

b) It is vulnerable to timing attacks.

c) It has a slow hashing speed.

d) It is not resistant to length extension attacks.

17. In SHA-512, the compression function combines the message block with the current hash value using which operation?

a) XOR

b) Addition

c) Modular multiplication

d) Modular addition

18. Which of the following applications commonly uses SHA-512 for security purposes?

a) Email communication

b) Database indexing

c) Password hashing

d) Video streaming

19. The output of the SHA-512 algorithm is often represented as a:

a) Hexadecimal string

b) Binary tree

c) ASCII text

d) Decimal number

20. The "512" in SHA-512 refers to:

a) The number of rounds in the compression function

b) The size of the internal state

c) The length of the output hash in bits

d) The size of the block processed in bytes

28.12 Summary

SHA-512 is a trusted and extensively used cryptographic hash function, to sum up. It offers robust security features, a huge hash size, and a wide range of applications in different security systems.

However, it is crucial to take into account the particular needs and potential weaknesses related to its execution.

28.13. Terminal Questions

1. Demonstrate Single block processing of SHA-512
2. Illustrate Single Round Operations of SHA-512
3. Summarize the steps involved in generating Hash Code using SHA 512.
4. What is the difference between little-endian and big-endian format?
5. What basic arithmetical and logical functions are used in SHA?

28.14 Answer Key:

Self -Assessment-Questions -Answers

1. a) Secure Hash Algorithm
2. d) 512 bits
3. d) It is a cryptographic hash function.
4. c) 512 bits
5. c) SHA-2
6. c) 80
7. c) Creating a digital signature for a document
8. a) It is infeasible to find two different inputs that produce the same hash output.
9. b) 64 bytes
10. a) Birthday attack
11. c) Create the padding for the input message
12. c) It is immune to all known cryptographic attacks.
13. d) The first 64 bits of the fractional parts of the square roots of the first 8 prime numbers
14. b) It pads the message to a multiple of the block size.
15. c) Higher collision resistance
16. c) It has a slow hashing speed.
17. a) XOR
18. c) Password hashing

19. a) Hexadecimal string

20. c) The length of the output hash in bits

1.

Each round updates the contents of the buffer using the 512-bit buffer value abcdefgh as input. The intermediate hash value H_{i-1} is present in the buffer at the start of the first round. Each round t uses a 64-bit value W_t that is taken from the 1024-bit block that is currently being processed. These values are obtained using the message scheduling that is detailed below. Additionally, an additive constant K_t is utilized for each of the 80 rounds. The first 64 bits of the cube roots of the first 80 prime numbers are represented by these words. A "randomized" set of 64-bit patterns are provided by the constants, which should get rid of any regularities in the input data. The result is created by adding the input from the first round H_{i-1} to the output of the eighty-first round. Using addition modulo 2^{64}, each of the eighth words in the buffer is separately added to each of the corresponding words in H_{i-1}.

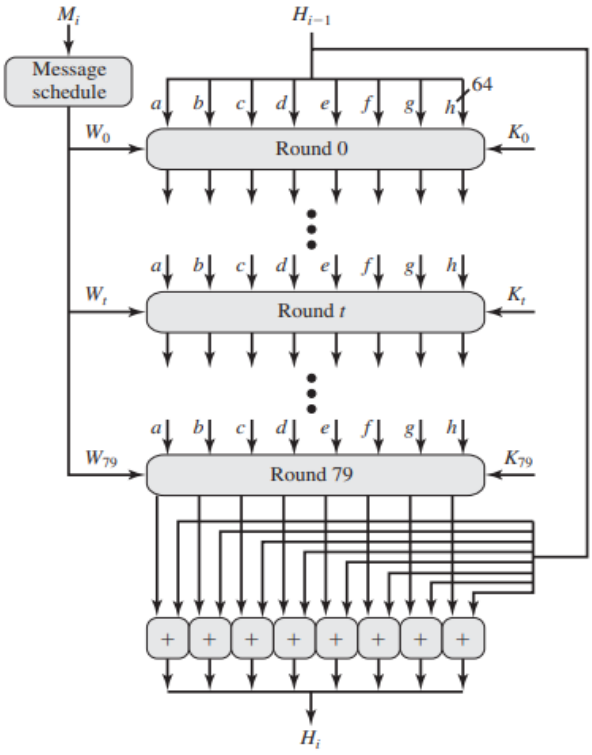


Figure SHA-512 Processing of a Single 1024 Bit Block

Note: Copyrights of this diagram are reserved for original author

where

IV = initial value of the abcdefgh buffer, defined in step 3

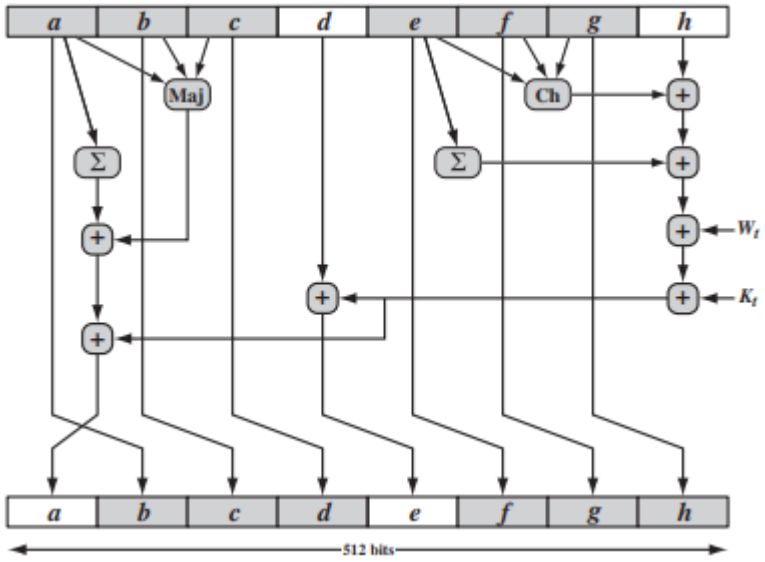
$abcdefgh_i$ = the output of the last round of processing of the ith message block

N = the number of blocks in the message (including padding and length fields)

SUM_{64} = addition modulo 2^{64} performed separately on each word of the pair of inputs

MD = final message digest value

2.



$$T_1 = h + \text{Ch}(e, f, g) + \left(\sum_1^{512} e\right) + W_t + K_t$$

$$T_2 = \left(\sum_0^{512} a\right) + \text{Maj}(a, b, c)$$

$$h = g$$

$$g = f$$

$$f = e$$

$$e = d + T_1$$

$$d = c$$

$$c = b$$

$$b = a$$

$$a = T_1 + T_2$$

where

t = step number; $0 \le t \le 79$

$\text{Ch}(e, f, g) = (e \text{ AND } f) \oplus (\text{NOT } e \text{ AND } g)$
the conditional function: If e then f else g

$\text{Maj}(a, b, c) = (a \text{ AND } b) \oplus (a \text{ AND } c) \oplus (b \text{ AND } c)$
the function is true only of the majority (two or three) of the arguments are true

$\left(\sum_0^{512} a\right) = \text{ROTR}^{28}(a) \oplus \text{ROTR}^{34}(a) \oplus \text{ROTR}^{39}(a)$

$\left(\sum_1^{512} e\right) = \text{ROTR}^{14}(e) \oplus \text{ROTR}^{18}(e) \oplus \text{ROTR}^{41}(e)$

$\text{ROTR}^n(x)$ = circular right shift (rotation) of the 64-bit argument x by n bits

W_t = a 64-bit word derived from the current 512-bit input block

K_t = a 64-bit additive constant

$+$ = addition modulo 2^{64}

$$W_t = \sigma_1^{512}(W_{t-2}) + W_{t-7} + \sigma_0^{512}(W_{t-15}) + W_{t-16}$$

where

$\sigma_0^{512}(x) = \text{ROTR}^1(x) \oplus \text{ROTR}^8(x) \oplus \text{SHR}^7(x)$

$\sigma_1^{512}(x) = \text{ROTR}^{19}(x) \oplus \text{ROTR}^{61}(x) \oplus \text{SHR}^6(x)$

$\text{ROTR}^n(x)$ = circular right shift (rotation) of the 64-bit argument x by n bits

$\text{SHR}^n(x)$ = left shift of the 64-bit argument x by n bits with padding by zeros on the right

$+$ = addition modulo 2^{64}

Figure Single Round Processing of SHA-512

Note: Copyrights of this diagram are reserved for original author

3.

The algorithm outputs a 512-bit message digest from an input message with a maximum length of less than 2^{128} bits. 1024-bit blocks of the input are processed at once.

a. ***Append Padding Bits:*** The message is padded to make it exactly 896 modulo 1024 in length. Even if the message is of the desired length, padding is always applied. The range of padding bits is therefore from 1 to 1024. A single 1 bit precedes the necessary amount of 0 bits in the padding.
b. ***Append Length:*** The message has a block of 128 bits added to it.The most significant byte

is placed first in this block, which is interpreted as an unsigned 128-bit integer and contains the length of the original message (before padding).

The result of the first two stages is a message with a length that is an integer multiple of 1024 bits.

c. **Initialize hash buffer**. The hash function's intermediate and final results are stored in a 512-bit buffer.Eight 64-bit registers (designated as a, b, c, d, e, f, g, and h) can be used to represent the buffer. The following 64-bit numbers (represented in hexadecimal values) are used as the registers' initial values:. Big-endian format, which places the most important byte of a word at the low-address (leftmost) byte position, is how these values are stored.

d. **Process message in 1024-bit (128-word) blocks:** The heart of the algorithm is a module that consists of 80 rounds.

e. **Output.** After all 1024-bit blocks have been processed, the output from the th stage is the 512-bit message digest.

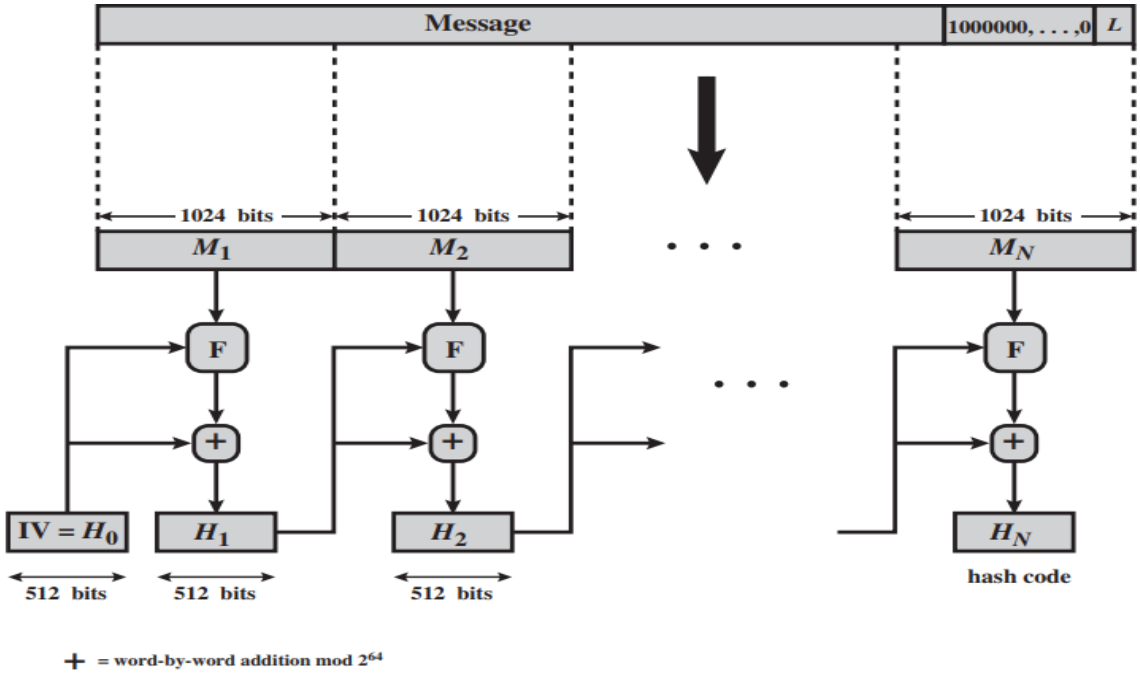


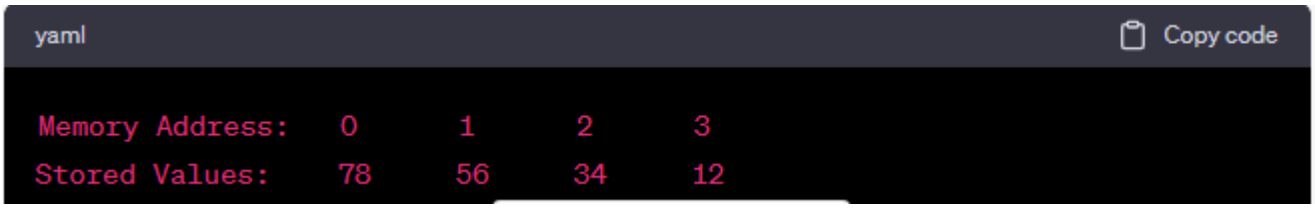
Figure SHA-512 Block Diagram

4.

Little-Endian: In little-endian format, the most significant byte (MSB) is saved at the highest memory address while the least significant byte (LSB) is placed at the lowest memory address for

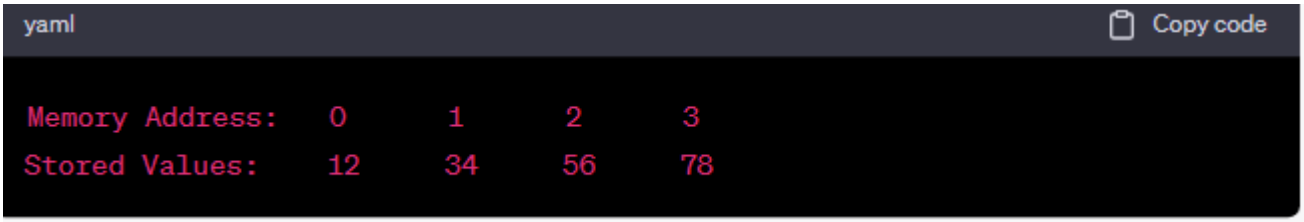
a multi-byte data type. It reads data normally, starting with the LSB and reading from left to right. In x86-based processors like Intel and AMD, little-endian is frequently employed.

Example: A 32-bit little-endian integer with the value 0x12345678 would be kept in memory as follows:



Big-Endian: In big-endian format, the least significant byte (LSB) is saved at the highest memory address and the least significant byte (MSB) is placed at the lowest memory address for a multi-byte data type. The MSB is read first as is customary when reading data, which is done from left to right. Network protocols and architectures like ARM and PowerPC frequently employ big-endian.

Example: The same 32-bit integer, in big-endian format, with the value 0x12345678, would be kept in memory as follows:



4.

logical bitwise operations

AND: Converts two operands into a bitwise AND operation. It is frequently used to merge or mask bits in SHA.

OR: Converts two operands into a bitwise OR operation. It's employed to set or combine particular bits.

XOR: Executes an exclusive OR (bitwise) operation between two operands. It is employed to toggle or flip bits.

Functions for bitwise shifting:

Shifts an operand's bits left by a predetermined number of places using the left shift operation. In SHA, it is applied to rotate or relocate bits.

Right Shift: Moves an operand's bits to the right by a predetermined number of places. It is employed to remove or eliminate bits.

Addition via modules:

Addition (mod 2 N): Addition is done mod 2 N, where N is the number of bits in the operands. By performing this process, the desired bit length is maintained in the result.

XOR and modular addition:

Updates to the working variables and intermediate hash values in SHA are made via the modular addition and XOR procedure.

logical processes

NOT: Flips all the bits in a bitwise complement operation on an operand. In some SHA computations, it is utilized for negation or inversion.

Logical Operations: To manipulate and combine bits, SHA uses a variety of logical operations, including logical AND, logical OR, and logical NOT.

28.15 Case studies: NA

28.16 Glossary: NA

28.17 References

1. Cryptography and Network Security Principles and Practice, by William stallings, Pearson, 5th edition.

2.Applied Cryptography: Protocols, Algorthms, and Source Code in C , by Bruce Schneier, Second Edition , John Wiley & Sons, Inc., 2015.

3.Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, by Hamid R. Nemati and Li Yang, IGI Global, 2011

4. Forouzon B, “Cryptography and Network Security,” Indian Edition, TMH (2010).

28.18 Keywords

Simple Hash Function, bit-by-bit XOR,CBC

CRYPTANALYSIS & CYBER DEFENSE

21CS3041RA

Course Description: This course provides an introduction to the core principles of cryptography and its relevance in the field of network security. Students will gain a comprehensive understanding of cryptographic methods used to ensure secure communication in potentially insecure environments. Topics covered include techniques for verifying message source authenticity, ensuring message integrity during transmission across unsecured channels, and establishing unique message origin identification. The course also addresses cryptanalysis attacks on cryptographic techniques, as well as various attack models.

SESSION: 29

Message Digest 5 (MD5)

29.1 Aim

Demonstrate hash algorithm like Message Digest 5 (MD5).

29.2 Instructional Objectives

The objective of this session is to introduce the basic concepts of Hash Functions. It provides the necessary theoretical background and demonstrates attacks on hash functions.

29.3 Learning Outcomes

At the end of this session, you should be able to:

8. Demonstrate MD5 hash algorithm.

29.4 Module Description

This module defines Hash function. Applications of Hash algorithms are also discussed in this module. Secure Hash Algorithm (SHA 512) algorithms are demonstrated. Calculating Hash value using two simple hash functions is also discussed. Similarly MD5 is also discussed. Message Authentication Code (MAC) algorithms are also discussed.

29.5 Session Introduction

This session starts with the introduction of MD5. It illustrates block diagram of MD5and the operations being carried in a single round of MD5 in detail.

29.6 Session Description

29.6.1 Message Digest Algorithm (MD5)

The Hash Function Family

- ✓ **MD (Message Digest)**

Designed by Ron Rivest

Family: MD2, MD4, MD5

MD (Message Digest)

- A message digest, also known as a hash value or hash code, is a fixed-size numerical representation derived from a given input data of arbitrary length. It is generated using a mathematical algorithm called a hash function.
- The purpose of a message digest is to provide a unique and condensed representation of the input data. The resulting digest is typically a fixed-length sequence of characters or bits, regardless of the size of the original input. This makes it useful for verifying the integrity of data, detecting changes or tampering, and ensuring data authenticity.

Message digests have several important properties:

- **Deterministic**: Given the same input, a hash function will always produce the same digest. This property allows for consistency and reproducibility.
- **Fixed Size:** The length of the digest is typically fixed, regardless of the input size. Common hash functions, such as MD5, SHA-1, and SHA-256, produce digests of specific lengths (e.g., 128 bits, 160 bits, 256 bits).
- **One-Way:** It is computationally infeasible to reconstruct the original input data from its digest. A small change in the input will result in a significantly different digest.
- **Collision Resistance:** It is extremely unlikely for two different inputs to produce the same digest. However, as the input space is typically larger than the digest space, collisions (two different inputs producing the same digest) are theoretically possible, but highly improbable with well-designed hash functions.

Message digests are widely used in various applications, including data integrity checks, digital signatures, password storage (with salted hashes), and checksums. They provide a way to verify that data remains unchanged and hasn't been tampered with during transmission or storage.

MD5, SHA-1

	MD5	SHA-1
Digest length	128 bits	160 bits
Basic unit of processing	512 bits	512 bits
Number of steps	64 (4 rounds of 16)	80 (4 rounds of 20)
Maximum message size	∞	2^{64} - 1 bits
Primitive logical functions	4	4
Additive constants used	64	4
Endianness	Little-endian	Big-endian

Fig 29.1 MD5 & SHA-1
Note: Copyrights of this figure are reserved with original author

Sample Processing

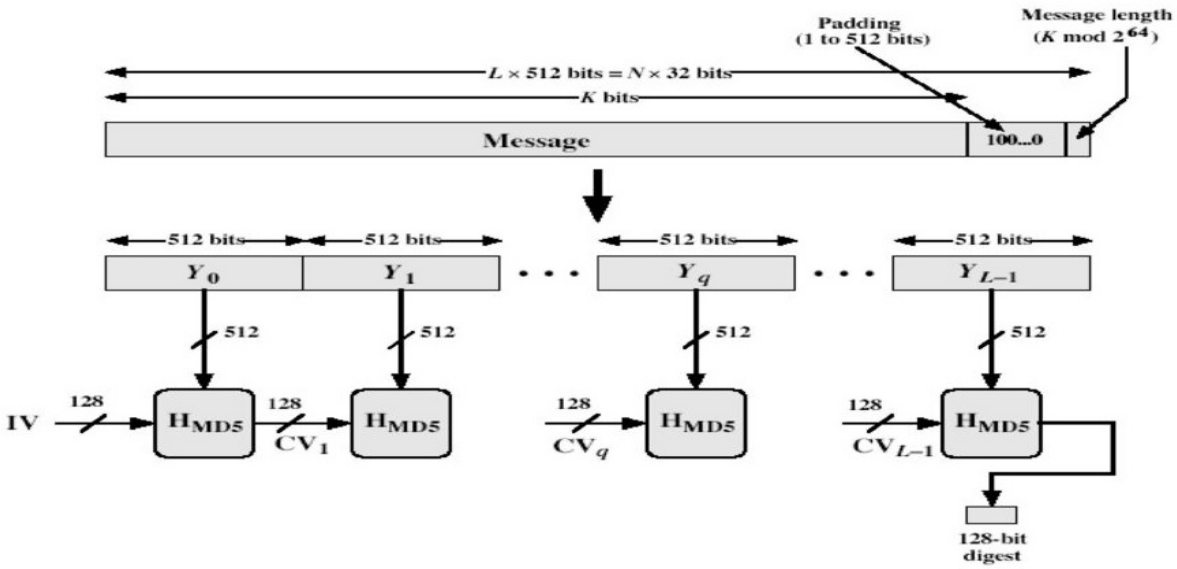
Type	bits	data processed
MD5	128	469.7 MB/s
SHA-1	160	339.4 MB/s
SHA-512	512	177.7 MB/s

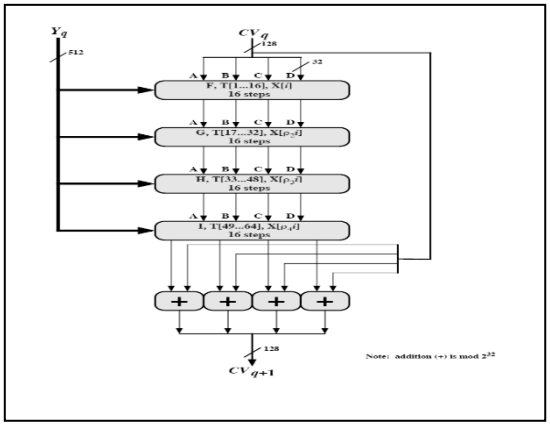
Mac Intel 2.66 Ghz core i7
1024 bytes block of data

MD2, MD4 and MD5

- Family of one-way hash functions by Ronald Rivest
  - All produces 128 bits hash value
- MD2: 1989
  - Optimized for 8 bit computer
  - Collision found in 1995
- MD4: 1990
  - Full round collision attack found in 1995
- MD5: 1992
  - Specified as Internet standard in RFC 1321
  - since 1997 it was theoretically not so hard to create a collision
  - Practical Collision MD5 has been broken since 2004

- CA attack published in 2007

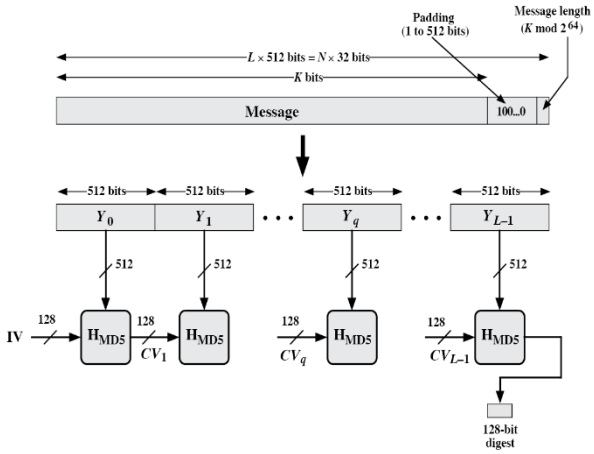


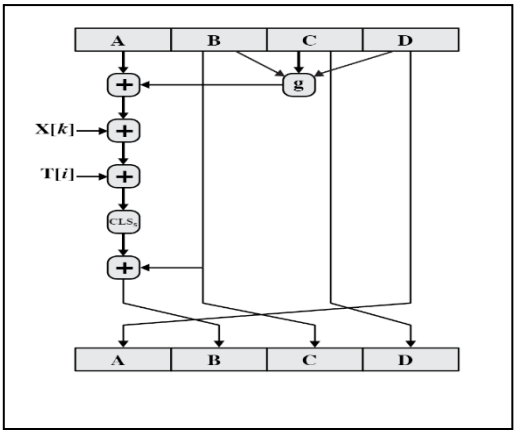


b	c	d	F	G	H	I
0	0	0	0	0	0	1
0	0	1	1	0	1	0
0	1	0	0	1	1	0
0	1	1	1	0	0	1
1	0	0	0	0	1	1
1	0	1	0	1	0	1
1	1	0	1	1	0	0
1	1	1	1	1	1	0

Figure 29.2 Overview of MD5

Note: Copyrights of this figure are reserved with original author





X[k] = M [q*16+k] (32 bit)

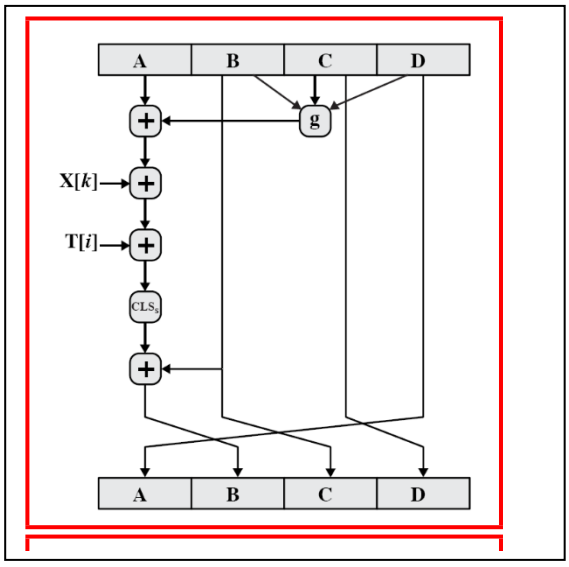
X[k] = M [q*16+k] (32 bit)

Figure 29.3 Hash Algorithm Design – MD5

Note: Copyrights of this figure are reserved with original author

The ith 32-bit word in matrix T, constructed from the sine function

M [q*16+k] = the kth 32-bit word from the qth 512-bit block of the



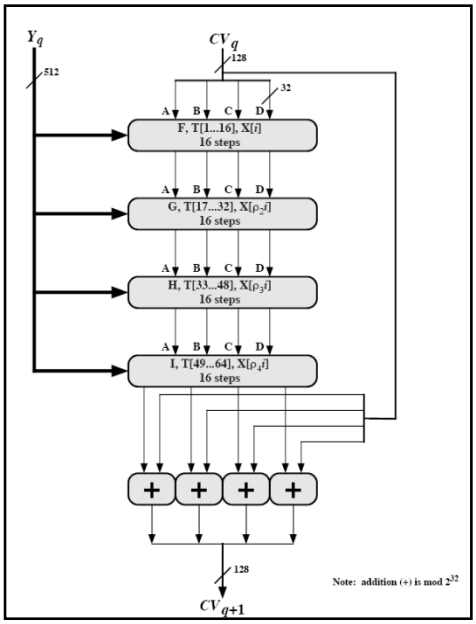


Fig 29.4 Hash Algorithm Design – MD5

Note: Copyrights of this figure are reserved with original author

Hash Function Cryptanalysis

- cryptanalytic attacks exploit some property of algorithm so faster than exhaustive search
- hash functions use iterative structure
  - process message in blocks (incl length)
- attacks focus on collisions in function f

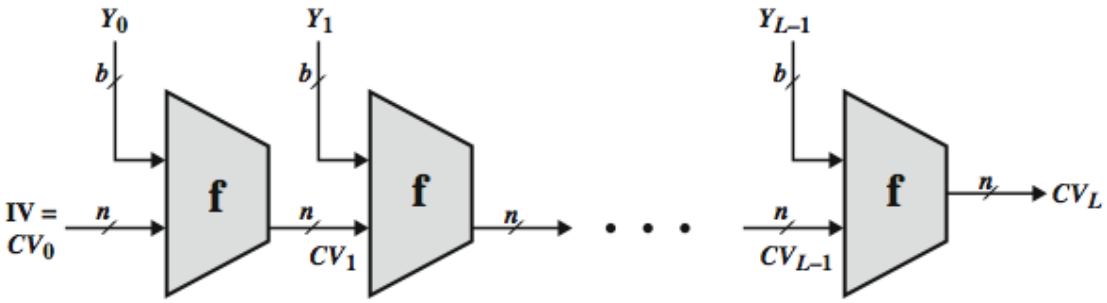


Fig 29.5 Hash Function Cryptanalysis

Note: Copyrights of this figure are reserved with original author

"md5 and sha1 are both clearly broken (in terms of collision-resistance"

Ron Rivest

Attacks on Hash Functions

- brute-force attacks and cryptanalysis
    - cryptanalytic attacks exploit some property of algorithm so faster than brute-force
- a preimage or second preimage attack
    - find *y* such that *H(y)*equals a given hash value
- collision resistance
    - find two messages x &*y* with same hash so H(x) = H(y)

The need of new Hash standard

- *MD5 should be considered cryptographically broken and unsuitable for further use*, US CERT 2010
- In 2004, a collision for the full SHA-0 algorithm was announced
- SHA-1 not yet fully "broken"
    - but similar to the broken MD5 & SHA-0
    - so considered insecure and be fade out
- SHA-2 (esp. SHA-512) seems secure
    - shares same structure and mathematical operations as predecessors so have concern

29.7 Activities (Problem Solving): NA

29.8 Example :NA

29.9 Table Numbering : NA

29.10 Figures with captions

29.11 Self-Assessment Questions

1. What is MD5 used for in cryptography?
   a) Data Encryption
   b) Data Compression
   c) Data Integrity
   d) Data Authentication

2. What is the output size of MD5 in bits?
   a) 32 bits
   b) 64 bits
   c) 128 bits
   d) 256 bits

3. MD5 produces a fixed-size hash value for any input of arbitrary length. What is the size of this hash value in bytes?
   a) 4 bytes
   b) 8 bytes
   c) 16 bytes
   d) 32 bytes

4. Is MD5 a cryptographic hash function?
   a) Yes
   b) No

5. Which of the following is a security weakness of MD5?
   a) Pre-image resistance
   b) Collision resistance
   c) Second pre-image resistance
   d) Output size resistance

6. Can MD5 be used for password hashing?
   a) Yes
   b) No

7. What is a primary reason why MD5 is considered weak for many cryptographic applications?
   a) It is slow
   b) It has a small block size
   c) It is vulnerable to collision attacks
   d) It produces large hash values

8. Which of the following hash functions is more secure than MD5?
   a) SHA-1
   b) SHA-256
   c) SHA-512
   d) SHA-3

9. MD5 is commonly used in which area of security protocols?

a) SSL/TLS Certificates
b) Digital Signatures
c) Password Storage
d) Public Key Infrastructure (PKI)

10. MD5 is a one-way function. What does it mean?
a) The function can only be computed in one direction.
b) The function can be computed in both directions.
c) The function can be reversed with a secret key.
d) The function can be decrypted with the original data.

11. Which property ensures that even a small change in the input will produce a significantly different hash value?
a) Pre-image resistance
b) Second pre-image resistance
c) Collision resistance
d) Avalanche effect

12. Can two different inputs produce the same MD5 hash value?
a) Yes, it is possible
b) No, it is not possible

13. What type of attack involves finding two different inputs that produce the same MD5 hash?
a) Pre-image attack
b) Second pre-image attack
c) Collision attack
d) Birthday attack

14. Which organization introduced MD5 in 1991?
a) National Institute of Standards and Technology (NIST)
b) International Organization for Standardization (ISO)
c) United States Computer Emergency Readiness Team (US-CERT)
d) RSA Data Security, Inc.

15. True or False: MD5 is still considered secure for cryptographic applications.
A) Ture
b) False
16. Which of the following applications would benefit most from using MD5 for integrity checking?
a) Digital Signatures
b) Password Storage
c) Digital Certificates
d) File Integrity Verification

17. Which of the following attacks is NOT relevant when discussing the security weaknesses of MD5?
a) Brute-force attack
b) Rainbow table attack

c) Collision attack
d) Differential cryptanalysis

18. What is the primary reason why MD5 is no longer considered secure?
a) It has a short key length
b) It lacks pre-image resistance
c) It is computationally slow
d) It has a large block size

19. Which cryptographic property does MD5 lack, making it vulnerable to collision attacks?
a) Pre-image resistance
b) Second pre-image resistance
c) Avalanche effect
d) Compression function

20. What is the recommended replacement for MD5 in modern cryptographic applications?
a) SHA-1
b) SHA-256
c) AES
d) DES

29.12 Summary

MD5 is a trusted and extensively used cryptographic hash function, to sum up. It offers robust security features, a huge hash size, and a wide range of applications in different security systems. However, it is crucial to take into account the particular needs and potential weaknesses related to its execution.

29.13. Terminal Questions

1. Compare & Contrast SHA-512 & MD5.

2. Illustrate MD5 with a neat diagram

3. How does the MD5 algorithm process input messages of arbitrary length? Explain the steps involved in dividing the input message into fixed-sized blocks.

4. Describe the series of logical functions, bitwise operations, and modular addition used in MD5 to process each block of the input message. How do these operations contribute to the computation of the final hash value?

5. Discuss the internal state maintained by MD5 during its computation. How is the state updated as the algorithm progresses through the blocks of the input message? Explain the role of the intermediate hash value in this process.

29.14 Answer Key:

Self- Assessment-Questions -Answers

1c) Data Integrity
2. c) 128 bits
3. c) 16 bytes
4. a) Yes
5. b) Collision resistance
6. a) Yes
7. c) It is vulnerable to collision attacks
8. b) SHA-256
9. c) Password Storage
10. a) The function can only be computed in one direction.
11. d) Avalanche effect
12a) Yes, it is possible
13. c) Collision attack
14. d) RSA Data Security, Inc.
15. Answer: b)False
16. d) File Integrity Verification
17. d) Differential cryptanalysis
18. b) It lacks pre-image resistance
19. c) Avalanche effect
20. b) SHA-256

1. Security:

SHA-512: This hash function is regarded as being quite secure. It is a member of the widely used SHA-2 family of algorithms, which is currently thought to be secure against known attacks.

On the other hand, MD5 is now regarded as insecure for cryptographic applications. It has a number of weaknesses, including pre-image assaults, collision attacks, and the availability of effective computational methods to compromise its security.

Output Size:

SHA-512: The output of SHA-512 has a fixed length of 512 bits (64 bytes).

A fixed-length output of 128 bits (16 bytes) is produced by MD5.

Computational Complexity:

SHA-512: When compared to MD5, SHA-512 is computationally more difficult. It is slower but offers better security because it has a greater state size, more calculation rounds, and more complicated operations.

Compared to SHA-512, MD5 is computationally simpler and faster. It is less secure and more vulnerable to brute-force and other attacks since it has a lower state size and fewer computation rounds.

Vulnerabilities:

SHA-512: At this time, SHA-512 is regarded as secure against recognized cryptographic attacks, and no usable flaws have been discovered.

MD5: MD5 is susceptible to a number of techniques, such as collision attacks, in which two distinct inputs can result in the same hash value. Additionally, it is vulnerable to pre-image attacks, in which a perpetrator creates input that exactly matches a certain hash value.

Usage and Recommendation:

SHA-512: SHA-512 is suggested for a number of cryptographic applications, including secure data integrity checks, password hashing, and digital signatures.

For cryptographic uses, MD5 is no longer advised owing to security flaws. In particular, it shouldn't be utilized for activities like password storage or digital signatures in applications that require high levels of security.

2.

The Hash Function Family

✓ MD (Message Digest)

Designed by Ron Rivest

Family: MD2, MD4, MD5

MD (Message Digest)

- A message digest, also known as a hash value or hash code, is a fixed-size numerical representation derived from a given input data of arbitrary length. It is generated using a mathematical algorithm called a hash function.
- The purpose of a message digest is to provide a unique and condensed representation of the input data. The resulting digest is typically a fixed-length sequence of characters or bits, regardless of the size of the original input. This makes it useful for verifying the integrity of data, detecting changes or tampering, and ensuring data authenticity.

Message digests have several important properties:

- Deterministic: Given the same input, a hash function will always produce the same digest. This property allows for consistency and reproducibility.
- Fixed Size: The length of the digest is typically fixed, regardless of the input size. Common hash functions, such as MD5, SHA-1, and SHA-256, produce digests of specific lengths (e.g., 128 bits, 160 bits, 256 bits).
- One-Way: It is computationally infeasible to reconstruct the original input data from its digest. A small change in the input will result in a significantly different digest.
- Collision Resistance: It is extremely unlikely for two different inputs to produce the same digest. However, as the input space is typically larger than the digest space, collisions (two different inputs

producing the same digest) are theoretically possible, but highly improbable with well-designed hash functions.

Message digests are widely used in various applications, including data integrity checks, digital signatures, password storage (with salted hashes), and checksums. They provide a way to verify that data remains unchanged and hasn't been tampered with during transmission or storage.

MD5, SHA-1

	MD5	SHA-1
Digest length	128 bits	160 bits
Basic unit of processing	512 bits	512 bits
Number of steps	64 (4 rounds of 16)	80 (4 rounds of 20)
Maximum message size	∞	2^{64} - 1 bits
Primitive logical functions	4	4
Additive constants used	64	4
Endianness	Little-endian	Big-endian

Fig 26.1 MD5 & SHA-1

Note: Copyrights of this figure are reserved with original author

Sample Processing

Type	bits	data processed
MD5	128	469.7 MB/s
SHA-1	160	339.4 MB/s
SHA-512	512	177.7 MB/s

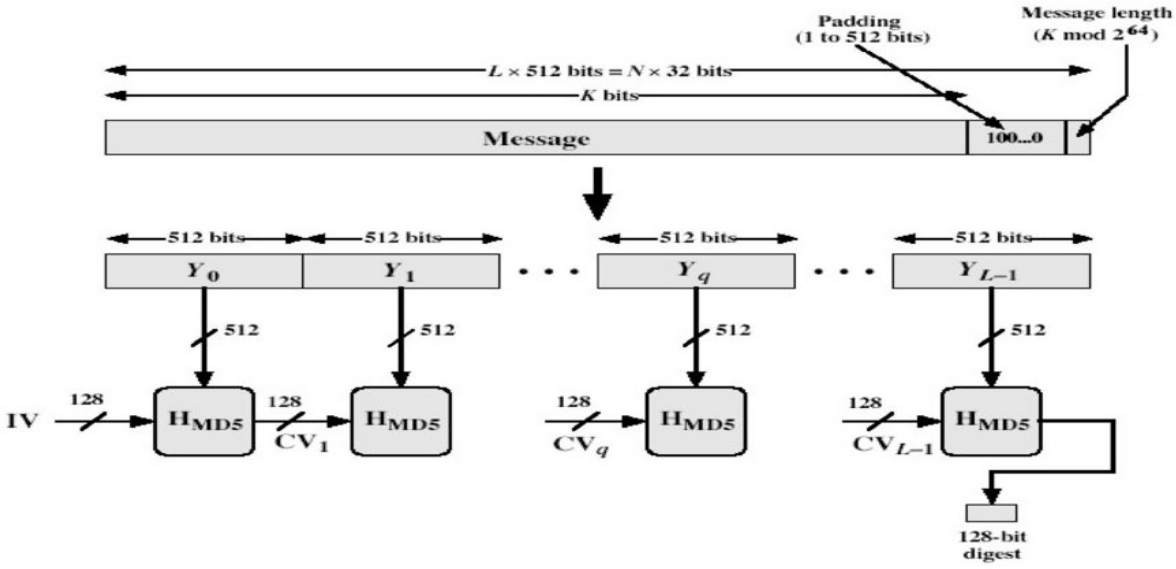
Mac Intel 2.66 Ghz core i7

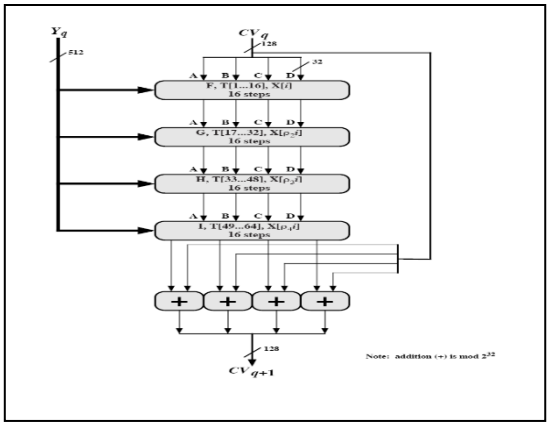
1024 bytes block of data

MD2, MD4 and MD5

- Family of one-way hash functions by Ronald Rivest
- All produces 128 bits hash value
- MD2: 1989
- Optimized for 8 bit computer
- Collision found in 1995

- MD4: 1990
- Full round collision attack found in 1995
- MD5: 1992
- Specified as Internet standard in RFC 1321
- since 1997 it was theoretically not so hard to create a collision
- Practical Collision MD5 has been broken since 2004
- CA attack published in 2007

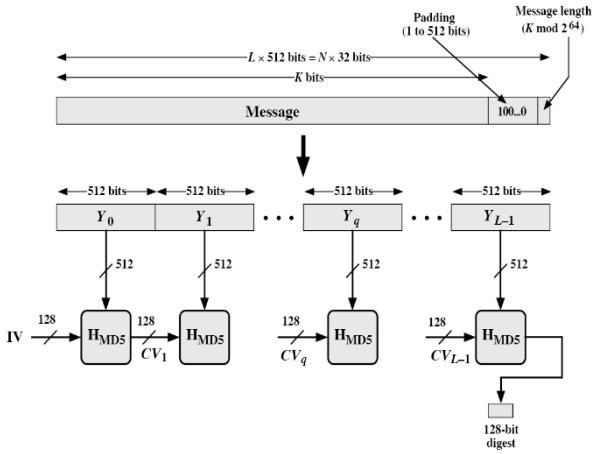


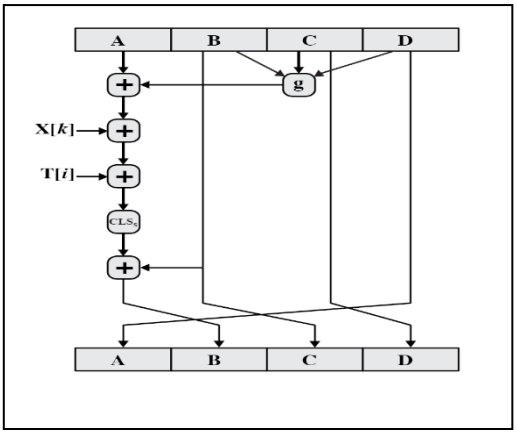


b	c	d	F	G	H	I
0	0	0	0	0	0	1
0	0	1	1	0	1	0
0	1	0	0	1	1	0
0	1	1	1	0	0	1
1	0	0	0	0	1	1
1	0	1	0	1	0	1
1	1	0	1	1	0	0
1	1	1	1	1	1	0

Figure 29.2 Overview of MD5

Note: Copyrights of this figure are reserved with original author





X[k] = M [q*16+k] (32 bit)

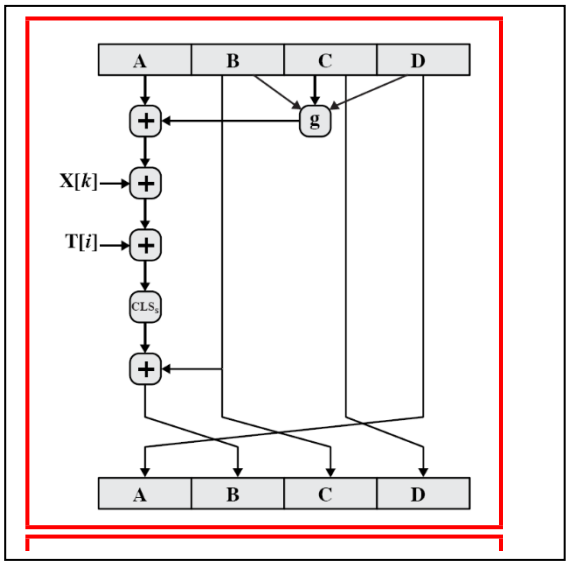
X[k] = M [q*16+k] (32 bit)

Figure 29.3 Hash Algorithm Design – MD5

Note: Copyrights of this figure are reserved with original author

The ith 32-bit word in matrix T, constructed from the sine function

M [q*16+k] = the kth 32-bit word from the qth 512-bit block of the



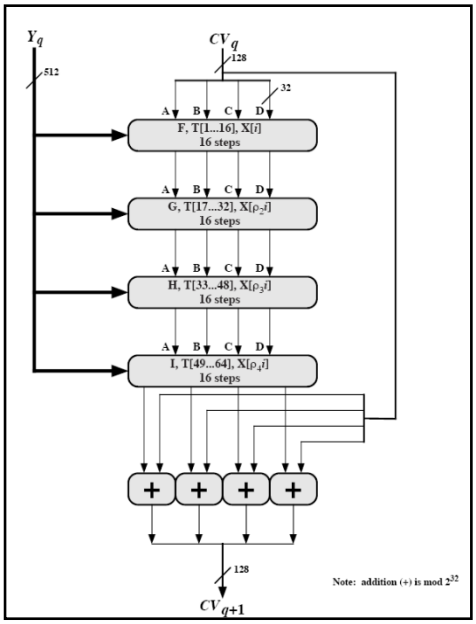


Fig 29.4 Hash Algorithm Design – MD5

Note: Copyrights of this figure are reserved with original author

3.

Padding: To enable it to be separated into equal-sized blocks, MD5 first paddings the input message. To make the message the desired length, the padding scheme adds extra bits. The padding ensures that the message's overall length is consistent with 448 modulo 512 and always consists of a "1" bit followed by a string of "0" bits.

After padding, MD5 adds a 64-bit representation of the original message length as the length representation. The length in bits is added as a binary representation in this representation. The 64-bit representation, for instance, would be "000...0010010110" if the original message was 150 bits long. This is because the leading zeroes are appended to make the length 64 bits.

Block Division: The message is then split into fixed-sized blocks of 512 bits (64 bytes) after padding and length representation have been added. 16 words, each measuring 32 bits (4 bytes), make up each block.

Block processing: The MD5 algorithm goes over each block one at a time. The "IV" (Initialization

Vector), a set of specified constant values, serves as the initial state. The final state corresponds to the hash value of the full input message and is updated as each block is analyzed.

The compression function used by MD5 uses a series of logical operations, bitwise transformations, and modular additions to each block. The current block, the intermediate hash value, and particular MD5 algorithm constants are all included in this function.

State Update: The MD5 state is updated as each block is processed. The four 32-bit words that make up the state are A, B, C, and D. These words' values are altered by the compression algorithm dependent on the input block and the current situation. The final state, which is the hash value of the entire input message, is what remains after all blocks have been processed

4.

logical processes

The three 32-bit words X, Y, and Z are used by the non-linear logical function known as the F function. The logical operation (X AND Y) OR ((NOT X) AND Z) is carried out. This function adds nonlinearity and aids in dispersing the impact of the input bits across the entire computation.

The G function uses the same three 32-bit words, X, Y, and Z, as the X function does. It is another non-linear logical function. The logical operation (X AND Z) OR (Y AND (NOT Z)) is carried out. It introduces non-linearity and disperses the influence of the input bits similarly to the F function.

The third non-linear logical operation, known as the H function, uses the same three 32-bit words, X, Y, and Z. The logical procedure X XOR Y XOR Z is carried out. This function increases the computation's complexity and introduces additional non-linearity.

I Function: In MD5, the I function is the last non-linear logical operation. The same three 32-bit words, X, Y, and Z, are used in its operation. The logical operation Y XOR (X OR (NOT Z)) is carried out. This function ensures a good distribution of the input bits while adding additional non-linearity.

Operations using Bits:

Bitwise AND (AND) compares the corresponding bits of two operands and generates a result where the output bit is set to 1 only if both the input bits are 1.

Bitwise OR (OR): This operation compares the corresponding bits of two operands, setting the output bit to 1 if at least one of the input bits is 1.

Bitwise XOR (XOR): When two operands' corresponding bits are compared, the result is an output bit that is set to 1 if the input bits are different and 0 if they are the same.

Bitwise NOT (NOT): This operation flips the bits of a single operand so that each bit of a 1 becomes

a 0 and vice versa.

Addition via modules:

Modular addition (addition modulo 232): During computing, MD5 employs addition modulo 232 to merge data. By ensuring that the outcome stays inside the range of 32 bits, this technique enables effective bitwise operations.

5.

Initialization: The IV values that make up the initial state are loaded into the A, B, C, and D words before processing the first block.

The current intermediate hash value is set to the current state (A, B, C, or D) at the start of processing each block. The total hash value up to the preceding block is represented by this intermediate hash value.

Processing the Block: The current block is compressed using the MD5 algorithm, using the intermediate hash value, the data from the current block, and a few constants. This function generates a new intermediate hash value unique to the current block using a combination of logical operations, bitwise operations, and modular addition.

Update of the State: The intermediate hash value is used to update the state after the current block has been processed. The intermediate hash value is used to modify the state's A, B, C, and D words. The updated state for the following block is determined by the new values of A, B, C, and D.

The algorithm repeats steps 2-4 for each block in the input message, changing the state and the intermediate hash value as necessary. This iterative procedure makes sure that the state changes with each block, taking into account both the data from the most recent block and the total hash computation up to that point.

Final State: The hash value of the entire input message is represented in the final state after all the blocks have been processed. The 128-bit hash value, which is the result of the MD5 algorithm, is produced by concatenating or converting the final state values of A, B, C, and D.

29.15 Case studies: NA

29.16 Glossary:

MD5 – Message Digest

29.17 References

1. Cryptography and Network Security Principles and Practice, by William stallings, Pearson, 5th

edition.

2.Applied Cryptography: Protocols, Algorthms, and Source Code in C , by Bruce Schneier, Second Edition , John Wiley & Sons, Inc., 2015.

3.Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, by Hamid R. Nemati and Li Yang, IGI Global, 2011

4. Forouzon B, “Cryptography and Network Security,” Indian Edition, TMH (2010).

29.18 Keywords

Hash Function, MD5

CRYPTANALYSIS & CYBER DEFENSE

21CS3041RA

Course Description: This course provides an introduction to the core principles of cryptography and its relevance in the field of network security. Students will gain a comprehensive understanding of cryptographic methods used to ensure secure communication in potentially insecure environments. Topics covered include techniques for verifying message source authenticity, ensuring message integrity during transmission across unsecured channels, and establishing unique message origin identification. The course also addresses cryptanalysis attacks on cryptographic techniques, as well as various attack models.

SESSION: 30

Message Authentication Code Algorithms (MAC)

30.1 Aim

Demonstrate Message Authentication Code algorithms.

30.2 Instructional Objectives

The objective of this session is to introduce the basic concepts of MAC. It provides the necessary theoretical background and demonstrates MAC algorithms.

30.3 Learning Outcomes

At the end of this session, you should be able to:

9. Illustrate Message Encryption.
10. Demonstrate HMAC,DAA & CMAC

30.4 Module Description

This module defines Hash function. Applications of Hash algorithms are also discussed in this module. Secure Hash Algorithm (SHA 512) algorithms are demonstrated. Calculating Hash value using two simple hash functions is also discussed. Similarly MD5 is also discussed. Message Authentication Code (MAC) algorithms are also discussed.

30.5 Session Introduction

This session starts with the introduction of MAC. It illustrates block diagram of DAA, HMAC, CMAC. This session also describes functions of MAC.

30.6 Session Description

30.6.1MAC

MAC function accepts a variable length message and a secret key as input and produces a fixed-length MAC value as output. This MAC value serves as the authenticator.

$$MAC = MAC(K, M)$$

where M= input message

C = MAC function

K= shared secret key

MAC = message authentication code

30.6.2 Message Encryption

a. Message is encrypted by the source with the secret key using any symmetric encryption algorithm and the ciphertext is sent to destination. Destination decrypts the message with the same secret key used by the source and restores the plaintext. Confidentiality and Authentication of the message is achieved.
b. Message is encrypted by the source with public key (PU_b) of destination and the ciphertext is sent to destination. Destination decrypts the message with private key (PR_b) and restores the plaintext. Confidentiality of the message is preserved in this case.
c. Message is encrypted by the source with private key (PR_a) of source and the ciphertext is sent to destination. Destination decrypts the message with public key (PU_a) of source and restores the plaintext. Authentication and digital signature of the message are preserved in this case.
d. Message is encrypted by the source with private key (PR_a) of source and re-encrypted with public key (PU_b) of destination. The resultant ciphertext is sent to the destination. Destination decrypts the message with private key (PU_a) of source and again it decrypts with private key (PR_b) of destination there by restores the plaintext. Confidentiality, authentication and digital signature of the message are preserved in this case.

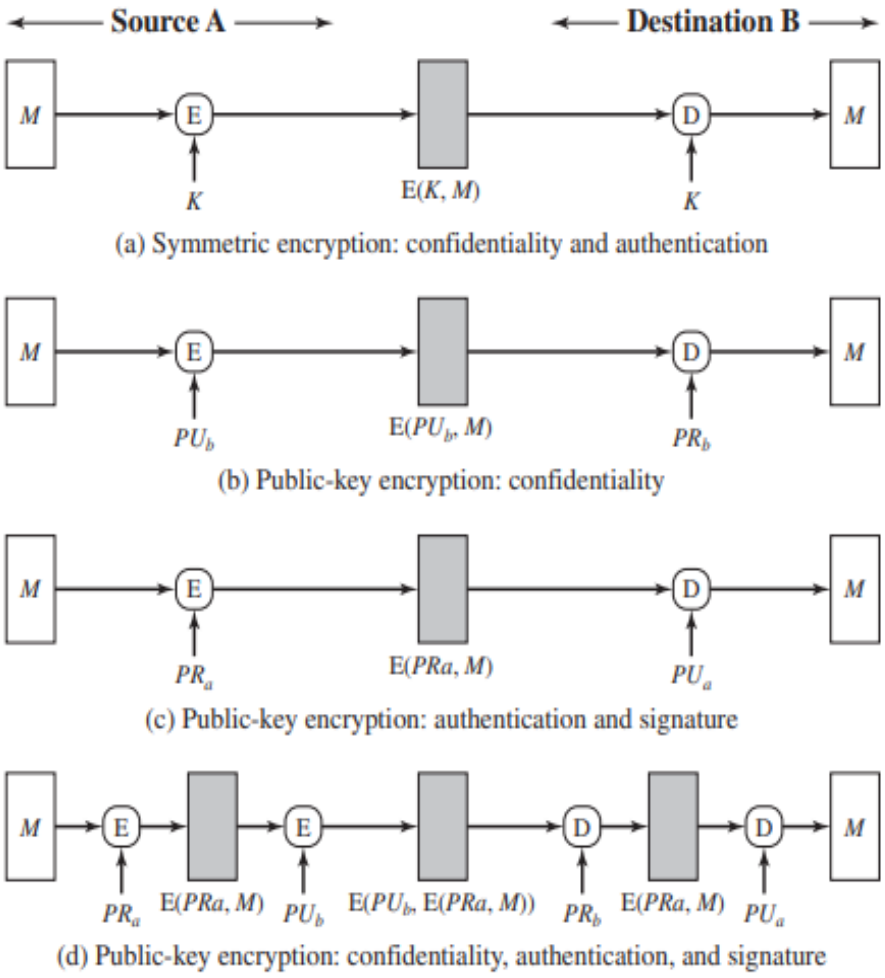


Figure 30.1. Basic Uses of Message Encryption

30.6.3 Internal & External Error Control

- **Internal Error Control**

Source calculates checksum of the message and appends to the message. Message appended with checksum is encrypted with secret key and the ciphertext is sent to the destination. Destination decrypts the ciphertext with the same key used by the source and for the received message it calculates the checksum and compares with the checksum sent by the source. If the checksum calculated by the destination is equal to the checksum sent by the source then the integrity of the message is preserved. It means that the message is received without modification.

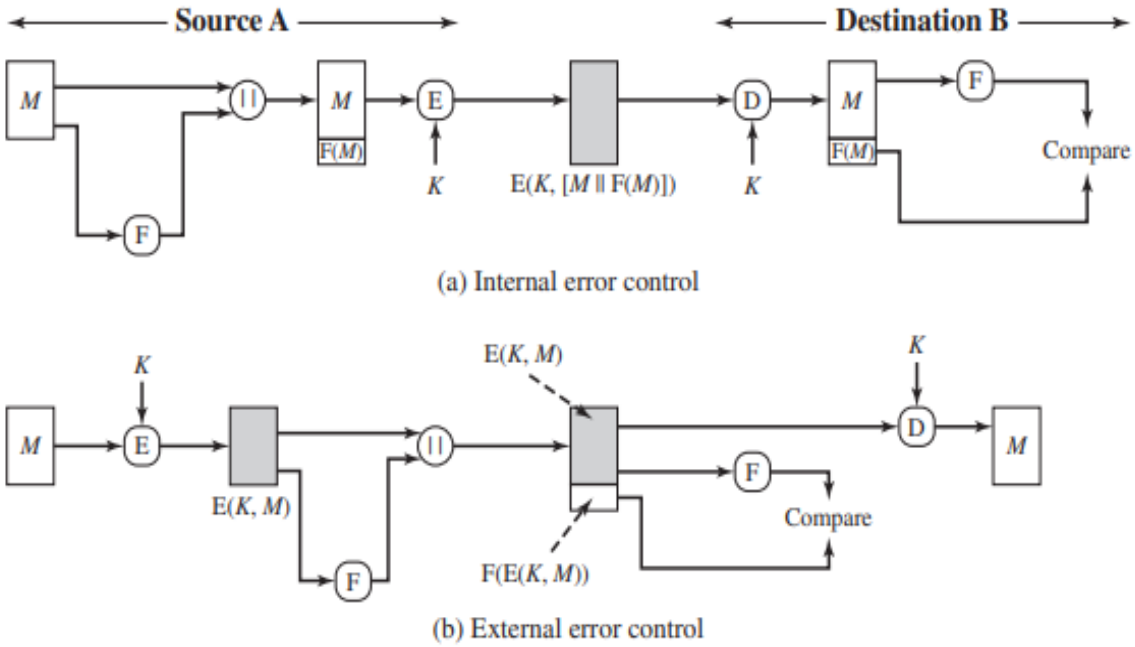


Figure 30.2. Internal Error Control & External Error Control

- **External Error Control**

Source encrypts the message with secret key and then calculates checksum .Appends checksum to the message. Destination decrypts the message with the same key used by the source and restores original message and calculates checksum for the received message. If the checksum calculated by the destination is equal to the checksum sent by the source then the integrity of the message is preserved. It means that the message is received without modification.

- **Basic Uses of MAC**

a. Source calculates MAC value of the message and appends to the message. Message appended with MAC value is sent to the destination. Destination calculates the MAC Value and compares with the MAC value sent by the source. If the MAC value calculated by the destination is equal to the MAC value sent by the source it means that message is received without modification. Message authentication is achieved in this process.

b. Source calculates MAC value of the message using key (k1) and appends MAC

to the message. Message appended with MAC value is encrypted with secret key (k2) and the ciphertext is sent to the destination. Destination decrypts the ciphertext with the same key (k2) used by the source and for the received message it calculates the MAC Value using key (k1) and compares with the MAC value sent by the source. If the MAC value calculated by the destination is equal to the MAC value MAC value sent by the source then the integrity of the message is preserved. It means that the message is received without modification. Message Authentication and confidentiality tied to plaintext is achieved in this method.

c. Source encrypts the message with secret key (k2) and then calculates MAC value using key (k1). Appends MAC value to the message. Destination decrypts the message with the same key (k2) used by the source and restores original message and calculates MAC value using key (k10 for the received message. If the MAC value calculated by the destination is equal to the MAC value sent by the source then the integrity of the message is preserved. It means that the message is received without modification. Message Authentication and confidentiality tied to ciphertext is achieved in this method.

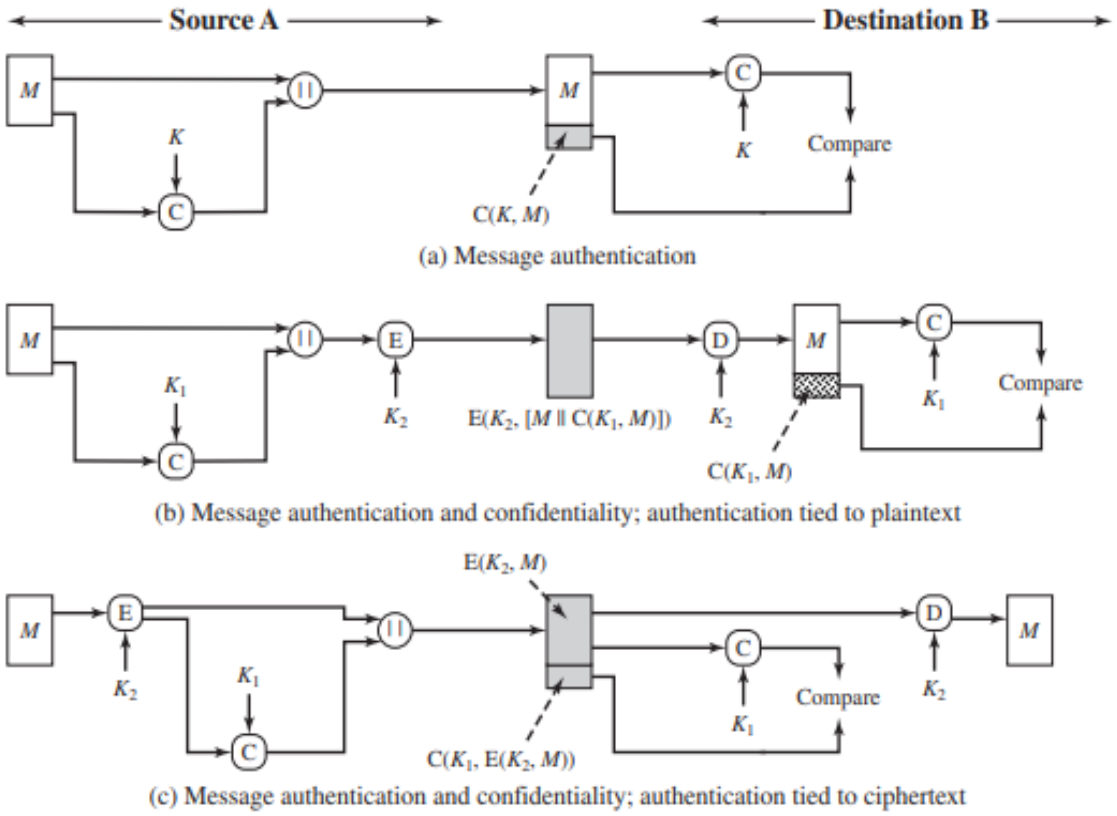


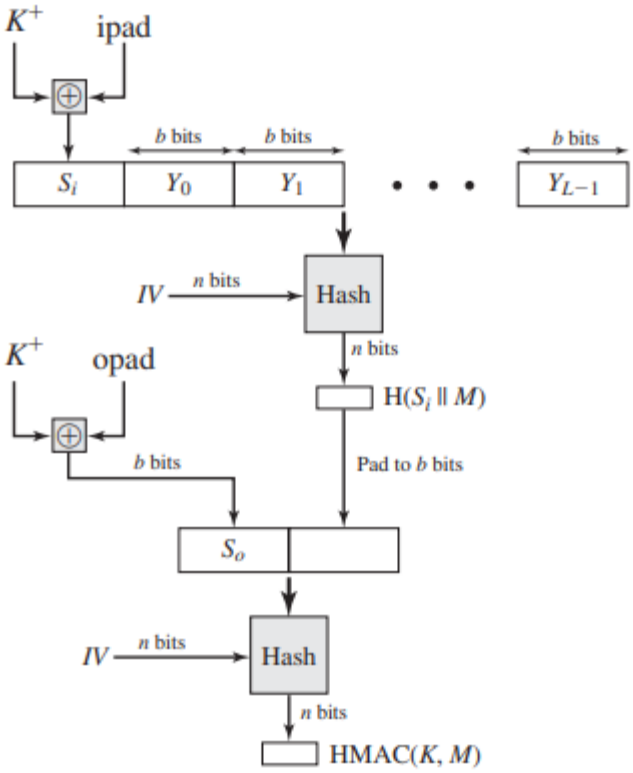
Figure 30.3. Basic Uses of MAC

- **Hash Based MAC (HMAC)**

1. Secret key K is padded with zeros on the left so that it becomes b bits in length and is called as K+.
2. Message M is divided into b bit blocks $Y_0, Y_1, \ldots Y_{n-1}$
3. 00110110 (36 in hexadecimal) is repeated b/8 times and is called as ipad.
4. XOR K+ with ipad and the resultant block is called as Si.
5. Append Message M to the Si.
6. Apply Hash Algorithm to the result of Step 5. IV is the initialization vector given as input to the Hash algorithm.
7. 01011100 (5C in hexadecimal) is repeated b/8 times and is called as opad.
8. XOR K+ with opad and the resultant block is called as So.
9. Append result of step 6 to S_0.
10. Result of step 9 is given to Hash algorithm which uses an Initialization

Vector (IV).

11. The output of step 10 is called as HMAC value for a given message M.



H = embedded hash function (e.g., MD5, SHA-1, RIPEMD-160)
IV = initial value input to hash function
M = message input to HMAC (including the padding specified in the embedded hash function)
Y_i = i th block of $M, 0 \leq i \leq (L-1)$
L = number of blocks in M
b = number of bits in a block
n = length of hash code produced by embedded hash function
K = secret key; recommended length is $\geq n$; if key length is greater than b, the key is input to the hash function to produce an n-bit key

K^+ = K padded with zeros on the left so that the result is b bits in length
ipad = 00110110 (36 in hexadecimal) repeated $b/8$ times
opad = 01011100 (5C in hexadecimal) repeated $b/8$ times

Figure 30.4. Hash based MAC (HMAC) Algorithm

➢ Data Authentication Algorithm (DAA)

Message M is divided into D blocks (D_1, D_2,…..D_N). Block size is 64 bits.

Consider first block of data (D_1) give it as input to DES algorithm for encryption. The ciphertext (O_1) thus produced which is of 64 bits acts as key to process next block of data D_2. These process continues until last block of data (D_N) is processed. The output after processing last block of data (O_N) leftmost 16 to 64 bits is treated as MAC value.

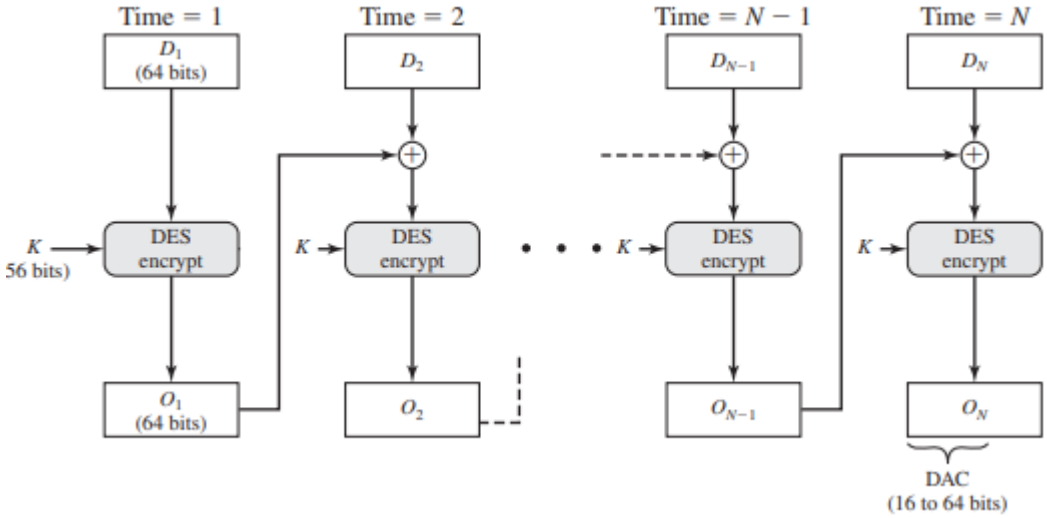


Figure 30.5. Data Authentication Algorithm (DAA) Algorithm.

- **Cipher based Message Authentication Code (CMAC)**

a. If the Message M is integer multiple of block size no need to append padding Message M is divided into blocks (M_1, M_2,…..M_n). Block size depends upon the encryption algorithm being used i.e., block size will be 64 bits if DES algorithm is used/ 128 bits if AES algorithm is used. Consider first block of data (M_1) give it as input to algorithm for encryption. The ciphertext thus produced acts as key to process next block of data M_2. This process continues until last block of data (M_n) is processed. The output after processing last block of data (M_n) leftmost 16 to 64 bits is treated as MAC value.

b. If the Message M is not an integer multiple of block size append padding bits to the right of the last block M_n in the pattern 1 followed by necessary number of 0's.

(Message M is divided into blocks (M_1, M_2,…..M_n). Block size depends upon the encryption algorithm being used i.e., block size will be 64 bits if DES algorithm is used/ 128 bits if AES algorithm is used. Consider first block of data (M_1) give it as input to algorithm for encryption. The ciphertext thus produced acts as key to process next block of data M_2. This process continues until last block of data (M_n) is processed. The output after processing last block of data (M_n) leftmost 16 to 64 bits is treated as MAC value

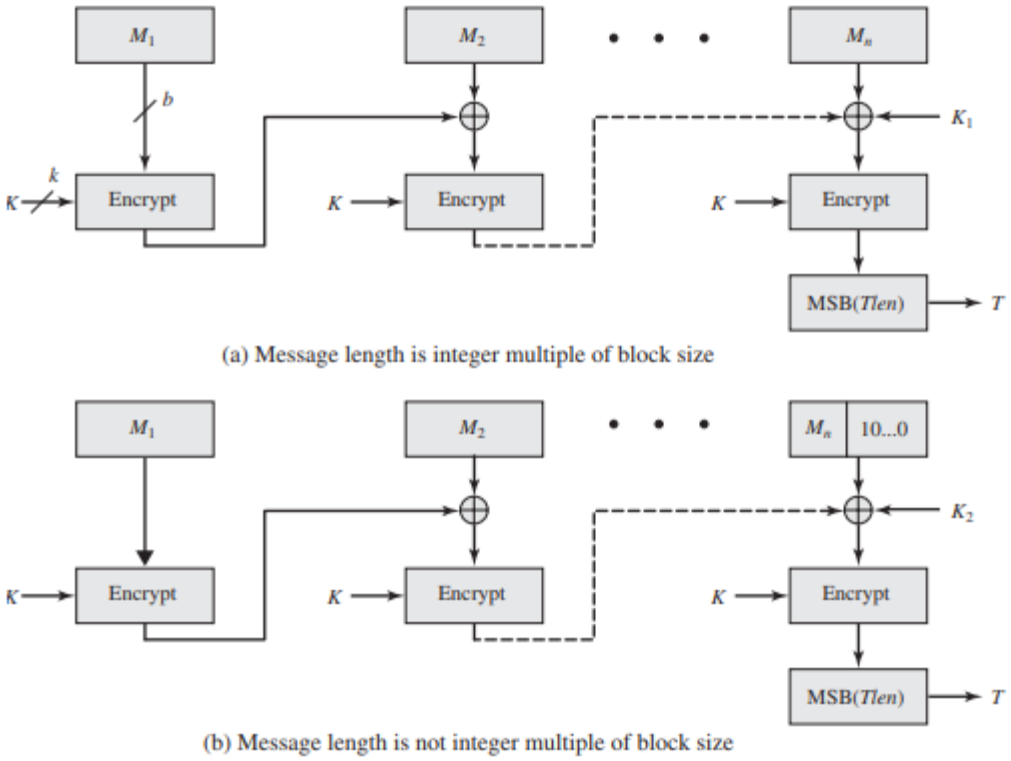


Figure 30.6. Cipher based MAC (CMAC) Algorithm.

30.7 Activities (Problem Solving): NA

30.8 Example: NA

30.9 Table Numbering: NA

30.10 Figures with captions

Figure 30.1. Basic Uses of Message Encryption

Figure 30.2. Internal Error Control & External Error Control

Figure 30.3. Basic Uses of MAC

Figure 30.4. Hash based MAC (HMAC) Algorithm

Figure 30.5. Data Authentication Algorithm (DAA) Algorithm.

Figure 30.6. Cipher based MAC (CMAC) Algorithm.

30.11 Self-Assessment Questions

1. What is the primary purpose of a Message Authentication Code (MAC) in cryptography?
   a) Encryption
   b) Message integrity and authenticity
   c) Key distribution
   d) Digital signature

2. Which of the following is NOT a commonly used MAC algorithm?
   a) HMAC
   b) RSA
   c) CBC-MAC
   d) CMAC

3. Which of the following cryptographic primitives is often used as the building block for MAC algorithms?
   a) Public key encryption
   b) One-time pad
   c) Hash functions
   d) Symmetric key encryption

4. What key is shared between the sender and receiver in a MAC algorithm?
   a) Public key
   b) Private key
   c) Secret key
   d) Session key

5. Which MAC algorithm is designed to work with block ciphers and can process messages of variable length?
   a) HMAC
   b) CBC-MAC
   c) CMAC
   d) UMAC

6. Which property ensures that given a MAC for a message, it is computationally infeasible to find a MAC for a different message using the same key?
   a) Confidentiality
   b) Authenticity
   c) Integrity
   d) Unforgeability

7. Which of the following MAC algorithms uses a double application of a block cipher with an XOR operation?
   a) HMAC
   b) CBC-MAC
   c) CMAC
   d) UMAC

8. Which type of attack attempts to find two different messages that produce the same MAC?
   a) Birthday attack
   b) Collision attack
   c) Differential attack
   d) Chosen plaintext attack

9. Which of the following MAC algorithms is based on the Merkle-Damgård construction and uses a hash function?
   a) HMAC
   b) CBC-MAC
   c) CMAC
   d) UMAC

10. Which mode of operation is commonly used with block ciphers to construct a MAC?
   a) ECB
   b) CTR
   c) OFB
   d) CBC

11. Which of the following MAC algorithms is resistant to length extension attacks?
   a) HMAC
   b) CBC-MAC
   c) CMAC
   d) UMAC

12. Which security property ensures that an adversary cannot generate a valid MAC without knowing the secret key?
   a) Unforgeability
   b) Confidentiality
   c) Integrity
   d) Authentication

13. Which MAC algorithm is widely used in combination with AES and other block ciphers?

a) HMAC
b) CBC-MAC
c) CMAC
d) UMAC

14. Which MAC algorithm is based on the use of a universal hash function family?
a) HMAC
b) CBC-MAC
c) CMAC
d) UMAC

15. Which of the following is a drawback of using a MAC compared to digital signatures?
a) Slower computation
b) Requires more storage space
c) No protection against replay attacks
d) Less secure

16. In HMAC, what is the role of the inner and outer hash keys?
a) Both keys are used in parallel for hashing the message
b) The inner key encrypts the message, and the outer key decrypts it
c) The inner key is used for encryption, and the outer key is used for decryption
d) Both keys are mixed together in a specific way during the hashing process

17. Which of the following is a commonly used hash function in HMAC?
a) MD5
b) DES
c) RSA
d) AES

18. Which MAC algorithm is more suitable for parallel processing and high-speed networks due to its efficient design?
a) HMAC
b) CBC-MAC
c) CMAC
d) UMAC

19. Which of the following is an essential requirement for the security of MAC algorithms?
a) The MAC length should be equal to the message length.
b) The hash function used should be reversible.
c) The MAC key must be kept secret.
d) The MAC algorithm should be deterministic.

20. Which of the following is NOT a typical application of MAC algorithms?
a) SSL/TLS for secure communication
b) VPN for remote access
c) Digital signatures for document signing
d) Message verification in blockchain networks

30.12 Summary

The primary purpose of using a MAC is to guarantee message integrity. It detects any unauthorized modifications to the message, including accidental or deliberate changes. Unlike encryption, MAC does not provide confidentiality; it only verifies the integrity and authenticity of the message. Algorithms include HMAC,CMAC,DAA.

30.13. Terminal Questions

1. Define MAC.
2. Demonstrate Data Authentication Algorithm (DAA) with a neat diagram.
3. Illustrate Cipher based MAC (CMAC) with a neat diagram.
4. Elucidate uses of Message Authentication Code (MAC).
5. Summarize Hash based MAC (HMAC) algorithm.

30.14 Answer Key:

Self-Assessment Questions-Answers

1. b) Message integrity and authenticity
2. b) RSA
3. c) Hash functions
4. c) Secret key
5. c) CMAC
6. d) Unforgeability
7. c) CMAC
8. b) Collision attack
9. a) HMAC
10. d) CBC
11. c) CMAC
12. a) Unforgeability
13. c) CMAC
14. d) UMAC
15. c) No protection against replay attacks
16. d) Both keys are mixed together in a specific way during the hashing process
17. a) MD5
18. d) UMAC
19. c) The MAC key must be kept secret.
20. c) Digital signatures for document signing

1. MAC function accepts a variable length message and a secret key as input and produces a fixed-length MAC value as output. This MAC value serves as the authenticator.

MAC = MAC(K, M)

where M= input message

C = MAC function

K= shared secret key

MAC = message authentication code

2.Data Authentication Algorithm (DAA)

Message M is divided into D blocks (D_1, D_2,…..D_N). Block size is 64 bits.

Consider first block of data (D_1) give it as input to DES algorithm for encryption. The ciphertext (O_1) thus produced which is of 64 bits acts as key to process next block of data D_2. These process continues until last block of data (D_N) is processed. The output after processing last block of data (O_N) leftmost 16 to 64 bits is treated as MAC value.

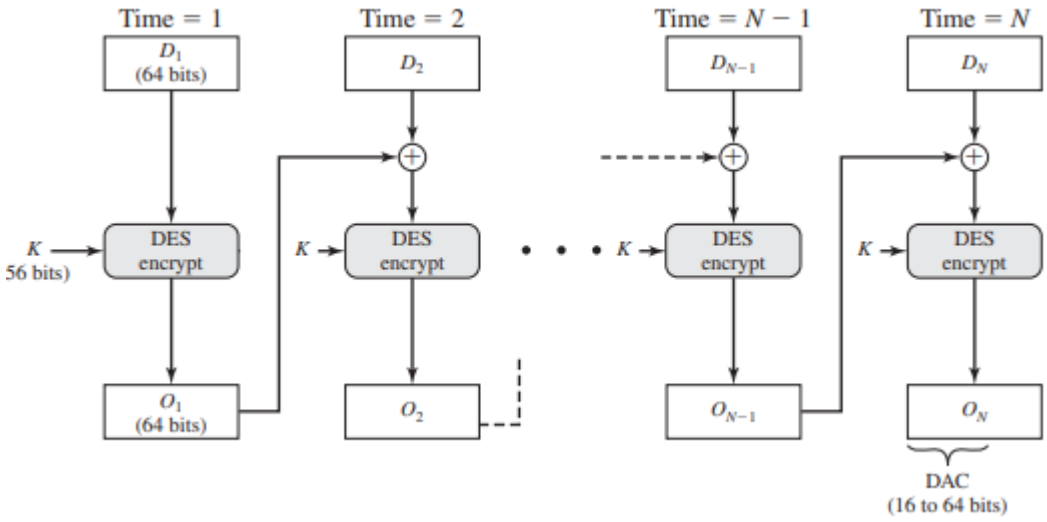


Figure Data Authentication Algorithm (DAA) Algorithm.

➢ 3. Cipher based Message Authentication Code (CMAC)

c. If the Message M is integer multiple of block size no need to append padding Message M is divided into blocks (M_1, M_2,…..M_n). Block size depends upon the encryption algorithm being used i.e., block size will be 64 bits if DES algorithm is used/ 128 bits if AES algorithm is used. Consider first block of data (M_1) give it as input to algorithm for encryption. The ciphertext thus produced acts as key to

process next block of data M_2. This process continues until last block of data (M_n) is processed. The output after processing last block of data (M_n) leftmost 16 to 64 bits is treated as MAC value.

d. If the Message M is not an integer multiple of block size append padding bits to the right of the last block M_n in the pattern 1 followed by necessary number of 0's. (Message M is divided into blocks (M_1, M_2,…..M_n). Block size depends upon the encryption algorithm being used i.e., block size will be 64 bits if DES algorithm is used/ 128 bits if AES algorithm is used. Consider first block of data (M_1) give it as input to algorithm for encryption. The ciphertext thus produced acts as key to process next block of data M_2. This process continues until last block of data (M_n) is processed. The output after processing last block of data (M_n) leftmost 16 to 64 bits is treated as MAC value

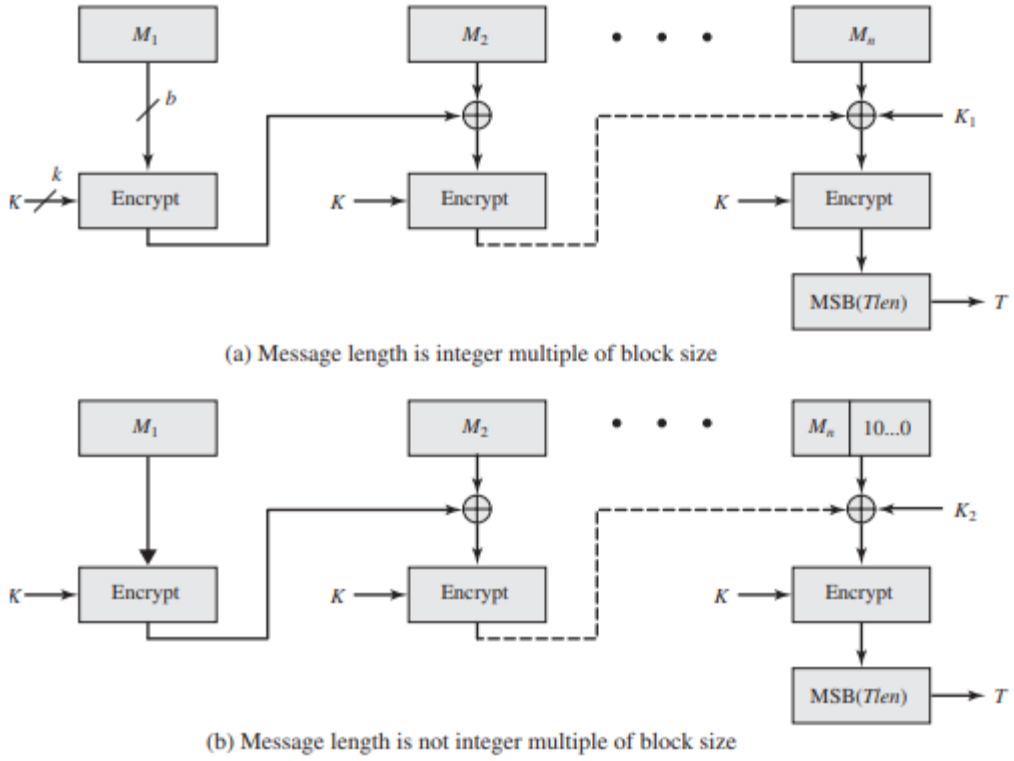


Figure Cipher based MAC (CMAC) Algorithm.

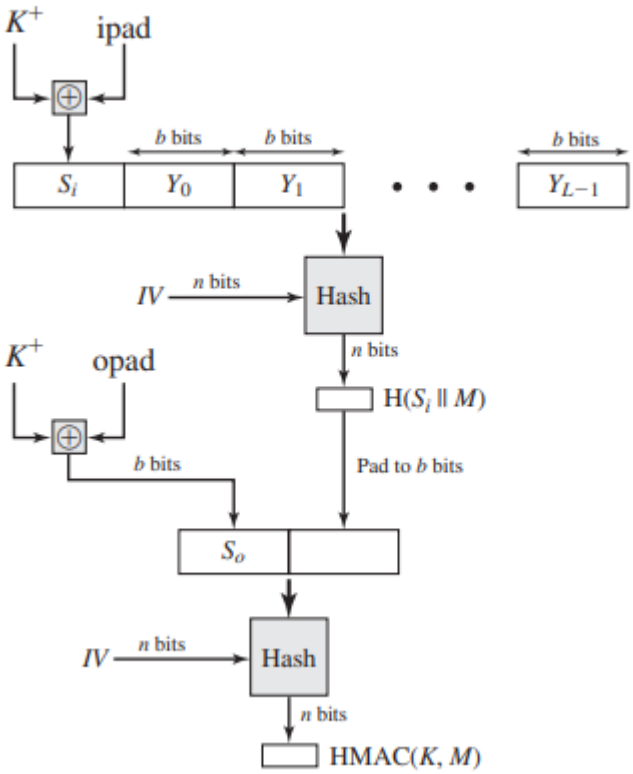
11. Basic Uses of MAC

a. Source calculates MAC value of the message and appends to the message. Message appended with MAC value is sent to the destination. Destination calculates the MAC Value and compares with the MAC value sent by the source. If the MAC value calculated by the destination is equal to the MAC value sent by the source it means that message is received without modification. Message authentication is achieved in this process.
b. Source calculates MAC value of the message using key (k1) and appends MAC to the message. Message appended with MAC value is encrypted with secret key (k2) and the ciphertext is sent to the destination. Destination decrypts the ciphertext with the same key (k2) used by the source and for the received message it calculates the MAC Value using key (k1) and compares with the MAC value sent by the source. If the MAC value calculated by the destination is equal to the MAC value MAC value sent by the source then the integrity of the message is preserved. It means that the message is received without modification. Message Authentication and confidentiality tied to plaintext is achieved in this method.
c. Source encrypts the message with secret key (k2) and then calculates MAC value using key (k1). Appends MAC value to the message. Destination decrypts the message with the same key (k2) used by the source and restores original message and calculates MAC value using key (k10 for the received message. If the MAC value calculated by the destination is equal to the MAC value sent by the source then the integrity of the message is preserved. It means that the message is received without modification. Message Authentication and confidentiality tied to ciphertext is achieved in this method.

Figure Basic Uses of MAC

12. Hash Based MAC (HMAC)

12. Secret key K is padded with zeros on the left so that it becomes b bits in length and is called as K+.
13. Message M is divided into b bit blocks $Y_0, Y_1, \ldots . Y_{n-1}$
14. 00110110 (36 in hexadecimal) is repeated b/8 times and is called as ipad.
15. XOR K+ with ipad and the resultant block is called as Si.
16. Append Message M to the Si.
17. Apply Hash Algorithm to the result of Step 5. IV is the initialization vector given as input to the Hash algorithm.
18. 01011100 (5C in hexadecimal) is repeated b/8 times and is called as opad.
19. XOR K+ with opad and the resultant block is called as So.
20. Append result of step 6 to S_0.
21. Result of step 9 is given to Hash algorithm which uses an Initialization Vector (IV).
22. The output of step 10 is called as HMAC value for a given message M.



H = embedded hash function (e.g., MD5, SHA-1, RIPEMD-160)
IV = initial value input to hash function
M = message input to HMAC (including the padding specified in the embedded hash function)
Y_i = i th block of M, $0 \leq i \leq (L-1)$
L = number of blocks in M
b = number of bits in a block
n = length of hash code produced by embedded hash function
K = secret key; recommended length is $\geq n$; if key length is greater than b, the key is input to the hash function to produce an n-bit key

K^+ = K padded with zeros on the left so that the result is b bits in length
ipad = 00110110 (36 in hexadecimal) repeated $b/8$ times
opad = 01011100 (5C in hexadecimal) repeated $b/8$ times

Figure Hash based MAC (HMAC) Algorithm

30.15 Case studies: NA

30.16 Glossary:

MAC – Message Authentication Code

30.17 References

1. Cryptography and Network Security Principles and Practice, by William stallings, Pearson, 5th edition.

2.Applied Cryptography: Protocols, Algorthms, and Source Code in C , by Bruce Schneier, Second Edition , John Wiley & Sons, Inc., 2015.

3.Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, by Hamid R. Nemati and Li Yang, IGI Global, 2011

4. Forouzon B, “Cryptography and Network Security,” Indian Edition, TMH (2010).

30.18 Keywords

MAC, Hash, HMAC,

Session-31

INCIDENT RESPONSE PROCESS

31.1 Aim

To understand incident response and the concepts of NIST Incident Response Life Cycle.

31.2 Instructional Objectives

The objective of intrusion analysis and incident response is to swiftly and accurately identify and assess security breaches, and effectively mitigate the impact by taking immediate actions to contain and resolve the incidents. NIST Incident Response Life Cycle is to provide organizations with a systematic approach to effectively respond to and manage cybersecurity incidents.

31.3 Learning Outcomes

At the end of this session, students are expected to

Analyze know the intrusion analysis and incident response.

Demonstrate NIST Incident Response Life Cycle.

31.4 Module Description

This module deals about skills in recognizing, gathering, and safeguarding digital evidence. Incident response plan is discussed in detail. Functionalities of Incident Response Team are illustrated in this module. Communication Plan and stake holder management is also discussed. Cyber Kill Chain Attack Framework is analyzed. This module also covers disaster recovery and retention policy.

31. 5 Session Introduction

In this session, we cover the Incident Response. This document will serve as a resource for understanding these topics in depth.

31.6 Session Description

Incident Response (IR)

Incident response (IR) is the steps used to prepare for, detect, contain, and recover from a data breach.

Incident response (IR) encompasses a range of actions undertaken by a business during a cybersecurity incident. In the context of IR, a cyber incident can be defined as any occurrence that jeopardizes the confidentiality, integrity, and/or availability of information, which are fundamental principles of information security often known as the "CIA triad."

The activities involved in IR are typically guided by an IR plan that aims to restore the organization's IT infrastructure swiftly while minimizing the overall impact of the incident.

The primary focus of these frameworks is to facilitate the recovery process. Moreover, they also assist organizations in developing their cyber maturity and expertise. This, in turn, aids in strengthening their defenses, preventing attacks and incidents from impacting businesses proactively.

What is an Incident Response Plan?

An incident response plan is a document that outlines an organization’s procedures, steps, and responsibilities of its incident response program.

- Incident response planning often includes the following details:
- how incident response supports the organization’s broader mission
- the organization’s approach to incident response
- activities required in each phase of incident response
- roles and responsibilities for completing IR activities
- communication pathways between the incident response team and the rest of the organization
- metrics to capture the effectiveness of its IR capabilities

It’s important to note that an IR plan’s value doesn’t end when a cyber security incident is over; it continues to provide support for successful litigation, documentation to show auditors, and historical knowledge to feed into the risk assessment process and improve the incident response process

itself.

Incident Response Steps

According to the National Institute of Standards and Technology (NIST), there are four key phases to IR:

Preparation: No organization can spin up an effective incident response on a moment's notice. A plan must be in place to both prevent and respond to events.

Detection and analysis: The second phase of IR is to determine whether an incident occurred, its severity, and its type.

Containment and eradication: The purpose of the containment phase is to halt the effects of an incident before it can cause further damage.

Post-incident recovery: A lessons learned meeting involving all relevant parties should be mandatory after a major incident and desirable after less severe incidents with the goal of improving security as a whole and incident handling in particular.

An incident response plan holds crucial significance as it addresses not only technical challenges but also the broader business implications of cyber incidents. By promptly mitigating these incidents, their potential for causing extensive harm is reduced.

Consider recent high-profile breaches that remained in the news for weeks. Was the organization notified well in advance but failed to address the issue adequately? Did their public statements downplay the severity of the incident, only to be contradicted by subsequent investigations? Were communications with affected individuals disorganized, leading to heightened confusion? Were executives accused of mishandling the incident by either not taking it seriously or exacerbating the situation, such as through stock sell-offs? These telltale signs often indicate the absence of a comprehensive plan.

An incident response plan extends beyond technical aspects and should be tailored to align with the organization's priorities and acceptable risk levels.

Incident response leaders must grasp their organization's short-term operational needs and long-term strategic objectives to minimize disruptions and mitigate data loss during and after an incident.

Moreover, the insights gained from the incident response process can inform the risk assessment and incident response processes themselves, enabling better handling of future incidents and fostering a stronger overall security posture. When confronted with inquiries from investors, shareholders, customers, the media, judges, or auditors regarding an incident, a business equipped with an incident response plan

can point to its records and demonstrate responsible and thorough actions taken in response to the attack.

NIST incident response lifecycle:

Incident response is an organization's process of reacting to IT threats such as cyberattack, security breach, and server downtime. The incident response lifecycle is your organization's step-by-step framework for identifying and reacting to a service outage or security threat.

NIST presents a four-step incident response process, as depicted in the accompanying diagram. This NIST model highlights that incident response is not a linear progression initiated upon incident detection and concluded with eradication and recovery. Instead, it is a cyclical endeavor that involves continuous learning and enhancement to enhance the organization's defensive capabilities.

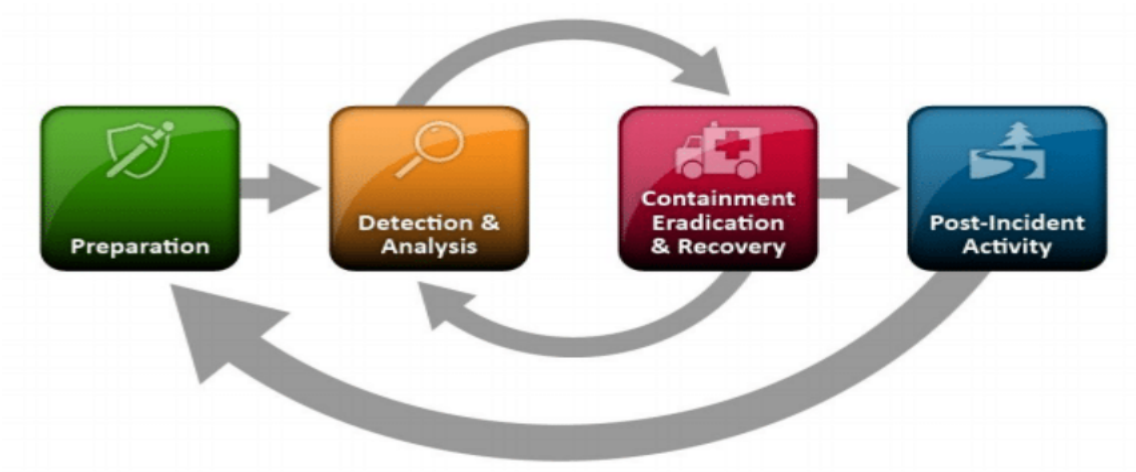


Fig 31.1: NIST Incident Response Life Cycle

Following each incident, a significant undertaking is made to document and examine the incident itself, providing valuable feedback for earlier stages and facilitating improved readiness, detection, and analysis for future incidents.

Additionally, a feedback loop exists between the containment and eradication phase and the detection and analysis phase. During the initial detection stage, numerous aspects of an attack may not be fully comprehended and are only revealed when incident responders actively engage in the investigation. These insights assist the team in enhancing their ability to detect and thoroughly analyze attacks in subsequent instances.

The Four Stages of NIST Incident Response

Preparatory Phase:

In order to be prepared for incidents, it is essential to compile a comprehensive inventory of IT assets such as networks, servers, and endpoints, assessing their significance and identifying critical systems or those containing sensitive data. Establish monitoring mechanisms to establish a baseline of normal activity and define the types of security events that warrant investigation. Develop detailed response procedures for common incident types.

Cynet 360 offers a comprehensive suite of essential capabilities for effective incident preparation, including a centralized visibility interface that provides insights into endpoint configurations, process execution, installed software, network traffic, and user activity.

Detection and Analysis Phase:

The detection stage involves gathering data from IT systems, security tools, publicly available sources, and individuals within and outside the organization to identify precursors (indications that an incident may occur in the future) and indicators (evidence of an ongoing or past attack).

Analysis entails establishing a baseline of normal activity for the affected systems, correlating related events, and identifying deviations from expected behavior.

An integrated security platform like Cynet 360 can automate these tasks by identifying behavioral baselines, detecting anomalies that indicate suspicious behavior, and collecting relevant data across networks, endpoints, and user activities to facilitate thorough investigations.

Discover more about the detection capabilities of Cynet 360, which covers a wide range of attack vectors through its natively integrated EDR (Endpoint Detection and Response), user behavior rules, network detection rules, and deception modules.

Containment, Eradication, and Recovery:

The objective of containment is to halt the attack before it causes significant damage or exhausts resources. Your containment strategy will depend on the potential impact of the incident, the need to maintain critical services for employees and customers, and the duration of the solution—whether it's a temporary measure for a few hours, days, or weeks, or a permanent resolution.

As part of containment, it is crucial to identify the source of the attack and verify its IP address. This enables you to block communication from the attacker and gain

insights into their modus operandi, as well as search for and block any other communication channels they might be utilizing.

Cynet 360 can assist in implementing remote manual actions for containment during security incidents, such as terminating malicious processes, deleting files, resetting passwords, and restarting affected devices. Additionally, it can perform automatic containment actions like halting rapid file encryption or automatically isolating endpoints infected with malware from the network.

Cynet's response orchestration capabilities empower organizations to eliminate attackers' presence and activities across various components of the environment, including infected hosts, malicious files, compromised user accounts, and attacker-controlled traffic. Discover more about Cynet 360's incident containment capabilities.

During the eradication and recovery phase, once the incident has been effectively contained, efforts should be directed towards eliminating all remnants of the incident from the environment. This may involve identifying all affected hosts, removing malware, and securing breached user accounts through password resets or closures.

Post-Incident Activity:

An integral part of the NIST incident response methodology involves learning from past incidents to enhance the overall process.

31.7 Activities: NA

31.8 Example: NA

31.9 Table Numbering: NA

31.10 Figures with Captions

Fig 31.1: NIST Incident Response Life Cycle

31.11 Self-Assessment Questions

- Define incident response.
- Write the purpose of incident response plan.
- List out the various stages in NIST Incident Response Life Cycle.
- Write the purpose of NIST Incident Response Life Cycle?

31.12 Summary

The NIST Incident Response Life Cycle is a structured framework that guides organizations in effectively responding to security incidents. It consists of a series of defined procedures and stages that provide a systematic workflow for incident

response. The life cycle encompasses preparation, detection, containment, eradication, recovery, and post-incident activities. By following this comprehensive approach, organizations can mitigate the impact of incidents, restore normal operations, and continuously improve their incident response capabilities.

31.13 Terminal Questions

- Write short notes on incident response.
- Explain in detail about NIST Incident Response Life Cycle.

31.14 Case Study: NA.

31.15 Answer Key:

Incident response (IR) is the steps used to prepare for, detect, contain, and recover from a data breach.

NIST Incident Response Life Cycle

- Preparatory Phase
- Detection and Analysis Phase
- Containment, Eradication, and Recovery
- Post-Incident Activity

31.16 Glossary

Intrusion analysis, also known as intrusion detection and analysis, is the process of identifying, analyzing, and responding to unauthorized or malicious activities within computer systems, networks, or digital environments.

Incident response (IR) is the steps used to prepare for, detect, contain, and recover from a data breach.

31.17 Reference

1. Boddington, Richard. Practical digital forensics. Packt Publishing Ltd, 2016.
2. Årnes, André, ed. Digital forensics. John Wiley & Sons, 2017.
3. Incident response: https://www.ibm.com/topics/incident-response

31.18 Keywords

Incident response, intrusion analysis, Diamond model of intrusion analysis, NIST Incident Response Life Cycle

SESSION: 32

INTRODUCTION TO INCIDENT RESPONSE PROCESS

32.1 Aim

To familiarize students with the basic concepts of incident response process, cyber incident response team.

32.2 Instructional Objectives

The objective of this session is to introduce the understanding of incidence response, explore incident response lifecycle, defining a cyber incident response team, creating a CIRT.

32.3 Learning Outcomes

At the end of this session, students are expected to know

Recall Incident Response

Summarize a Cyber Incident Response Team

32.4 Module Description

This module deals about skills in recognizing, gathering, and safeguarding digital evidence. Incident response plan is discussed in detail. Functionalities of Incident Response Team are illustrated in this module. Communication Plan and stake holder management is also discussed. Cyber Kill Chain Attack Framework is analyzed. This module also covers disaster recovery and retention policy

32.5 Session Introduction

The incident response procedure is not ad hoc, according to an analysis. An organization won't be able to determine the severity of the incident or be able to halt the bleeding in time to minimize harm if its processes or procedures are unclear. Understanding the incident response procedure is merely the beginning of a competence that must be developed within an organization.

32.6 Session Description

Incident Response Process: Each incident begins when the organization first learns

about a single occurrence or a chain of connected incidents that point to malicious behavior. This discovery may take the form of an external entity notifying the organization of a potential security issue or a security control alert.

Six unique phases make up the incident response process, each of which comprises a list of steps the organization might take to resolve the issue:

1. **Planning:** Without sound planning, any subsequent response to the crisis would be disorganized and may even make matters worse. The development of an event response plan is among the crucial aspects of preparation.
2. **Detection**: Finding possible occurrences is a difficult task. The number of distinct events that occur each day may exceed 100 million, depending on the size of the organization. Analysts are overloaded with data and must then separate the valuable pieces of signal from the large amount of network noise as a result of this mountain of events and other security controls that are continually alerting to activity. If Security Incident and Event Management (SIEM) solutions are not properly maintained with regular changes of rule sets that identify what events classify as a potential incident, even the most cutting-edge SIEM tools today lose their usefulness.
3. **Analysis:** After an incident has been found, organization personnel or a reliable outside party will start the analysis phase. During this stage, workers start gathering data from systems such running software processes, log files, network connections, and running memory. The time required for this gathering can range from a few hours to many days, depending on the kind of incident. The evidence must then be analyzed after it has been gathered.

32.7 Activities

The term "incident response process" refers to a series of predetermined actions and guidelines that an organization uses to identify, address, and resolve security events. It strives to reduce the harm brought on by incidents and swiftly resume normal activities.

Incident Types: A wide range of incidents are covered by the incident response process, including but not limited to insider threats, data breaches, network intrusions, malware infections, system failures, and natural disasters.

Phases: Depending on the organization, the process often consists of a number of

phases. Preparation, identification, confinement, eradication, recovery, and lessons gained are among the well recognized processes.

CSIRT Analyst: A CSIRT Analyst is a member of staff who performs CSIRT-related duties but has little exposure to or practical knowledge of incident response processes. They frequently only have one or two years of experience reacting to situations. They can thus carry out a variety of tasks, some of which are directed by senior analysts.
Analysts will train and practise to improve their skills as part of preparation phase activities. They might also participate in the incident response plan's evaluation and revision. They will be charged with obtaining proof during an incident from hosts that may have been compromised, from network equipment, or from numerous log sources. Assisting other team members in the remediation process, analysts will also participate in the examination of the evidence.

32.8 Example

Let's consider a scenario involving a cyber security breach in a company's network to give a specific illustration of the incident response process. The organization could take the following actions in response to the incident:
Preparation: An incident response team made up of officials from IT, security, legal, and management has already been established by the organization.
They have created an incident response plan that describes the tasks assigned to team members as well as the procedures to be followed in the event of an occurrence.
Identification: An alert is produced by the organization's intrusion detection system warning of suspected network activity. After receiving the warning, the incident response team starts their investigation.
Containment: In order to stop the breach from spreading further, the team swiftly isolates the vulnerable systems from the network. To prevent unauthorized access and disable compromised user accounts, they employ firewall restrictions.
Eradication: The team investigates the breach's cause by examining its type and scope. They learn that an employee's account was improperly accessed by using a phishing email. They alter passwords, delete the phishing email from the afflicted account, and scan the compromised system for malware.
Recovery: The team rebuilds the impacted systems from fresh backups in order to

restore them. They guarantee that all required security patches and updates are installed, and they check the reliability of the recovered systems. As they gradually reactivate the systems, they keep an eye out for any more evidence of compromise.

32.9 Table Numbering: NA

32.10 Figures with Captions: NA

32.11 Self Assessment Questions

1. Do I understand my part in the incident response plan for the company?
2. Do I understand how to spot the warning signals of a possible security incident?
3. Do I know about the equipment and procedures in place to identify and notify of security incidents?

32.12 Summary

In conclusion, organizations must adhere to the Incident Response Process as a critical foundation for managing and mitigating security issues. Eradication entails locating the source of the problem, getting rid of risks, and repairing damaged systems. The goal of recovery is to get afflicted systems back to regular operation. The lessons learned phase also includes revising incident response strategies and analyzing incidents to find areas for improvement. It is crucial to remember that the Incident Response Process' implementation and specifics can change depending on the organizational needs and incident characteristics. However, the procedure offers a well-organized method that may be modified and tailored to meet unique requirements.

32.13 Terminal Questions

1. Can I help with efforts to restore the system and recover lost data?
2. Have I actively participated in the analysis and conversations following the incident?
3. Have I spotted any weaknesses in the incident response procedure?

32.14 Answer Key:

Self Assessment Questions:

1. Knowing your role in the incident response plan is essential to ensure that

emergencies are handled effectively inside your organisation. Understanding your part in the reaction helps to minimise the effects of incidents through a coordinated effort. Your comprehension should cover a number of important points.

Start by becoming familiar with the incident response plan's overarching goals and structure. This includes being aware of the principal stakeholders, the functioning of the communication channels, and the appropriate course of action in certain situations.

Next, specify your precise roles and responsibilities during an occurrence. This could entail doing things like alerting the appropriate people, acquiring data, carrying out instructions, or supporting the recovery process.

Furthermore, it's critical to comprehend the chain of command and escalation procedures. Knowing when and how to escalate problems to higher-ups ensures that decisions are made quickly and that resources are allocated properly.

Maintaining your comprehension and improving your talents require regular training and practise. You will internalise the plan and strengthen your response skills by actively taking part in these exercises.

In conclusion, having a solid understanding of your role in the incident response plan will enable you to carry out your duties successfully and contribute to a coordinated and effective response to any incidents that may occur inside your firm.

2. Maintaining the security of your business requires knowing how to recognise the warning signs of a potential security problem. You can take proactive steps to stop or lessen potential hazards by identifying these indicators. This entails remaining knowledgeable about typical security flaws, keeping an eye out for strange behaviour or trends, and watching network activity for anomalies. Your capacity to see warning signs and respond appropriately to protect your company's assets and data can be improved with regular security awareness

training and keeping up with new threats and attack methods.

Terminal Questions

1. Yes, your help will be extremely helpful in our efforts to repair the system and retrieve lost data. You can participate in different ways depending on your position and area of specialisation. This could entail consulting with pertinent stakeholders to design recovery strategies, offering technical support, helping with data recovery operations, or closely interacting with IT teams to address problems. You may speed up the restoration process, reduce downtime, and improve the possibility of successfully recovering any lost data by providing your skills, knowledge, and support throughout these efforts.
2. In order to learn from an incident and enhance future incident response tactics, active engagement in the analysis and discussions that follow the incident is essential. You can assist in determining the causes of an incident, its vulnerabilities, and any gaps in the incident response plan by actively participating in discussions, offering your observations and thoughts, and contributing to the analysis process. Your involvement can encourage knowledge exchange, teamwork, and the creation of efficient corrective actions. By actively taking part, you show that you are dedicated to ongoing improvement and help your firm develop a stronger and more durable security posture.

32.15 Case Study: NA

32.16 Glossary: NA

32.17 References

1. Boddington, Richard. Practical digital forensics. Packt Publishing Ltd, 2016.
2. Årnes, André, ed. Digital forensics. John Wiley & Sons, 2017.
3. Incident response: https://www.ibm.com/topics/incident-response

32.18 Keywords

Incident Response, CIRT

SESSION: 33

COMMUNICATION PLAN & STAKEHOLDER MANAGEMENT

33.1 Aim

To familiarize students with the basic concepts of cyber incident response team and plan for communication and managing stakeholders.

33.2 Instructional Objectives

The objective of this session is to introduce incidence response, explore incident response lifecycle, defining a cyber-incident response team, creating a CIRT, creating a communication strategy, Creating Effective Communication, and coordinating other Communication.

33.3 Learning Outcomes

At the end of this session, students are expected to know

Analyze Communication Plan and Stake holder management

33.4 Module Description

This module deals about skills in recognizing, gathering, and safeguarding digital evidence. Incident response plan is discussed in detail. Functionalities of Incident Response Team are illustrated in this module. Communication Plan and stake holder management is also discussed. Cyber Kill Chain Attack Framework is analyzed. This module also covers disaster recovery and retention policy.

33.5 Session Introduction

The incident response procedure is not ad hoc, according to an analysis. An organization won't be able to determine the severity of the incident or be able to halt the bleeding in time to minimize harm if its processes or procedures are unclear. Understanding the incident response procedure is merely the beginning of a competence that must be developed within an organization. What is required is a framework that uses the resources already at the disposal of the organization to implement that procedure.

The incident response plan must now be created after the incident response charter has been prepared and the CSIRT has been established. Cyber attacks have grown to be a serious threat to businesses of all sizes and in all sectors in today's networked society. Understanding the lifecycle of a cyber assault and the processes attackers take to penetrate systems and steal data is essential for successfully combating these threats.

33.6 Session Description

Incident Response Process: Each incident begins when the organisation first learns about a single occurrence or a chain of connected incidents that point to malicious behavior. This discovery may take the form of an external entity notifying the organization of a potential security issue or a security control alert.

Six unique phases make up the incident response process, each of which comprises a list of steps the organization might take to resolve the issue:

1. Containment: Organizations can enter the containment phase after having a thorough understanding of the incident and the systems involved. Organizations implement efforts to restrict threat actors' capacity to continue compromising other network resources, interacting with command and control infrastructures, or leaking sensitive data during this phase.

2. Eradication and recovery: The organization expels the threat actor from the affected network during the eradication phase. The company may use an improved anti-malware program in the event of a malware infection. Sometimes it's necessary to erase and reimage infected computers. Changing or deleting compromised user accounts is another action. Vendor patches or software upgrades are applied when a vulnerability that was exploited by an organization is discovered.

3. Post-incident activity: A thorough analysis of the incident is conducted with all the key stakeholders at the conclusion of the incident procedure. An exhaustive review of all the actions taken during the incident is a part of post-incident activity. Discussions should include both what succeeded and, more significantly, what failed.

Communication Plan and Managing Stakeholders: Network architect or administrator: Network infrastructure is frequently a factor in occurrences. This covers assaults on switches, routers, and other pieces of hardware and software used in networks. It is essential for the Network Architect or Administrator to have insight into

the typical and unusual behavior of these devices as well as the ability to spot unusual network traffic.

Server Administrator: Systems on a network that store sensitive or important data are frequently targeted by threat actors. Frequently, these high-value targets are file servers, database servers, or domain controllers.

Application support: Threat actors frequently target web apps. Some security lapses are caused by coding errors that enable for attacks like SQL injection or by incorrect security configurations.

Desktop support: People who work in desktop support are frequently involved in keeping measures like data loss prevention and antivirus on desktop systems up to date. They can aid in supplying log files and other evidence to the CSIRT in the event of an incident. During the incident's remediation phase, they can also be in charge of clearing out affected systems.

33.7 Activities

Analysts will train and practice to improve their skills as part of preparation phase activities. They might also participate in the incident response plan's evaluation and revision. They will be charged with obtaining proof during an incident from hosts that may have been compromised, from network equipment, or from numerous log sources. Assisting other team members in the remediation process, analysts will also participate in the examination of the evidence.

Human resources: Employees or contractors are often the ones who commit crimes against businesses. The CSIRT may need to conduct investigations on behaviours ranging from fraud to significant data theft. The human resources division can help to make sure that the CSIRT's actions are in line with relevant labour laws and corporate regulations if the subject of the inquiry is an employee or contractor. The CSIRT can work with human resources staff to ensure that all necessary documentation of the incident is finished before an employee or contractor is let go, lowering the risk of a wrongful termination lawsuit.

33.8 Example

Let's consider a scenario involving a cyber security breach in a company's network to give a specific illustration of the incident response process. The organization could

take the following actions in response to the incident:

Eradication: The team investigates the breach's cause by examining its type and scope. They learn that an employee's account was improperly accessed by using a phishing email. They alter passwords, delete the phishing email from the afflicted account, and scan the compromised system for malware.

Recovery: The team rebuilds the impacted systems from fresh backups in order to restore them. They guarantee that all required security patches and updates are installed, and they check the reliability of the recovered systems. As they gradually reactivate the systems, they keep an eye out for any more evidence of compromise.

Reporting incidents and escalating them:

Specify the procedure in detail for informing the designated incident response team about incidents. Establish escalation protocols to guarantee that problems are promptly handled according to their seriousness. responsibilities and roles:

Decide on and assign each member of the incident response team their specific tasks and responsibilities. Establish the team's command structure and channels for communication.

Protocols for communication:

Establish communication guidelines for management, IT teams, legal departments, and external partners, among other stakeholders, both internally and externally. Provide details regarding the channels and timing of communication during incident response efforts.

Incident Classification and Levels of Severity:

Create a method for classifying situations according to their importance, seriousness, and immediacy. To order event response efforts and resource allocation, define severity levels.

33.9 Table Numbering: NA

33.10 Figures with Captions: NA

33.11 Self Assessment Questions

1. Do I understand my part in the incident response plan for the company?
2. Do I understand how to spot the warning signals of a possible security incident?
3. Do I know about the equipment and procedures in place to identify and notify of security incidents?

33.12 Summary

In conclusion, organizations must adhere to the Incident Response Process as a critical foundation for managing and mitigating security issues. Eradication entails locating the source of the problem, getting rid of risks, and repairing damaged systems. The goal of recovery is to get afflicted systems back to regular operation. The lessons learned phase also includes revising incident response strategies and analyzing incidents to find areas for improvement. It is crucial to remember that the Incident Response Process' implementation and specifics can change depending on the organizational needs and incident characteristics. However, the procedure offers a well-organized method that may be modified and tailored to meet unique requirements.

33.13 Terminal Questions

1. Can I help with efforts to restore the system and recover lost data?
2. Have I actively participated in the analysis and conversations following the incident?
3. Have I spotted any weaknesses in the incident response procedure?

33.14 Answer Key:

Self Assessment Questions:

3. Maintaining the security of your business requires knowing how to recognise the warning signs of a potential security problem. You can take proactive steps to stop or lessen potential hazards by identifying these indicators. This entails remaining knowledgeable about typical security flaws, keeping an eye out for strange behaviour or trends, and watching network activity for anomalies. Your capacity to see warning signs and respond appropriately to protect your company's assets and data can be improved with regular security awareness training and keeping up with new threats and attack methods.
4. Maintaining a strong security posture requires being familiar with the tools and processes used to detect and notify security incidents. Learn about the security tools used by your organisation, such as firewalls, intrusion detection systems, and antivirus software. Recognise how these tools operate and how to understand any alerts or messages they may send. Learn about the incident

reporting and escalation processes that your firm has implemented. Knowing who to alert, what details to share, and the proper methods or procedures for reporting issues are all part of this. You will be well-informed and ready to use the tools and adhere to the protocols required to properly identify and notify security incidents if you receive regular training and updates on security measures.

Terminal Questions:

1. Yes, your help will be extremely helpful in our efforts to repair the system and retrieve lost data. You can participate in different ways depending on your position and area of specialisation. This could entail consulting with pertinent stakeholders to design recovery strategies, offering technical support, helping with data recovery operations, or closely interacting with IT teams to address problems. You may speed up the restoration process, reduce downtime, and improve the possibility of successfully recovering any lost data by providing your skills, knowledge, and support throughout these efforts.
2. In order to learn from an incident and enhance future incident response tactics, active engagement in the analysis and discussions that follow the incident is essential. You can assist in determining the causes of an incident, its vulnerabilities, and any gaps in the incident response plan by actively participating in discussions, offering your observations and thoughts, and contributing to the analysis process. Your involvement can encourage knowledge exchange, teamwork, and the creation of efficient corrective actions. By actively taking part, you show that you are dedicated to ongoing improvement and help your firm develop a stronger and more durable security posture.
3. Yes, I've found a few flaws in the incident response process. I have found areas that could use improvement after evaluating the present practises. These include a lack of clear roles and duties, a lack of communication gaps, poor documentation, and slow escalation procedures. I think fixing these issues will improve the effectiveness and efficiency of our incident response initiatives. I am ready to offer thorough criticism and recommendations to improve the incident response process and aid in reducing future risks.

33.15 Case Study: NA

33.16 Glossary: NA

33.17 References

1. Boddington, Richard. Practical digital forensics. Packt Publishing Ltd, 2016.
2. Årnes, André, ed. Digital forensics. John Wiley & Sons, 2017.
3. Incident response: https://www.ibm.com/topics/incident-response

33.18 Keywords

Eradication, Recovery, Communication and Collaboration, Post-Incident Analysis.

Session 34

CYBER KILL CHAIN FRAMEWORK

34.1 Aim

To understand the concepts of attack attribution and Cyber Kill Chain attacks.

34.2 Instructional Objectives

The objective of this session to provide a schematic and generic description of the nexus attribution in cyber attacks. Cyber kill chain are the two broad terms to address cyber attacks against an organisation. Cyber Kill Chain with its seven phases, addresses the cyber attack process from a high level.

34.3 Learning Outcomes:

At the end of this session, students are expected to know the attack attribution and Cyber Kill Chain attacks.

34.4 Module Description

This module deals about skills in recognizing, gathering, and safeguarding digital evidence. Incident response plan is discussed in detail. Functionalities of Incident Response Team are illustrated in this module. Communication Plan and stake holder management is also discussed. Cyber Kill Chain Attack Framework is analyzed. This module also covers disaster recovery and retention policy

34.5 Session Introduction

This session aims to provide a schematic and generic description of the nexus between attribution and characterization in cyber attacks.

34.6 Session Description

Attack attribution:

Attack attribution in the context of cyber security refers to the process of identifying and assigning responsibility for a cyber attack or intrusion to a specific individual, group, organization, or nation-state. It involves investigating and analysing various pieces of evidence to gather intelligence and make informed assessments about the identity of the attacker.

The primary goal of attack attribution is to determine who is behind the attack and understand their motivations, capabilities, and intentions. This information is crucial for developing appropriate response strategies, implementing necessary security measures, and potentially taking legal or diplomatic actions against the responsible parties.

The process of attack attribution involves multiple steps and relies on a combination of technical, intelligence, and investigative techniques. Here are some key aspects involved in attack attribution:

Evidence Collection: Gathering relevant evidence is the first step in the attribution process. This can include analysing network logs, system logs, malware samples, intrusion detection system alerts, IP addresses, domain names, and any other digital artefacts associated with the attack.

Forensic Analysis: Conducting in-depth forensic analysis helps in understanding the attack vectors, techniques, and tools used by the attacker. This may involve reverse engineering malware, analysing network traffic, examining system artifacts, and reconstructing the attack timeline.

Attribution Indicators: Identifying attribution indicators involves looking for patterns, signatures, or characteristics that can link the attack to a specific individual, group, or known threat actor. This can include TTPs (Tactics, Techniques, and Procedures) used in previous attacks, known affiliations, infrastructure overlaps, language or cultural clues, and geopolitical context.

Intelligence Gathering: Collaborating with intelligence agencies, cyber security firms, and other industry partners to gather additional intelligence on threat actors can provide valuable insights for attribution. This may involve sharing information, analysing threat intelligence reports, and leveraging specialized tools and resources.
Contextual Analysis: Understanding the context surrounding the attack is crucial for attribution. This involves considering geopolitical factors, historical relationships, ongoing conflicts, and motivations that could influence the behaviour of potential threat actors.
Corroborative Sources: Cross-referencing and validating findings with multiple sources of information and intelligence helps ensure the accuracy and reliability of the attribution assessment. This can include corroborating evidence from different organizations, government agencies, open-source intelligence, and expert opinions.
It's important to note that attack attribution is a challenging and complex process. Determining attribution with absolute certainty is often difficult due to the ability of attackers to obfuscate their tracks and employ various techniques to mislead investigators. As a result, attribution assessments are often presented as a range of possibilities or confidence levels, based on the available evidence and the expertise of the investigators.
Ultimately, the goal of attack attribution is to provide actionable intelligence that enables organizations to better defend against future attacks, mitigate risks, and respond effectively to cyber threats.

Cyber Kill Chain

The "cyber kill chain" refers to a series of stages that an attacker must go through to breach a network and extract data. Each stage represents a distinct objective in the attacker's progression. Implementing a monitoring and response strategy based on the cyber kill chain model proves effective as it centres on understanding the actual progression of attacks.
The stages of an attack, following the cyber kill chain model, are as follows:

Reconnaissance:

Gathering information about the target, such as through social media, email addresses, and intellectual property.

Weaponization:

Combining a trojan with an exploitable application, typically in the form of weaponized deliverables like Adobe PDF or MS Office documents.

Delivery

Transporting the weapon to the target environment, often through email attachments, USB removable media, or compromised websites.

Exploitation:

Activating the intruder's code, which may auto-execute by exploiting vulnerabilities in the operating system or applications.

Installation/Spread

Establishing a backdoor or trojan for persistence, while remaining hidden from security devices.

Command & Control

Setting up channels for sending and receiving information between the attacker and the compromised system.

Accomplish Mission

Carrying out the intended goals of the attack, which may involve theft of money, theft of intellectual property, or destruction of data.

Exfiltration

Collecting, encrypting, and extracting information from the target system, often with the objective of using it to compromise other machines.

Defensible Actions

- Detect: verify that some attacker is looking around
- Deny: prevent the attacker from gaining information
- Disrupt: stop or change outbound traffic (to attacker)
- Degrade: attack attacker's command & control
- Deceive: interfere with command & control
- Contain: network segmentation changes

Attack Patterns

Indicators: any piece of information that describes an intrusion Atomic: ip addresses, email addresses, vulnerability identifiers Computed: derived from data collected during an incident.

Behavioural: collections of atomic and computed indicators

34.7 Activities

34.8 Example

34.9 Table Numbering; NA

34.10 Figures with captions: NA

34.11 Self Assessment Questions

- How the MITRE ATT&CK Framework used in financial industry?
- What are the stages available in the cyber kill chain model?
- Compare MITRE ATT&CK and cyber kill chain?
- Mention the Attack Levels in MITRE ATT?

34.12 Summary

The MITRE ATT&CK Framework and the Cyber Kill Chain provide valuable insights into the lifecycle of cyberattacks. The MITRE ATT&CK Framework offers a comprehensive catalog of adversary techniques and tactics, enabling organizations to better understand and defend against threats. On the other hand, the Cyber Kill Chain outlines the stages an attacker typically goes through to infiltrate a network.

34.13 Terminal Questions

- Compare the MITRE ATT&CK Framework and Cyber Kill Chain.
- Illustrate the various attack levels in MITRE ATT&CK Framework.
- Explain the in cyber kill chain model.

34.14 Answer key:

MITRE ATT&CK Framework: It provides a comprehensive catalog of adversary tactics, techniques, and procedures (TTPs).

The Cyber Kill Chain: It outlines the sequential stages of an attack, from reconnaissance to accomplishing the mission.

Attack Levels in MITRE ATT

- *Tactics*
- *Techniques*
- *Sub-techniques*
- *Procedures*

The stages of an attack in cyber kill chain model, are as follows:

- *Reconnaissance*
- *Weaponization*
- *Delivery*

- *Installation/Spread*
- *Command & Control*
- *Accomplish Mission*
- *Exfiltration*

Glossary:

- Attack attribution in the context of cybersecurity refers to the process of identifying and assigning responsibility for a cyber attack or intrusion to a specific individual, group, organization, or nation-state.
- MITRE ATT&CK Framework: It provides a comprehensive catalog of adversary tactics, techniques, and procedures (TTPs).
- The Cyber Kill Chain: It outlines the sequential stages of an attack, from reconnaissance to accomplishing the mission.

34.15 Case Study: NA

34.16 Glossary

34.17 Reference Books

1. Boddington, Richard. Practical digital forensics. Packt Publishing Ltd, 2016.

2. Årnes, André, ed. Digital forensics. John Wiley & Sons, 2017.

Sites and Web links:

MITRE ATT&CK Frameworkvs The Cyber Kill Chain: https://www.xcitium.com/cyber-kill-chain-vs-mitre-att&ck/

Attribution: https://carnegieendowment.org/2022/03/28/attribution-and-characterization-of-cyber-attacks-pub-86698

34.18 Keywords

Cyber Kill Chain Framework

SESSION: 35

DISASTER RECOVERY

35.1 Aim

To make students familiarize with the basic concepts of incident response as well as Disaster recovery and Retention policy.

35.2 Instructional Objectives

The objective of this session is to introduce the understanding of purpose of incident response, identifying incident types, understanding disaster recovery and identifying critical assets.

35.3 Learning Outcomes

At the end of this session, students are expected to know

Understanding disaster recovery

Developing disaster recovery plan

Implementing data backup and recovery strategies

35.4 Module Description

This module deals about skills in recognizing, gathering, and safeguarding digital evidence. Incident response plan is discussed in detail. Functionalities of Incident Response Team are illustrated in this module. Communication Plan and stake holder management is also discussed. Cyber Kill Chain Attack Framework is analyzed. This module also covers disaster recovery and retention policy

35.5 Session Introduction

Organizations face a rising number of cyber security events in today's digital environment, including malware infections, data breaches, ransomware attacks, and insider threats. Serious repercussions from these situations may include monetary

losses, reputational harm, legal liability, and weakened customer confidence. Data loss, system downtime, financial losses, and reputational harm can all arise from disasters, whether they are brought on by natural events, human error, or cyber attacks.

35.6 Session Description

A thorough incident response strategy is built upon an incident response plan. It describes the positions to be filled and the protocols to be followed in the event of an incident. The following elements ought to be included in the IRP:

An incident response team should be formed, consisting of members from IT, security, legal, communication, and management, with roles and duties clearly defined.

Communication strategy: A strong communication strategy ensures timely and accurate communication between team members, stakeholders, and outside parties including customers, regulators, and law enforcement.

Prioritizing response efforts and categorizing incidents: A classification framework should be created to categorize incidents according to severity.

Establishing a reporting system for employees to promptly report issues and a clearly defined escalation process for handling serious incidents is essential.

To launch a prompt reaction, effective event identification and analysis are necessary. This phase entails:

Monitoring and logging: Putting in place dependable monitoring systems to find and record suspicious activity, such as unusual network traffic, system events, and user behavior.

SIEM stands for security information and event management. SIEM systems are used to gather and analyze security events and logs from diverse sources, allowing for the early detection of possible incidents.

Using external threat intelligence sources to stay up to date on new threats and vulnerabilities is known as threat intelligence.

35.7 Activities

For cyber security incidents to have as little of an effect as possible and to limit potential harm, quick and effective incident response is essential.

A methodical methodology known as incident response is used to identify, contain, eliminate, recover from, and analyse cyber security occurrences.
A formalised structure known as an incident response plan (IRP) describes the steps, roles, and duties for incident response activities.
The execution of the incident response plan and the coordination of response efforts are key functions performed by incident response teams, which are made up of qualified specialists.
Activities related to incident response include incident detection and reporting, threat containment and elimination, system and data recovery, post-event analysis, and lessons learned.
To ensure their efficacy and alignment with changing threats and organisational requirements, incident response plans should be periodically tested, updated, and improved.

35.8 Example

Consider the scenario where a business discovers a malware infestation on a computer belonging to one of its employees. The steps in the incident response procedure would be as follows:
Security monitoring systems at the organisation spot unusual network traffic and notify the incident response team.
To keep the infection in check, the compromised employee's PC has been cut off from the network. The incident response team limits access to sensitive data and prevents contact with known malicious IP addresses.
Eradication: After examining the malware, the incident response team creates a strategy to get rid of it from the compromised computer. They install antivirus software and carry out a full scan to find and get rid of any malware remnants.

35.9 Table Numbering: NA

35.10 Figures with Captions: NA

35.11 Self Assessment Questions

What function does an incident response team serve?

Why is communication crucial while responding to incidents?
How do data replication and backup help with disaster recovery?
Why are disaster recovery plans need to be tested and validated?

35.12 Summary

The cyber security strategy of an organisation must include incident response. Organisations may efficiently detect, respond to, and recover from cyber security problems by implementing a proactive and well-defined incident response methodology. The overall risk management and business continuity strategy of an organisation must include a well defined catastrophe recovery and retention policy. Organisations may lessen the effects of disasters and guarantee the resilience of crucial data and systems by putting pre-emptive measures into place, carrying out routine risk assessments, establishing reliable backup and restoration procedures, and following best practises.

35.13 Terminal Questions

1. How does incident response help to preserve client confidence?
2. What distinguishes incident containment from incident detection?
3. How does business continuity benefit from a disaster recovery and retention policy?
4. What essential components of the policy's data disposal process?

35.14 Answer Key:

Self Assessment Questions:

1. An organization's cybersecurity strategy must include an incident response team. They are in charge of quickly identifying, assessing, and reacting to security incidents. Their main objective is to lessen the effects of incidents, prevent additional harm, and promptly resume normal activities. The incident response team organises incident response activities, works with pertinent parties, looks into event causes, puts remediation plans into place, and makes sure that all legal and regulatory requirements are met. In the event of security risks, their knowledge and prompt action help protect the company's resources, reputation, and clientele.

2. For a number of reasons, communication is essential while responding to incidents. The incident response team may share information, plan activities, and arrive at well-informed judgements more quickly with effective communication. It aids in keeping stakeholders updated on the incident's status, active mitigation measures, and anticipated results. Collaboration is facilitated by timely and clear communication, which guarantees that the relevant individuals are involved and that resources are allocated properly. Additionally, it fosters confidence in the organization's capability to handle the crisis, preserves transparency, and aids in managing internal and external expectations. Communication enables a planned and effective reaction, reducing the incident's overall impact.

Terminal Questions:

1. In numerous respects, incident response is essential for maintaining client confidence. First and foremost, organisations show their dedication to safeguarding client data and assets by quickly identifying and responding to security events. Rapid incident response helps sustain uninterrupted services, minimises the effects of incidents, and cuts downtime, giving customers the assurance that their requirements are being given priority. Clients are apprised of the organization's efforts to handle the situation and are reassured by open communication during crisis response, including prompt updates and alerts. A well-executed incident response plan demonstrates an organization's professionalism and preparedness, fostering client loyalty and trust.
2. The incident response procedure comprises two separate phases: incident detection and incident containment. Monitoring systems, reviewing logs, and utilising various detection procedures are all part of incident detection, which entails determining the occurrence of a security issue. It focuses on identifying signs of compromise and unusual behaviours that can point to a security breach. On the other hand, incident containment describes the quick steps taken to stop the incident from spreading, reduce its impact, and stop future harm. To contain the crisis and lessen its effects, it entails isolating impacted systems, shutting off access points, and putting security controls in place.

35.15 Case Study: NA

35.16 Glossary: NA

35.17 References

1. Boddington, Richard. Practical digital forensics. Packt Publishing Ltd, 2016.

2. Årnes, André, ed. Digital forensics. John Wiley & Sons, 2017.

Sites and Web links:

MITRE ATT&CK Frameworkvs The Cyber Kill Chain: https://www.xcitium.com/cyber-kill-chain-vs-mitre-att&ck/

Attribution: https://carnegieendowment.org/2022/03/28/attribution-and-characterization-of-cyber-attacks-pub-86698

35.18 Keywords

Cyber security Incident, Eradication, Recovery, Recovery Time Objective.

SESSION: 36

RETENTION POLICY

36.1 Aim

To make the students familiarize with the basic concepts of incident response as well as Disaster recovery and Retention policy.

36.2 Instructional Objectives

The objective of this session is to introduce the understanding of purpose of incident response, identifying incident types, understanding disaster recovery and identifying critical assets.

36.3 Learning Outcomes

At the end of this session, students are expected to know
A comprehension of the catastrophe recovery process
Making preparations for the aftermath of a catastrophe
Establishing procedures for the backup and restoration of data

36.4 Module Description

Performing Incident Response: Introduction to Incident Response Process, Cyber Incident Response Team, Communication Plan and Stakeholder Management, Incident Response Plan, Cyber Kill Chain Attack Framework, Incident Response, Disaster Recovery, and Retention Policy

36.5 Session Introduction

In today's increasingly digital world, businesses are confronted with an increasing number of cyber security incidents. These incidents include malware infections, data breaches, ransomware attacks, and insider threats. There is a possibility that these events may have serious ramifications, including monetary losses, damage to reputation, legal liabilities, and a reduction in consumer trust. Disasters, whether they be caused by natural occurrences, human mistake, or cyber attacks, may result in the loss of data, the inability to operate systems, financial losses, and reputational damage.

36.6 Session Description

Analyzing the occurrence and conducting a thorough investigation to determine its scope, effects, and underlying causes. This covers malware analysis, digital forensics, and the detection of indicators of compromise (IOCs).

A. Business Impact Analysis and Risk Assessment: Creating a disaster recovery and retention policy effectively requires doing a thorough risk assessment and business impact analysis (BIA). Important elements include:
Identifying potential risks and dangers, such as natural disasters, power outages, hardware malfunctions, and cyber events that could result in data loss or system

interruptions.
BIA: Determining how these risks may affect crucial business systems, processes, and data in order to priorities recovery efforts and allocate resources effectively.
Implementing precautionary measures, such as redundant systems, routine maintenance, and security controls, to reduce the chance of disasters.
B. Backup and restoration of data:Procedures for data backup and restoration are crucial for recovering crucial data and guaranteeing business continuity:
Setting up backup rules, such as frequency, storage locations, and encryption techniques, is a backup strategy that protects data from loss or corruption. This could entail differential, incremental, or complete backups.

Offsite storage: Keeping backups in geographically distinct places to guard against localised catastrophes and guarantee data accessibility in the event of a site-level failure.
Establishing protocols for restoring data from backups, as well as testing and verification methods to guarantee the accuracy and usability of the data.
RTOs and RPOs are recovery time and recovery point objectives, respectively. The allowed turnaround time for recovering systems and data is determined by setting RTOs and RPOs:
RTO: The quickest possible period of time following a disaster when systems can be restored and regular operations can resume.
RPO: The maximum permitted data loss, which reflects the most recent point in time from which data can be restored.

36.7 Activities

A thorough structure outlining an organization's strategy to disaster impact reduction and data retention is known as a disaster recovery and retention policy.

The policy contains methods, steps, and principles for restoring activities and systems following a disruptive incident, such as a natural disaster, a cyberattack, or a hardware malfunction.

Disaster recovery entails creating recovery time objectives (RTOs) and recovery point objectives (RPOs), planning for system and data restoration, and putting backup and recovery techniques into practise.

For disaster recovery to be effective and reduce downtime, redundancy, off-site storage, and data replication are essential elements.

Data retention requirements are also covered by a disaster recovery and retention policy, which specifies how long data must be kept in accordance with legal, regulatory, and business requirements.

To ensure compliance with privacy and data protection laws and to safely dispose of superfluous or outdated data, data retention and disposal procedures are laid forth.

36.8 Example

Recovery: The incident response team works with the employee to return their machine to a safe and secure state after the infection has been eliminated. then check to see if all security patches and updates are installed as appropriate, and then run extra scans to make sure the system is clean of any lingering dangers.

Post-Incident Analysis: To ascertain the origin of the malware infection and locate any holes in the organization's security procedures, the incident response team performs a thorough investigation. Lessons learnt from the incident are recorded, and suggestions are made to improve the business's security posture to avoid repeat incidents.

36.9 Table Numbering: NA

36.10 Figures with Captions: NA

36.11 Self Assessment Questions

What function does an incident response team serve?
Why is communication crucial while responding to incidents?
How do data replication and backup help with disaster recovery?
Why are disaster recovery plans need to be tested and validated?

36.12 Summary

Incident response must be included into the cyber security strategy of any company. By putting in place a preventative and well defined incident response process, organisations improve their ability to identify, react to, and recover from cyber security

issues. A well-defined disaster recovery and retention policy should be a component of an organization's overall risk management and business continuity plan. This component is required. Putting preventative safeguards in place, conducting regular risk assessments, developing dependable data backup and restoration protocols, and adhering to industry best practises are some of the ways in which businesses may mitigate the negative impacts of natural disasters and ensure the resilience of their most important data and computer systems.

36.13 Terminal Questions

What distinguishes incident containment from incident detection?
How does business continuity benefit from a disaster recovery and retention policy?
What essential components of the policy's data disposal process?

36.14 Answer Key

Self Assessment Questions:

3. For a number of reasons, communication is essential while responding to incidents. The incident response team may share information, plan activities, and arrive at well-informed judgements more quickly with effective communication. It aids in keeping stakeholders updated on the incident's status, active mitigation measures, and anticipated results. Collaboration is facilitated by timely and clear communication, which guarantees that the relevant individuals are involved and that resources are allocated properly. Additionally, it fosters confidence in the organization's capability to handle the crisis, preserves transparency, and aids in managing internal and external expectations. Communication enables a planned and effective reaction, reducing the incident's overall impact.
4. Backup and replication of data are essential components of disaster recovery plans. Data redundancy is achieved by retaining copies of the data across several systems or locations. Data replication enables seamless failover to the duplicated copies in the case of a disaster or data loss, minimising downtime and guaranteeing business continuity. Data backup, on the other hand, is routinely making copies of data and securely storing them. After a disaster, backups can be used to restore data, allowing businesses to fix damaged or deleted files and

carry on with their regular activities. Data replication and backup work together to preserve data integrity and speed up restoration procedures, providing essential safeguards for disaster recovery.

5. For a number of reasons, disaster recovery strategies need to be tested and verified. Testing enables required plan revisions and improvements by revealing any flaws, gaps, or inefficiencies. It guarantees that the strategy is realistic, efficient, and capable of being carried out successfully during a genuine emergency. The incident response team is better trained and trust in the plan's dependability is increased through testing. Regular testing ensures a quick and easy recovery in the event of a disaster while also assisting organisations in meeting regulatory obligations and demonstrating their preparation to stakeholders.

Terminal Questions:

3. The incident response procedure comprises two separate phases: incident detection and incident containment. Monitoring systems, reviewing logs, and utilising various detection procedures are all part of incident detection, which entails determining the occurrence of a security issue. It focuses on identifying signs of compromise and unusual behaviours that can point to a security breach. On the other hand, incident containment describes the quick steps taken to stop the incident from spreading, reduce its impact, and stop future harm. To contain the crisis and lessen its effects, it entails isolating impacted systems, shutting off access points, and putting security controls in place.
4. Having a disaster recovery and retention policy has various advantages for business continuity. A disaster recovery plan guarantees that activities can be quickly resumed after a disruptive incident and that systems, data, and key infrastructure can be restored. This reduces downtime and enables the company to continue operating, preventing financial losses and upholding consumer confidence. A retention policy makes sure that crucial information is kept for the required amount of time, easing compliance with legal requirements and business continuity initiatives by enabling the reconstruction of vital data in the event of a catastrophe.
5. The following crucial elements should be included in any policy's data disposal process:

a. Clearly defined rules: Specify the categories of data that must be disposed of as well as the techniques to be used.
b. Identify safe data destruction techniques, such as secure erasure, degaussing, physical destruction, or secure data wiping.
c. Legal compliance: Ensure adherence to applicable data protection laws and rules controlling data disposal, including obligations and timeframes for data retention.
d. Documentation: Keep a log of all data disposal actions, including the dates, procedures, and people in charge.
e. Training and awareness: Raise awareness of data privacy and security issues and train staff members on proper disposal processes.
f. Monitoring and auditing: Put in place routine monitoring and auditing procedures to make sure the data disposal policy is being followed.
g. Vendor management: Establish rules for how third-party vendors and service providers should dispose of their data, ensuring that they follow the organization's policy.

By including these elements, a company may create a thorough data disposal procedure that protects private data and reduces the possibility of hacking or other unauthorised access.

36.15 Case Study: NA

36.16 Glossary: NA

.

36.17 References

- Incident Response and Disaster Recovery Planning for IT Systems by Michael E. Whitman and Herbert J. Mattord.
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- https://www.sans.org/media/incident-response-plan-template.pdf
- https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14096.pdf
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

36.18 Keywords

Forensic Incident Classification, Situation Reporting, Retention and disposal of data, Redundancy, Validation and Testing

Session 34

CYBER KILL CHAIN FRAMEWORK

34.1 Aim

To understand the concepts of attack attribution and Cyber Kill Chain attacks.

34.2 Instructional Objectives

The objective of this session to provide a schematic and generic description of the nexus attribution in cyber attacks. Cyber kill chain are the two broad terms to address cyber attacks against an organisation. Cyber Kill Chain with its seven phases, addresses the cyber attack process from a high level.

34.3 Learning Outcomes:

At the end of this session, students are expected to know the attack attribution and Cyber Kill Chain attacks.

34.4 Module Description

This module deals about skills in recognizing, gathering, and safeguarding digital evidence. Incident response plan is discussed in detail. Functionalities of Incident Response Team are illustrated in this module. Communication Plan and stake holder management is also discussed. Cyber Kill Chain Attack Framework is analyzed. This module also covers disaster recovery and retention policy

34.5 Session Introduction

This session aims to provide a schematic and generic description of the nexus between attribution and characterization in cyber attacks.

34.6 Session Description

Attack attribution:

Attack attribution in the context of cyber security refers to the process of identifying and assigning responsibility for a cyber attack or intrusion to a specific individual, group, organization, or nation-state. It involves investigating and analysing various

pieces of evidence to gather intelligence and make informed assessments about the identity of the attacker.

The primary goal of attack attribution is to determine who is behind the attack and understand their motivations, capabilities, and intentions. This information is crucial for developing appropriate response strategies, implementing necessary security measures, and potentially taking legal or diplomatic actions against the responsible parties.

The process of attack attribution involves multiple steps and relies on a combination of technical, intelligence, and investigative techniques. Here are some key aspects involved in attack attribution:

Evidence Collection: Gathering relevant evidence is the first step in the attribution process. This can include analysing network logs, system logs, malware samples, intrusion detection system alerts, IP addresses, domain names, and any other digital artefacts associated with the attack.

Forensic Analysis: Conducting in-depth forensic analysis helps in understanding the attack vectors, techniques, and tools used by the attacker. This may involve reverse engineering malware, analysing network traffic, examining system artifacts, and reconstructing the attack timeline.

Attribution Indicators: Identifying attribution indicators involves looking for patterns, signatures, or characteristics that can link the attack to a specific individual, group, or known threat actor. This can include TTPs (Tactics, Techniques, and Procedures) used in previous attacks, known affiliations, infrastructure overlaps, language or cultural clues, and geopolitical context.

Intelligence Gathering: Collaborating with intelligence agencies, cyber security firms, and other industry partners to gather additional intelligence on threat actors can provide valuable insights for attribution. This may involve sharing information, analysing threat intelligence reports, and leveraging specialized tools and resources.

Contextual Analysis: Understanding the context surrounding the attack is crucial for attribution. This involves considering geopolitical factors, historical relationships, ongoing conflicts, and motivations that could influence the behaviour of potential threat actors.

Corroborative Sources: Cross-referencing and validating findings with multiple sources of information and intelligence helps ensure the accuracy and reliability of the

attribution assessment. This can include corroborating evidence from different organizations, government agencies, open-source intelligence, and expert opinions.

It's important to note that attack attribution is a challenging and complex process. Determining attribution with absolute certainty is often difficult due to the ability of attackers to obfuscate their tracks and employ various techniques to mislead investigators. As a result, attribution assessments are often presented as a range of possibilities or confidence levels, based on the available evidence and the expertise of the investigators.

Ultimately, the goal of attack attribution is to provide actionable intelligence that enables organizations to better defend against future attacks, mitigate risks, and respond effectively to cyber threats.

Cyber Kill Chain

The "cyber kill chain" refers to a series of stages that an attacker must go through to breach a network and extract data. Each stage represents a distinct objective in the attacker's progression. Implementing a monitoring and response strategy based on the cyber kill chain model proves effective as it centres on understanding the actual progression of attacks.

The stages of an attack, following the cyber kill chain model, are as follows:

Reconnaissance:

Gathering information about the target, such as through social media, email addresses, and intellectual property.

Weaponization:

Combining a trojan with an exploitable application, typically in the form of weaponized deliverables like Adobe PDF or MS Office documents.

Delivery

Transporting the weapon to the target environment, often through email attachments, USB removable media, or compromised websites.

Exploitation:

Activating the intruder's code, which may auto-execute by exploiting vulnerabilities in the operating system or applications.

Installation/Spread

Establishing a backdoor or trojan for persistence, while remaining hidden from security devices.

Command & Control

Setting up channels for sending and receiving information between the attacker and the compromised system.

Accomplish Mission

Carrying out the intended goals of the attack, which may involve theft of money, theft of intellectual property, or destruction of data.

Exfiltration

Collecting, encrypting, and extracting information from the target system, often with the objective of using it to compromise other machines.

Defensible Actions

- Detect: verify that some attacker is looking around
- Deny: prevent the attacker from gaining information
- Disrupt: stop or change outbound traffic (to attacker)
- Degrade: attack attacker's command & control
- Deceive: interfere with command & control
- Contain: network segmentation changes

Attack Patterns

Indicators: any piece of information that describes an intrusion Atomic: ip addresses, email addresses, vulnerability identifiers Computed: derived from data collected during an incident.

Behavioural: collections of atomic and computed indicators

34.7 Activities

34.8 Example

34.9 Table Numbering; NA

34.10 Figures with captions: NA

34.11 Self Assessment Questions

- How the MITRE ATT&CK Framework used in financial industry?
- What are the stages available in the cyber kill chain model?
- Compare MITRE ATT&CK and cyber kill chain?
- Mention the Attack Levels in MITRE ATT?

34.12 Summary

The MITRE ATT&CK Framework and the Cyber Kill Chain provide valuable insights into the lifecycle of cyberattacks. The MITRE ATT&CK Framework offers a

comprehensive catalog of adversary techniques and tactics, enabling organizations to better understand and defend against threats. On the other hand, the Cyber Kill Chain outlines the stages an attacker typically goes through to infiltrate a network.

34.13 Terminal Questions

- Compare the MITRE ATT&CK Framework and Cyber Kill Chain.
- Illustrate the various attack levels in MITRE ATT&CK Framework.
- Explain the in cyber kill chain model.

34.14 Answer key:

MITRE ATT&CK Framework: It provides a comprehensive catalog of adversary tactics, techniques, and procedures (TTPs).

The Cyber Kill Chain: It outlines the sequential stages of an attack, from reconnaissance to accomplishing the mission.

Attack Levels in MITRE ATT

- *Tactics*
- *Techniques*
- *Sub-techniques*
- *Procedures*

The stages of an attack in cyber kill chain model, are as follows:

- *Reconnaissance*
- *Weaponization*
- *Delivery*
- *Installation/Spread*
- *Command & Control*
- *Accomplish Mission*
- *Exfiltration*

Glossary:

- Attack attribution in the context of cybersecurity refers to the process of identifying and assigning responsibility for a cyber attack or intrusion to a specific individual, group, organization, or nation-state.
- MITRE ATT&CK Framework: It provides a comprehensive catalog of adversary tactics, techniques, and procedures (TTPs).
- The Cyber Kill Chain: It outlines the sequential stages of an attack, from reconnaissance to accomplishing the mission.

34.15 Case Study: NA

34.16 Glossary

34.17 Reference Books

1. Boddington, Richard. Practical digital forensics. Packt Publishing Ltd, 2016.

2. Årnes, André, ed. Digital forensics. John Wiley & Sons, 2017.

Sites and Web links:

MITRE ATT&CK Frameworkvs The Cyber Kill Chain: https://www.xcitium.com/cyber-kill-chain-vs-mitre-att&ck/

Attribution: https://carnegieendowment.org/2022/03/28/attribution-and-characterization-of-cyber-attacks-pub-86698

34.18 Keywords

Cyber Kill Chain Framework

SESSION: 35

DISASTER RECOVERY

35.1 Aim

To make students familiarize with the basic concepts of incident response as well as Disaster recovery and Retention policy.

35.2 Instructional Objectives

The objective of this session is to introduce the understanding of purpose of incident response, identifying incident types, understanding disaster recovery and identifying critical assets.

35.3 Learning Outcomes

At the end of this session, students are expected to know

Understanding disaster recovery

Developing disaster recovery plan

Implementing data backup and recovery strategies

35.4 Module Description

This module deals about skills in recognizing, gathering, and safeguarding digital evidence. Incident response plan is discussed in detail. Functionalities of Incident Response Team are illustrated in this module. Communication Plan and stake holder management is also discussed. Cyber Kill Chain Attack Framework is analyzed. This module also covers disaster recovery and retention policy

35.5 Session Introduction

Organizations face a rising number of cyber security events in today's digital environment, including malware infections, data breaches, ransomware attacks, and insider threats. Serious repercussions from these situations may include monetary losses, reputational harm, legal liability, and weakened customer confidence. Data loss, system downtime, financial losses, and reputational harm can all arise from

disasters, whether they are brought on by natural events, human error, or cyber attacks.

35.6 Session Description

A thorough incident response strategy is built upon an incident response plan. It describes the positions to be filled and the protocols to be followed in the event of an incident. The following elements ought to be included in the IRP:

An incident response team should be formed, consisting of members from IT, security, legal, communication, and management, with roles and duties clearly defined.

Communication strategy: A strong communication strategy ensures timely and accurate communication between team members, stakeholders, and outside parties including customers, regulators, and law enforcement.

Prioritizing response efforts and categorizing incidents: A classification framework should be created to categorize incidents according to severity.

Establishing a reporting system for employees to promptly report issues and a clearly defined escalation process for handling serious incidents is essential.

To launch a prompt reaction, effective event identification and analysis are necessary. This phase entails:

Monitoring and logging: Putting in place dependable monitoring systems to find and record suspicious activity, such as unusual network traffic, system events, and user behavior.

SIEM stands for security information and event management. SIEM systems are used to gather and analyze security events and logs from diverse sources, allowing for the early detection of possible incidents.

Using external threat intelligence sources to stay up to date on new threats and vulnerabilities is known as threat intelligence.

35.7 Activities

For cyber security incidents to have as little of an effect as possible and to limit potential harm, quick and effective incident response is essential.

A methodical methodology known as incident response is used to identify, contain, eliminate, recover from, and analyse cyber security occurrences.
A formalised structure known as an incident response plan (IRP) describes the steps, roles, and duties for incident response activities.
The execution of the incident response plan and the coordination of response efforts are key functions performed by incident response teams, which are made up of qualified specialists.
Activities related to incident response include incident detection and reporting, threat containment and elimination, system and data recovery, post-event analysis, and lessons learned.
To ensure their efficacy and alignment with changing threats and organisational requirements, incident response plans should be periodically tested, updated, and improved.

35.8 Example

Consider the scenario where a business discovers a malware infestation on a computer belonging to one of its employees. The steps in the incident response procedure would be as follows:
Security monitoring systems at the organisation spot unusual network traffic and notify the incident response team.
To keep the infection in check, the compromised employee's PC has been cut off from the network. The incident response team limits access to sensitive data and prevents contact with known malicious IP addresses.
Eradication: After examining the malware, the incident response team creates a strategy to get rid of it from the compromised computer. They install antivirus software and carry out a full scan to find and get rid of any malware remnants.

35.9 Table Numbering: NA

35.10 Figures with Captions: NA

35.11 Self Assessment Questions

What function does an incident response team serve?

Why is communication crucial while responding to incidents?
How do data replication and backup help with disaster recovery?
Why are disaster recovery plans need to be tested and validated?

35.12 Summary

The cyber security strategy of an organisation must include incident response. Organisations may efficiently detect, respond to, and recover from cyber security problems by implementing a proactive and well-defined incident response methodology. The overall risk management and business continuity strategy of an organisation must include a well defined catastrophe recovery and retention policy. Organisations may lessen the effects of disasters and guarantee the resilience of crucial data and systems by putting pre-emptive measures into place, carrying out routine risk assessments, establishing reliable backup and restoration procedures, and following best practises.

35.13 Terminal Questions

1. How does incident response help to preserve client confidence?
2. What distinguishes incident containment from incident detection?
3. How does business continuity benefit from a disaster recovery and retention policy?
4. What essential components of the policy's data disposal process?

35.14 Answer Key:

Self Assessment Questions:

6. An organization's cybersecurity strategy must include an incident response team. They are in charge of quickly identifying, assessing, and reacting to security incidents. Their main objective is to lessen the effects of incidents, prevent additional harm, and promptly resume normal activities. The incident response team organises incident response activities, works with pertinent parties, looks into event causes, puts remediation plans into place, and makes sure that all legal and regulatory requirements are met. In the event of security risks, their knowledge and prompt action help protect the company's resources, reputation, and clientele.

7. For a number of reasons, communication is essential while responding to incidents. The incident response team may share information, plan activities, and arrive at well-informed judgements more quickly with effective communication. It aids in keeping stakeholders updated on the incident's status, active mitigation measures, and anticipated results. Collaboration is facilitated by timely and clear communication, which guarantees that the relevant individuals are involved and that resources are allocated properly. Additionally, it fosters confidence in the organization's capability to handle the crisis, preserves transparency, and aids in managing internal and external expectations. Communication enables a planned and effective reaction, reducing the incident's overall impact.

Terminal Questions:

6. In numerous respects, incident response is essential for maintaining client confidence. First and foremost, organisations show their dedication to safeguarding client data and assets by quickly identifying and responding to security events. Rapid incident response helps sustain uninterrupted services, minimises the effects of incidents, and cuts downtime, giving customers the assurance that their requirements are being given priority. Clients are apprised of the organization's efforts to handle the situation and are reassured by open communication during crisis response, including prompt updates and alerts. A well-executed incident response plan demonstrates an organization's professionalism and preparedness, fostering client loyalty and trust.
7. The incident response procedure comprises two separate phases: incident detection and incident containment. Monitoring systems, reviewing logs, and utilising various detection procedures are all part of incident detection, which entails determining the occurrence of a security issue. It focuses on identifying signs of compromise and unusual behaviours that can point to a security breach. On the other hand, incident containment describes the quick steps taken to stop the incident from spreading, reduce its impact, and stop future harm. To contain the crisis and lessen its effects, it entails isolating impacted systems, shutting off access points, and putting security controls in place.

35.15 Case Study: NA

35.16 Glossary: NA

35.17 References

1. Boddington, Richard. Practical digital forensics. Packt Publishing Ltd, 2016.

2. Årnes, André, ed. Digital forensics. John Wiley & Sons, 2017.

Sites and Web links:

MITRE ATT&CK Frameworkvs The Cyber Kill Chain: https://www.xcitium.com/cyber-kill-chain-vs-mitre-att&ck/

Attribution: https://carnegieendowment.org/2022/03/28/attribution-and-characterization-of-cyber-attacks-pub-86698

35.18 Keywords

Cyber security Incident, Eradication, Recovery, Recovery Time Objective.

SESSION: 36

RETENTION POLICY

36.1 Aim

To make the students familiarize with the basic concepts of incident response as well as Disaster recovery and Retention policy.

36.2 Instructional Objectives

The objective of this session is to introduce the understanding of purpose of incident response, identifying incident types, understanding disaster recovery and identifying critical assets.

36.3 Learning Outcomes

At the end of this session, students are expected to know
A comprehension of the catastrophe recovery process
Making preparations for the aftermath of a catastrophe
Establishing procedures for the backup and restoration of data

36.4 Module Description

Performing Incident Response: Introduction to Incident Response Process, Cyber Incident Response Team, Communication Plan and Stakeholder Management, Incident Response Plan, Cyber Kill Chain Attack Framework, Incident Response, Disaster Recovery, and Retention Policy

36.5 Session Introduction

In today's increasingly digital world, businesses are confronted with an increasing number of cyber security incidents. These incidents include malware infections, data breaches, ransomware attacks, and insider threats. There is a possibility that these events may have serious ramifications, including monetary losses, damage to

reputation, legal liabilities, and a reduction in consumer trust. Disasters, whether they be caused by natural occurrences, human mistake, or cyber attacks, may result in the loss of data, the inability to operate systems, financial losses, and reputational damage.

36.6 Session Description

Analyzing the occurrence and conducting a thorough investigation to determine its scope, effects, and underlying causes. This covers malware analysis, digital forensics, and the detection of indicators of compromise (IOCs).

A. Business Impact Analysis and Risk Assessment: Creating a disaster recovery and retention policy effectively requires doing a thorough risk assessment and business impact analysis (BIA). Important elements include:
Identifying potential risks and dangers, such as natural disasters, power outages, hardware malfunctions, and cyber events that could result in data loss or system interruptions.
BIA: Determining how these risks may affect crucial business systems, processes, and data in order to priorities recovery efforts and allocate resources effectively.
Implementing precautionary measures, such as redundant systems, routine maintenance, and security controls, to reduce the chance of disasters.
B. Backup and restoration of data:Procedures for data backup and restoration are crucial for recovering crucial data and guaranteeing business continuity:
Setting up backup rules, such as frequency, storage locations, and encryption techniques, is a backup strategy that protects data from loss or corruption. This could entail differential, incremental, or complete backups.

Offsite storage: Keeping backups in geographically distinct places to guard against localised catastrophes and guarantee data accessibility in the event of a site-level failure.
Establishing protocols for restoring data from backups, as well as testing and verification methods to guarantee the accuracy and usability of the data.
RTOs and RPOs are recovery time and recovery point objectives, respectively. The allowed turnaround time for recovering systems and data is determined by setting

RTOs and RPOs:
RTO: The quickest possible period of time following a disaster when systems can be restored and regular operations can resume.
RPO: The maximum permitted data loss, which reflects the most recent point in time from which data can be restored.

36.7 Activities

A thorough structure outlining an organization's strategy to disaster impact reduction and data retention is known as a disaster recovery and retention policy.

The policy contains methods, steps, and principles for restoring activities and systems following a disruptive incident, such as a natural disaster, a cyberattack, or a hardware malfunction.

Disaster recovery entails creating recovery time objectives (RTOs) and recovery point objectives (RPOs), planning for system and data restoration, and putting backup and recovery techniques into practise.

For disaster recovery to be effective and reduce downtime, redundancy, off-site storage, and data replication are essential elements.

Data retention requirements are also covered by a disaster recovery and retention policy, which specifies how long data must be kept in accordance with legal, regulatory, and business requirements.

To ensure compliance with privacy and data protection laws and to safely dispose of superfluous or outdated data, data retention and disposal procedures are laid forth.

36.8 Example

Recovery: The incident response team works with the employee to return their machine to a safe and secure state after the infection has been eliminated. then check to see if all security patches and updates are installed as appropriate, and then run extra scans to make sure the system is clean of any lingering dangers.

Post-Incident Analysis: To ascertain the origin of the malware infection and locate any holes in the organization's security procedures, the incident response team performs a thorough investigation. Lessons learnt from the incident are recorded, and suggestions are made to improve the business's security posture to avoid repeat incidents.

36.9 Table Numbering: NA

36.10 Figures with Captions: NA

36.11 Self Assessment Questions

What function does an incident response team serve?
Why is communication crucial while responding to incidents?
How do data replication and backup help with disaster recovery?
Why are disaster recovery plans need to be tested and validated?

36.12 Summary

Incident response must be included into the cyber security strategy of any company. By putting in place a preventative and well defined incident response process, organisations improve their ability to identify, react to, and recover from cyber security issues. A well-defined disaster recovery and retention policy should be a component of an organization's overall risk management and business continuity plan. This component is required. Putting preventative safeguards in place, conducting regular risk assessments, developing dependable data backup and restoration protocols, and adhering to industry best practises are some of the ways in which businesses may mitigate the negative impacts of natural disasters and ensure the resilience of their most important data and computer systems.

36.13 Terminal Questions

What distinguishes incident containment from incident detection?
How does business continuity benefit from a disaster recovery and retention policy?
What essential components of the policy's data disposal process?

36.14 Answer Key

Self Assessment Questions:

1. For a number of reasons, communication is essential while responding to incidents. The incident response team may share information, plan activities, and arrive at well-informed judgements more quickly with effective communication. It aids in keeping stakeholders updated on the incident's status, active mitigation measures, and anticipated results. Collaboration is facilitated by timely and clear communication, which guarantees that the relevant individuals are involved and that resources are allocated properly. Additionally, it fosters confidence in the organization's capability to handle the crisis, preserves transparency, and aids in managing internal and external expectations. Communication enables a planned and effective reaction, reducing the incident's overall impact.
2. Backup and replication of data are essential components of disaster recovery plans. Data redundancy is achieved by retaining copies of the data across several systems or locations. Data replication enables seamless failover to the duplicated copies in the case of a disaster or data loss, minimising downtime and guaranteeing business continuity. Data backup, on the other hand, is routinely making copies of data and securely storing them. After a disaster, backups can be used to restore data, allowing businesses to fix damaged or deleted files and carry on with their regular activities. Data replication and backup work together to preserve data integrity and speed up restoration procedures, providing essential safeguards for disaster recovery.
3. For a number of reasons, disaster recovery strategies need to be tested and verified. Testing enables required plan revisions and improvements by revealing any flaws, gaps, or inefficiencies. It guarantees that the strategy is realistic, efficient, and capable of being carried out successfully during a genuine emergency. The incident response team is better trained and trust in the plan's dependability is increased through testing. Regular testing ensures a quick and easy recovery in the event of a disaster while also assisting organisations in meeting regulatory obligations and demonstrating their preparation to stakeholders.

Terminal Questions:

8. The incident response procedure comprises two separate phases: incident detection and incident containment. Monitoring systems, reviewing logs, and

utilising various detection procedures are all part of incident detection, which entails determining the occurrence of a security issue. It focuses on identifying signs of compromise and unusual behaviours that can point to a security breach. On the other hand, incident containment describes the quick steps taken to stop the incident from spreading, reduce its impact, and stop future harm. To contain the crisis and lessen its effects, it entails isolating impacted systems, shutting off access points, and putting security controls in place.

9. Having a disaster recovery and retention policy has various advantages for business continuity. A disaster recovery plan guarantees that activities can be quickly resumed after a disruptive incident and that systems, data, and key infrastructure can be restored. This reduces downtime and enables the company to continue operating, preventing financial losses and upholding consumer confidence. A retention policy makes sure that crucial information is kept for the required amount of time, easing compliance with legal requirements and business continuity initiatives by enabling the reconstruction of vital data in the event of a catastrophe.
10. The following crucial elements should be included in any policy's data disposal process:
    a. Clearly defined rules: Specify the categories of data that must be disposed of as well as the techniques to be used.
    b. Identify safe data destruction techniques, such as secure erasure, degaussing, physical destruction, or secure data wiping.
    c. Legal compliance: Ensure adherence to applicable data protection laws and rules controlling data disposal, including obligations and timeframes for data retention.
    d. Documentation: Keep a log of all data disposal actions, including the dates, procedures, and people in charge.
    e. Training and awareness: Raise awareness of data privacy and security issues and train staff members on proper disposal processes.
    f. Monitoring and auditing: Put in place routine monitoring and auditing procedures to make sure the data disposal policy is being followed.
    g. Vendor management: Establish rules for how third-party vendors and service providers should dispose of their data, ensuring that they follow the organization's policy.

By including these elements, a company may create a thorough data disposal procedure that protects private data and reduces the possibility of hacking or other unauthorised access.

36.15 Case Study: NA

36.16 Glossary: NA

36.17 References

- Incident Response and Disaster Recovery Planning for IT Systems by Michael E. Whitman and Herbert J. Mattord.

- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- https://www.sans.org/media/incident-response-plan-template.pdf
- https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14096.pdf
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

36.18 Keywords

Forensic Incident Classification, Situation Reporting, Retention and disposal of data, Redundancy, Validation and Testing