Cryptography & Network Security

BCSF186EI0

BE - III Year VI Semester
(2021-2022)

DEPARTMENT OF CSE

SRI CHANDRASEKHARENDRA SARASWATHI VISWA MAHAVIDYALAYA

(Deemed to be University established under section 3 of UGC act 1956)

ENATHUR, KANCHIPURAM - 631 561

Course Code :	CRYPTOGRAPHY AND NETWORK SECURITY	L	T	P	C
		3	0	0	3

PRE-REQUISITE : Operating Systems knowledge, Network architecture / administration experience. Basic knowledge of discrete mathematics (algebra), information theory and Analysis of Algorithms

OBJECTIVES

1. To understand the fundamentals of cryptography
2. To acquire knowledge on standard algorithms used to provide confidentiality. Integrity and authenticity
3. To understand the various key distribution and management schemes.
4. To enhance the knowledge of the students with concepts of computer network security.
5. To learn about the concepts, issues, principles of security related properties and validate using model checking.
6. To understand knowledge of a range of computer network security technologies as well as network security tools and services

COURSE OUTCOME:

On successful completion of the course, the student will:

1. Understand the knowledge about network security services and mechanisms.
2. Analyze about Symmetrical and Asymmetrical cryptography.
3. Analyze and Understand about the concept of Data integrity, Authentication, Digital Signatures.
4. Analyze about Various network security applications, IPSec, Firewall, IDS, Web security, Email security, and Malicious software etc.
5. Understand the security issues involved with different Network operating systems

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	S									
CO2			S							
CO3				M						
CO4				M						
CO5									S	

MAPPING WITH PROGRAMME OUTCOMES
S - STRONG; M – MEDIUM; L - LOW

UNIT - I

Introduction to Network Security - Attacks- Services- Mechanism – Conventional Encryption Principle – Cipher Principles – Data Encryption Standard – Block Cipher Design Principles and Modes of Operation - Triple DES – Placement of Encryption Function – Traffic Confidentiality – Key Distribution.

UNIT – II

Introduction to Public Key Cryptography – RSA - Diffie-Hellman key Exchange – Key Management- Session and Interchange keys, Key exchange and generation-PKI

UNIT - III

Authentication requirements – Authentication functions – Message Authentication Codes – Hash Functions – Security of Hash Functions and MACs – MD5 message Digest algorithm - Secure Hash Algorithm – HMAC - Digital Signatures – Authentication Protocols – Digital Signature Standard

UNIT- IV

Authentication Applications: Kerberos – X.509 Authentication Service – Electronic Mail Security – PGP – S/MIME - IP Security – Web Security.

UNIT- V

Intrusion detection – password management – Viruses and related Threats – Virus Counter measures – Firewall Design Principles – Trusted Systems.

TEXT BOOKS

1. William Stallings, "Cryptography and Network Security – Principles and Practices", March 2013
2. Forouzan, "Cryptography and Network Securiity", November 2015
3. William Stallings, "Cryptography and Network Security – Principles and Practices", Prentice Hall of India, Fourth Edition 2006.

UNIT I

Introduction to Network Security

Objectives:

This course is to discuss

- security needs
- security services
- security mechanisms and protocols

for data stored in computers and transmitted across computer networks

Learning Outcomes:

- Application security measures
- How to identify operating system holes
- The important interplay of privacy and digital rights management
- Trends in malware, privacy and security for mobile devices
- Ways to prevent network attacks and gaps in security policy

Prerequisites:

- Network security is one of the most important computer science issues today.

- It helps businesses meet mandatory compliance regulations, protect customer data, and reduce the risk of legal action.

- Without a secure infrastructure and the expertise to remedy an issue, critical performance functions for users and computer programs may not be executable.

- This course covers the latest practices for building reliable and secure code to defend against various attack techniques, harmful viruses and threats.

Plan for the lecture delivery:

- Teaching aid both Blackboard and Presentation Via LCD
- Topic should be start with Definition, System Model as follows:
  - Confidentiality
  - Integrity
  - Availability

Confidentiality, Integrity and Availability:

Confidentiality:

- In simple terms, confidentiality means something that is secret and is not supposed to be disclosed to unintended people or entities.
- Confidentiality ensures that sensitive information is accessed only by an authorized person and kept away from those not authorized to possess them.
- Everyone has information which they wish to keep secret. Thus Protecting such information is an important part of information security.

Examples of confidential information:

- Bank account statements
- Personal information
- Credit card numbers
- Trade secrets
- Government documents

Examples of attacks that affect confidentiality:

- Packet sniffing
- Password cracking
- Dumpster diving
- Wiretapping
- Keylogging
- Phishing

Way to ensure confidentiality:

- Usernames and passwords
- Two-factor authentication
- Biometric verification
- Security tokens or key fobs
- Data encryption

Integrity:

In the context of the information security (InfoSec) world, integrity means that when a sender sends data, the receiver must receive exactly the same data as sent by the sender.

Example attacks that affect Integrity:

- Salami attack
- Data diddling attacks
- Session hijacking
- Man-in-the-middle (MITM) attack

Availability:

- Availability implies that information is available to the authorized parties whenever required. Unavailability to data and systems can have serious consequences.

- It is essential to have plans and procedures in place to prevent or mitigate data loss as a result of a disaster. A disaster recovery plan must include unpredictable events such as natural disasters and fire.

Example attacks that affect Availability:

- DoS and DDoS attacks
- SYN flood attacks
- Physical attacks on server infrastructure

Physical Security Attack:

- Examples of **threats** that **physical security** protects against are unauthorized access into areas and theft of mobile devices.

- Attackers can gain entry into secured areas through tailgating, hacking into access control smart cards or breaking in through doors.

Practical Real World Example:

- Prevention

  locks at doors, window bars, secure the walls around the property, hire a guard

- Detection

  missing items, burglar alarms, closed circuit TV

- Reaction

  attack on burglar, call the police, replace stolen items, make an insurance claim

Internet Shopping Example:

Prevention

- Encrypt your order and card number, enforce merchants to do some extra checks, using PIN even for Internet transactions, don't send card number via Internet

Detection

- an unauthorized transaction appears on your credit card statement

Reaction

- complain, dispute, ask for a new card number

Application of Traffic Confidentialtiy:

- In commercial applications, traffic analysis may yield information that the traffic generators would like to conceal.

The following types of information that can be derived from a traffic analysis attack:

- Identities of partners, how frequent the partners are communicating, message pattern.

- Message length, or quantity of messages that suggest important information is being exchanged, and the events that correlate with special conversation between particular partners.

UNIT II

Introduction to Public Key Cryptography

Objectives:

This course is to discuss

- Public Key Cryptography
- PKI(Public Key Infrastructure) and Interchange Key
- Key Management

Learning Outcomes:

- Use basic security tools to enhance system security.
- Develop basic security enhancements in stand-alone applications.
- The importance of privacy and Key Management

Prerequisites:

- Network security is one of the most important computer science issues today.

- It helps businesses meet mandatory compliance regulations, protect customer data, and reduce the risk of legal action.

- Without a secure infrastructure and the expertise to remedy an issue, critical performance functions for users and computer programs may not be executable.

- This course covers the latest practices for building reliable and secure code to defend against various attack techniques, harmful viruses and threats.

Plan for the lecture delivery:

- Teaching aid both Blackboard and Presentation Via LCD
- Topic should be start with Definition, System Model as follows:
  - Double Key, Asymmetric Key, Two Key
  - RSA, Diffie Hellman Key Exchange Algorithm
  - E-mail Security(PGP, S/MIME)
  - PKI and Key Management
  - Confidentiality
  - Real Time Example of Public Key Cryptography


Sign In
Login
First Factor
Proposed Transaction
Second Factor

Public key cryptography is used in a wide variety of protocols and data formats, which are implemented by a huge range of application and system software:

- SSL (https) protocol
- SSH (secure remote login, tunneling, etc)
- Digitally signed PDF files (including attachments within the PDF)
- Signed Applets and jar archive files for Java
- Digital signatures in the packaging infrastructure for Debian, Ubuntu and Red Hat Linux distributions, etc.
- PGP/GPG for signed and/or encrypted files and email
- S/MIME for signed and/or encrypted email

- DNSSEC for securing the DNS
- Internet Key Exchange (IKE) in IPsec for secure low-level TCP/UDP networking
- RFC 3161 for authenticated timestamps
- A variety of other uses, like digital cash and secure transparent voting

Real time Example of Public Key Cryptography:

- HTTPS website connection
- Digital Signature
- Nowadays, it is used mainly to achieve Non-repudiation and Authentication.
- For Confidentiality: Any fast encryption algorithm.
- For Integrity: Any Hashing Algorithms

RSA Algorithm:

- RSA algorithm is often used to authenticate the sever and/or the client. As we want to maintain perfect forward secrecy, and RSA algorithm is slow, we use symmetric key encryption while transferring the actual data. But, initially the TLS connection uses public key encryption algorithm like RSA

- RSA is one of the cipher suites used in Transport Layer Security, which is used by HTTPS, so RSA may be used in any connection to an https: URL. (Elliptic Curve Cryptography may also be used in TLS/HTTPS in the same way.)

- Asymmetric cryptography (either RSA or ECC) is usually used in a lot of software for verifying that software updates are from the original developer.

The RSA algorithm is the most widely used Asymmetric Encryption algorithm deployed to date.

The acronym is derived from the last names of the three mathematicians who created it in 1977: Ron **R**ivest, Adi **S**hamir, Leonard **A**dleman.

In order to understand the algorithm, there are a few terms we have to define:

Prime – A number is said to be Prime if it is only divisible by 1 and itself. Such as: 2, 3, 5, 7, 11, 13, etc.

Factor – A factor is a number you can multiple to get another number. For example, the factors of 12 are 1, 2, 3, 4, 6, and 12.

Semi-Prime – A number is Semi Prime if its only factors are prime (excluding 1 and itself).

For example:
12 is *not* semi-prime — one of its factors is 6, which is not prime.
21 *is* semi-prime — the factors of 21 are 1, **3**, **7**, 21. If we exclude 1 and 21, we are left with 3 and 7, both of which are Prime.

RSA Key Generation:

- To acquire such keys, there are five steps:

- **Select two Prime Numbers: P and Q**
- This really is as easy as it sounds. Select two prime numbers to begin the key generation. For the purpose of our example, we will use the numbers **7** and **19**, and we will refer to them as **P** and **Q**.

- **Calculate the Product: (P*Q)**
- We then simply multiply our two prime numbers together to calculate the product:
- 7 * 19 = **133**
- We will refer to this number as **N**. Bonus question: given the terminology we reviewed above, what kind of number is N?

Calculate the Totient of N: (P-1)*(Q-1)

- To attain the Totient on a Semi Prime number is to calculate the product of one subtracted from each of its two prime factors. Or more simply stated, to calculate the Totient of a Semi-Prime number, calculate P-1 times Q-1.

Applied to our example, we would calculate:

- (7-1)*(19-1) = 6 * 18 = **108**

We will refer to this as **T** moving forward.

Select a Public Key

The Public Key is a value which must match three requirements:

- It must be Prime
- It must be less than the Totient
- It must NOT be a factor of the Totient

Select a Private Key:

- Finally, with what we have calculated so far, we can select our Private Key (which we will call **D**).The Private Key only has to match one requirement: The Product of the Public Key and the Private Key when divided by the Totient, must result in a remainder of 1. Or, to put it simply, the following formula must be true:

- (D*E) MOD T = 1

- There are a few values that would work for the Private Key as well. But again, for the sake of our example, we will select **41**. To test it against our formula, we could calculate: (41*29) MOD 108

  We can use a calculator to validate the result. Which means **41** will work as our Private Key.

Diffie-Hellman Key Exchange Algorithm:

- The Diffie-Hellman algorithm will be used to establish a secure communication channel. This channel is used by the systems to exchange a private key. This private key is then used to do symmetric encryption between the two users.

- Diffie-Hellman Algorithm is primarily a protocol that is used for key exchange. Using this interactive protocol two parties will derive a common secret key by communicating each other. The security of Diffie-Hellman algorithm is mainly based on the difficulty of computing the discrete logarithms.

Applications of Diffie Hellman Algorithm:

Many protocol uses Diffie-Hellman algorithm to enhance security and few of them are:

- Secure Shell (SSH)
- Transport Layer Security (TLS) / Secure Sockets Layer (SSL)
- Public Key Infrastructure (PKI)
- Internet Key Exchange (IKE)
- Internet Protocol Security (IPSec)

Limitations of Diffie Hellman Algorithm:

The following are the limitations of Diffie-Hellman algorithm:

- Lack of authentication procedure.
- Algorithm can be used only for symmetric key exchange.
- As there is no authentication involved, it is vulnerable to man-in-the-middle attack.
- As it is computationally intensive, it is expensive in terms of resources and CPU performance time.
- Encryption of information cannot be performed with the help of this algorithm.
- Digital signature cannot be signed using Diffie-Hellman algorithm.

Public Key Infrastructure:

- PKIs are complex distributed systems that are responsible for giving users enough information to make reasonable trust judgments about one another.

- While there are a number of metrics we can use to reason about PKIs, one measure stands out: we say a PKI is correct if it allows Alice to conclude about Bob what she should, and disallows her from concluding things she should not.

- PKI designers need tools which can accurately evaluate the correctness of their designs and clearly illustrate what types of trust judgments their systems enable.

Block chain uses public-key cryptography:

- Technically, both of those use public-key encryption; however, encryption of real-world files, that is, files over a couple of hundred bytes in size, requires the more ancient form of cryptography called symmetric cryptography, where the encryption key is the same as the decryption key.

- Therefore to share an encrypted file with others, encrypt the information along with symmetric key using receipt's public key.

- Then, only the recipient has the key to decrypt the file. Thus you can send both the encrypted file and the key to decrypt it over the open internet, and no one but the recipient will be able to decrypt the file.

Real time business applications for public-key cryptography are:

- Digital signatures - content is digitally signed with an individual's private key and is verified by the individual's public key.

- Encryption - content is encrypted using an individual's public key and can only be decrypted with the individual's private key.

Confidentiality, Integrity and Availability:

Confidentiality:

- In simple terms, confidentiality means something that is secret and is not supposed to be disclosed to unintended people or entities.
- Confidentiality ensures that sensitive information is accessed only by an authorized person and kept away from those not authorized to possess them.
- Everyone has information which they wish to keep secret. Thus Protecting such information is an important part of information security.

Integrity:

- In the context of the information security (InfoSec) world, integrity means that when a sender sends data, the receiver must receive exactly the same data as sent by the sender.

Example attacks that affect Integrity:

- Salami attack
- Data diddling attacks
- Session hijacking
- Man-in-the-middle (MITM) attack

Real Time Application:

Encryption in WhatsApp:

- WhatsApp uses the 'signal' protocol for encryption, which uses a combination of asymmetric and symmetric key cryptographic algorithms.

- The symmetric key algorithms ensure confidentiality and integrity whereas the asymmetric key cryptographic algorithms help in achieving the other security goals namely authentication and non-repudiation.

- In symmetric key cryptography a single key is used for encryption of the data as well as decryption. In asymmetric key cryptography there would be two separate keys.

Encryption in Instagram:

- The interaction with Instagram is likely an encrypted communication. When the phone requests data with Instagram, it will use SSL/TLS over port 443 to encrypt requests from Instagram servers and will send data over the same encrypted data stream.

- This prevents malicious parties from eavesdropping on the conversation between the user and instagram.

Real Time Application of RSA:

- Real-time is a bit ill defined. It can range from “not batch oriented” to “system must respond within 15 microseconds or less”.

- For soft real-time applications of RSA, one could cite https which often uses the RSA algorithm among others to perform public key cryptography between the server and the browser.

- For harder real-time applications such as embedded systems (think IoT in industry or smart cars) one would probably not chose RSA as the key generating step is quite resource heavy as it relies on

- 1. finding a huge number and
- 2. making sure that this number is (most likely) a prime number.
- 3. If 2. returns false, restarting with 1.

UNIT III

Authentication

Objectives:

This course is to discuss

- Hash Function
- Message Authentication Code
- MD5
- Authentication Protocol
- Digital Signature

Learning Outcomes:

- Use basic security for generating Hash Function.
- Develop basic security enhancements in Message Authentication Code.
- The importance of Authentication Protocol and Digital Signature

Prerequisites:

- Network security is one of the most important computer science issues today.

- It helps businesses meet mandatory compliance regulations, protect customer data, and reduce the risk of legal action.

- Without a secure infrastructure and the expertise to remedy an issue, critical performance functions for users and computer programs may not be executable.

- This course covers the latest practices for building reliable and secure code to defend against various attack techniques, harmful viruses and threats.

Plan for the lecture delivery:

- Teaching aid both Blackboard and Presentation Via LCD
-
- Topic should be start with Definition, System Model as follows:
    - Hash Function
    - Secure Hash Function
    - Message Authentication Code
    - Hash MAC
    - Digital Signature

Definition of Hash Function:

- A hash function converts strings of different length into fixed-length strings. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes. The values are usually used to index a fixed-size table called a hash table.

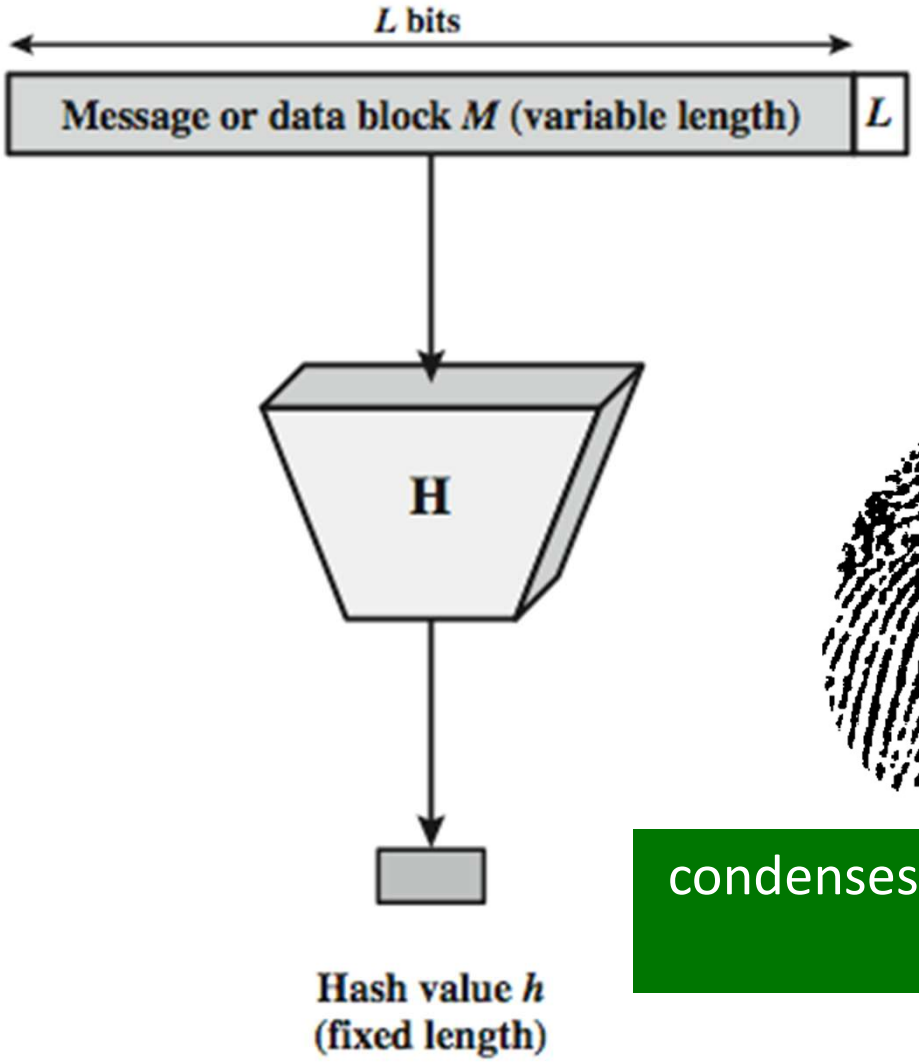
- Hashing can use scramble passwords into strings of authorized characters for example. The output values cannot be inverted to produce the original input.

Real life example of hashing:

- Cryptographic hash functions are very commonly used in password verification.

- Example: When the user access any online website, which requires a user login, that time the user enters his/her own e-mail and password to authenticate that the account has been belongs to authenticated user.

Hash Function

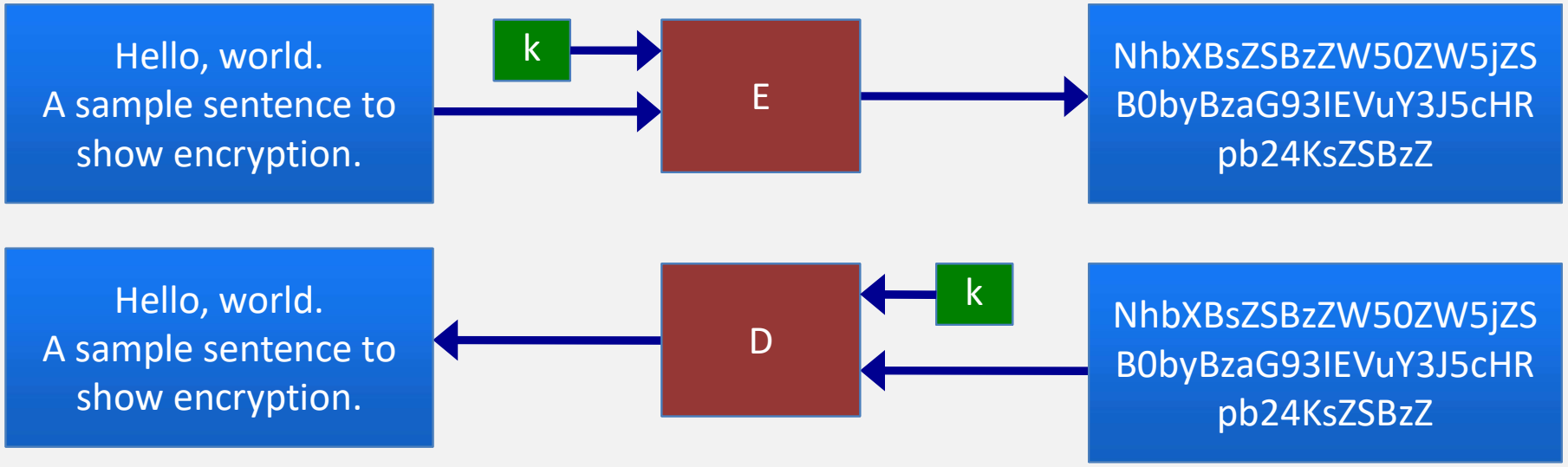


- The hash value represents concisely the longer message
  - may called the *message digest*
- A message digest is as a ``digital fingerprint" of the original document

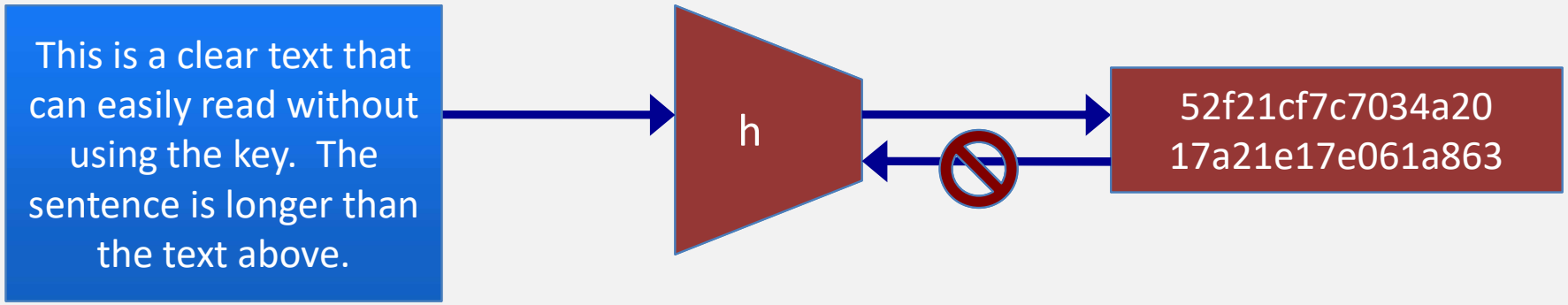
condenses arbitrary message to fixed size

$$h = H(M)$$

Hashing V.S. Encryption



- Encryption is two way, and requires a key to encrypt/decrypt



- Hashing is one-way. There is no 'de-hashing'

Hash Function – Applications:

Used Alone

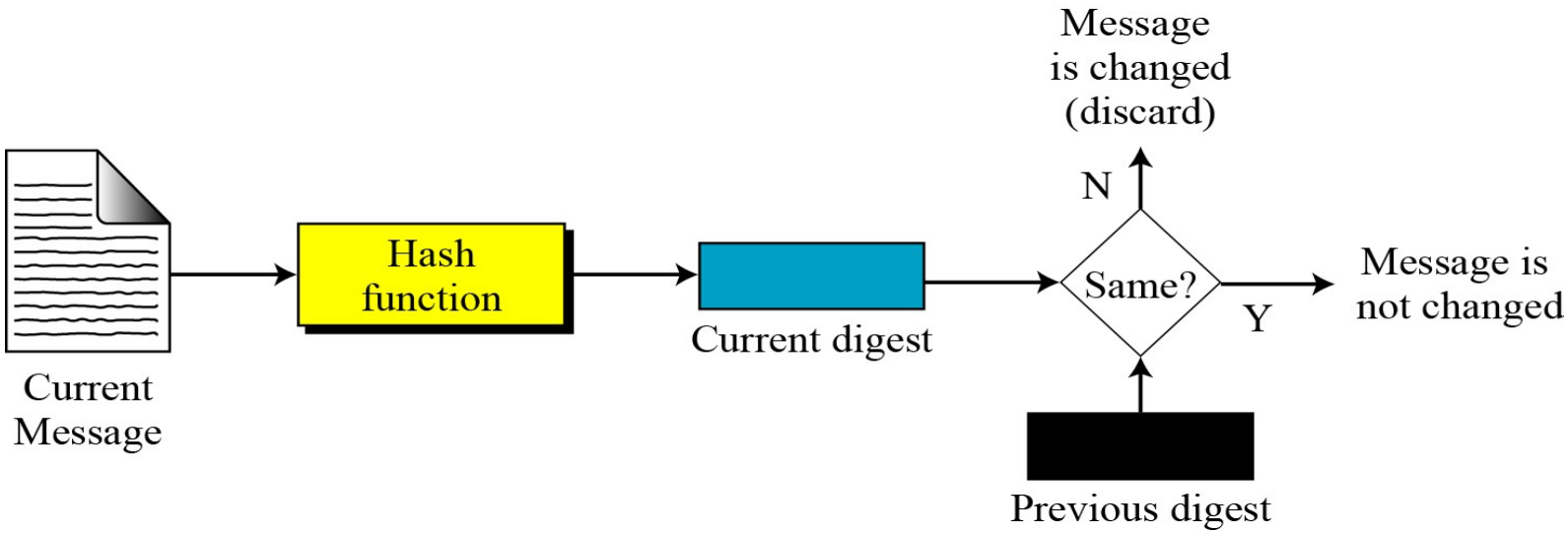
- Fingerprint -- file integrity verification, public key fingerprint
- Password storage (one-way encryption)

Combined with encryption functions

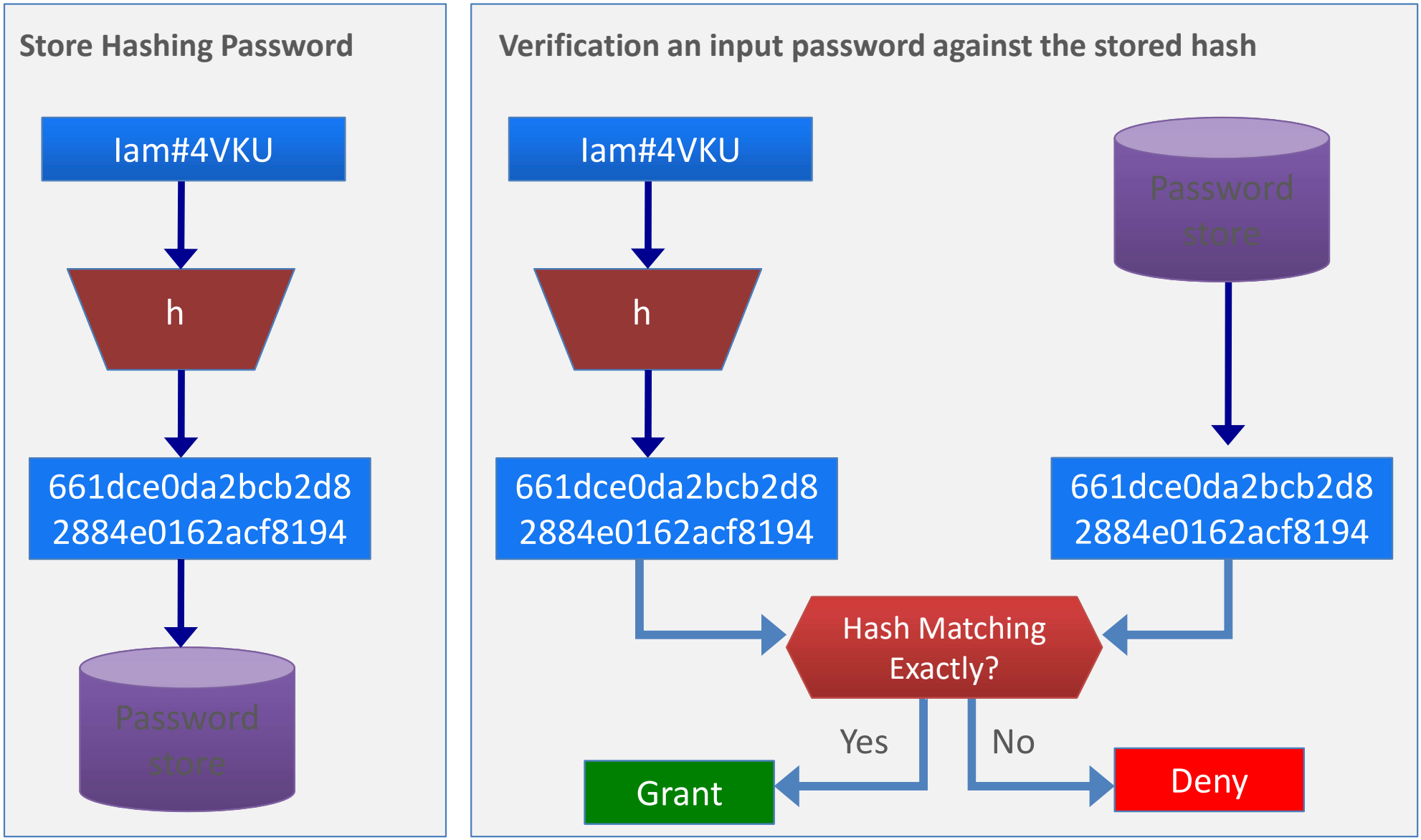
- Hash based Message Authentication Code (HMAC)
  - protects both a message's integrity and confidentaility
- Digital signature
  - Ensuring Non-repudiation
  - Encrypt hash with private (signing) key and verify with public (verification) key

Integrity:

- to create a one-way password file
  - store hash of password not actual password
- for intrusion detection and virus detection
  - keep & check hash of files on system

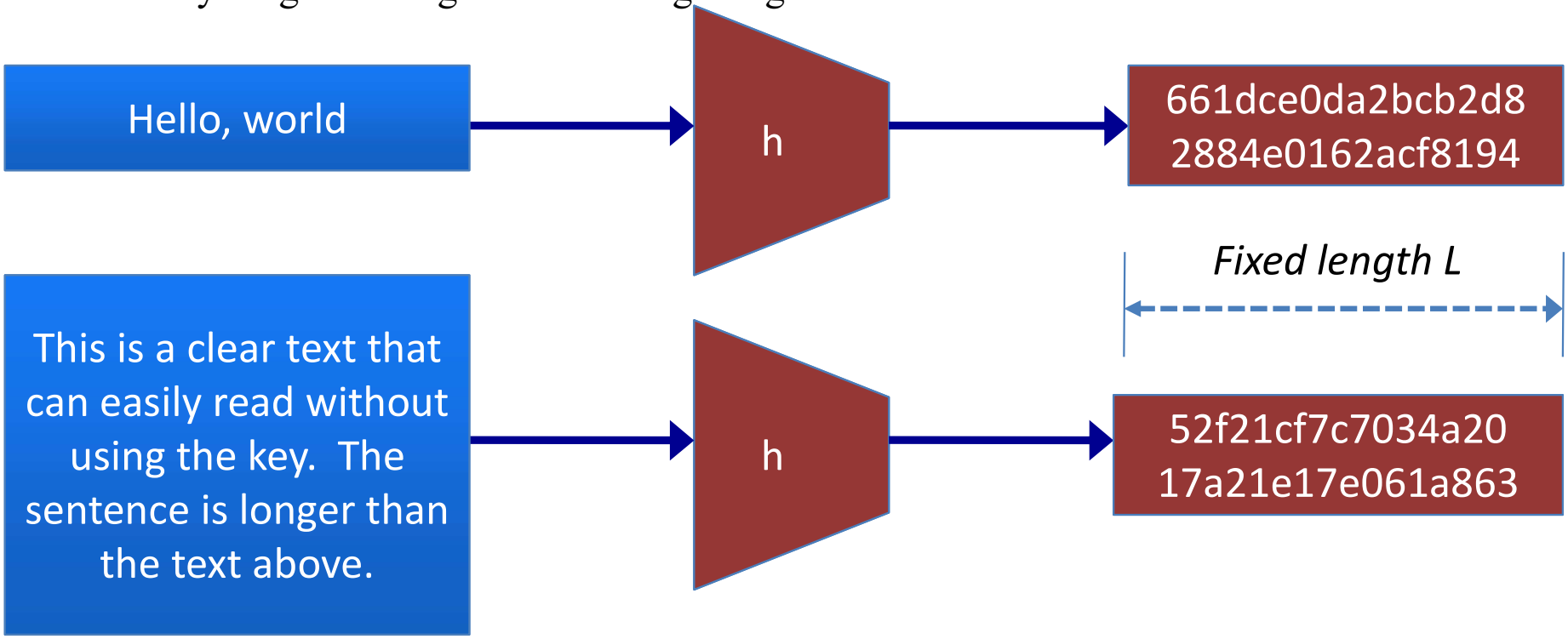


Password Verification



Properties : Fixed length

- Arbitrary-length message to fixed-length digest

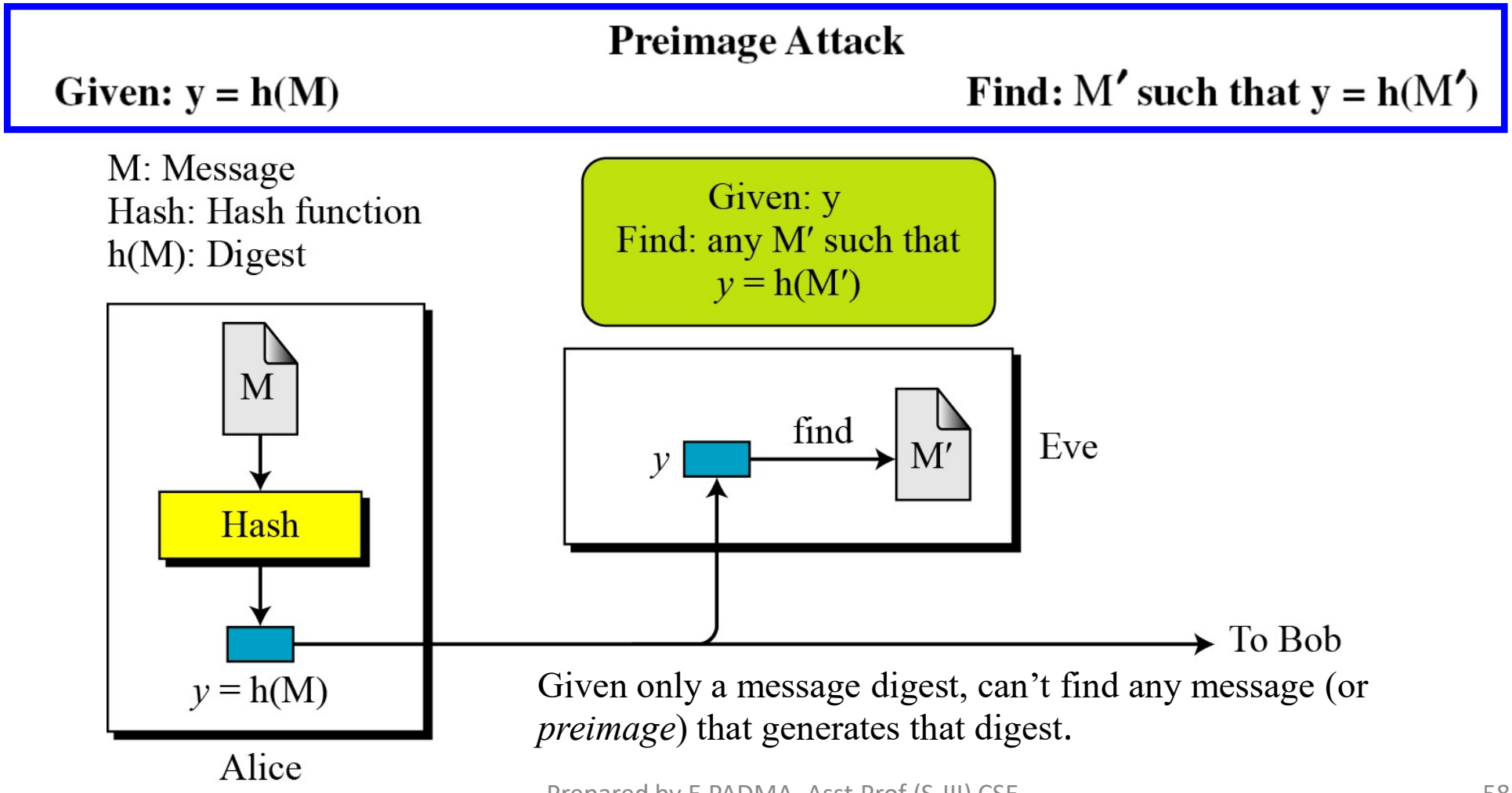


Properties of a Hash Function:

- Pre-image
- Second Pre-image
- Collision Resistant

Preimage resistant

- Preimage resistant measures how difficult to devise a message which hashes to the known digest and it must be one-way.

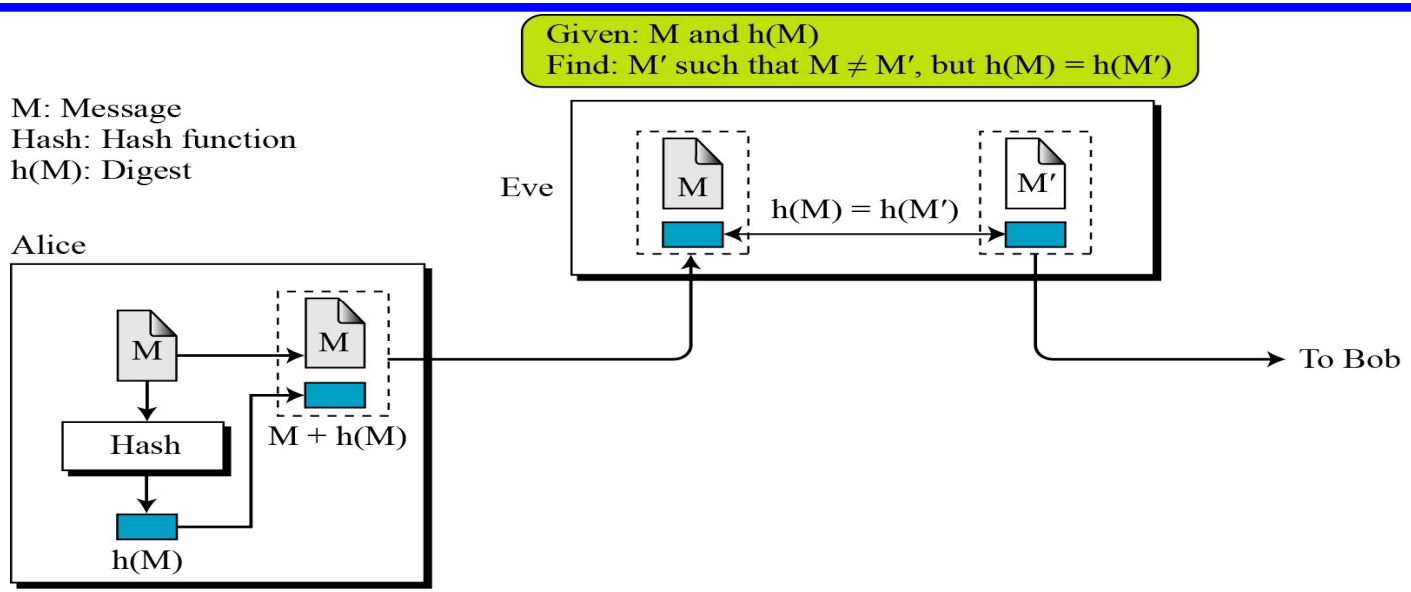


Second preimage resistant

- The second resistant measures how difficult to devise a message which hashes to the known digest and its message

Second Preimage Attack

Given: M and h(M) **Find: M′ ≠ M such that h(M) = h(M′)**



- Given one message, can't find another message that has the same message digest. An attack that finds a second message with the same message digest is a *second pre-image* attack.
  - It would be easy to forge new digital signatures from old signatures if the hash function used weren't second preimage resistant

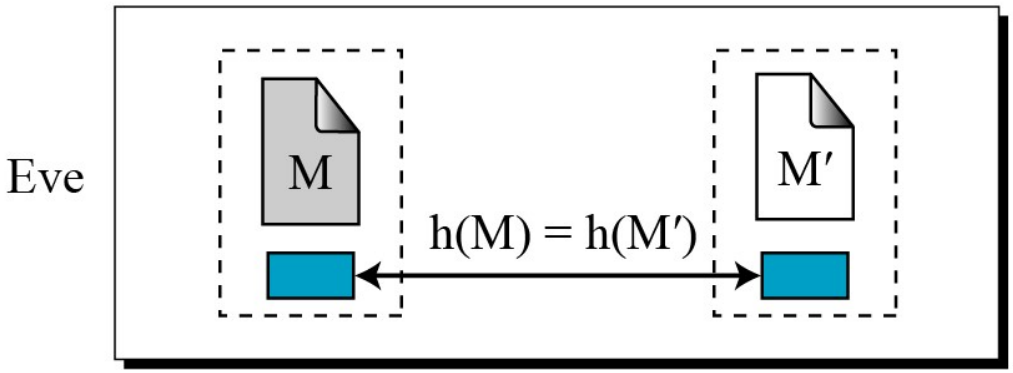
Collision Resistant

Collision Attack

Given: none **Find: M′ ≠ M such that h(M) = h(M′)**

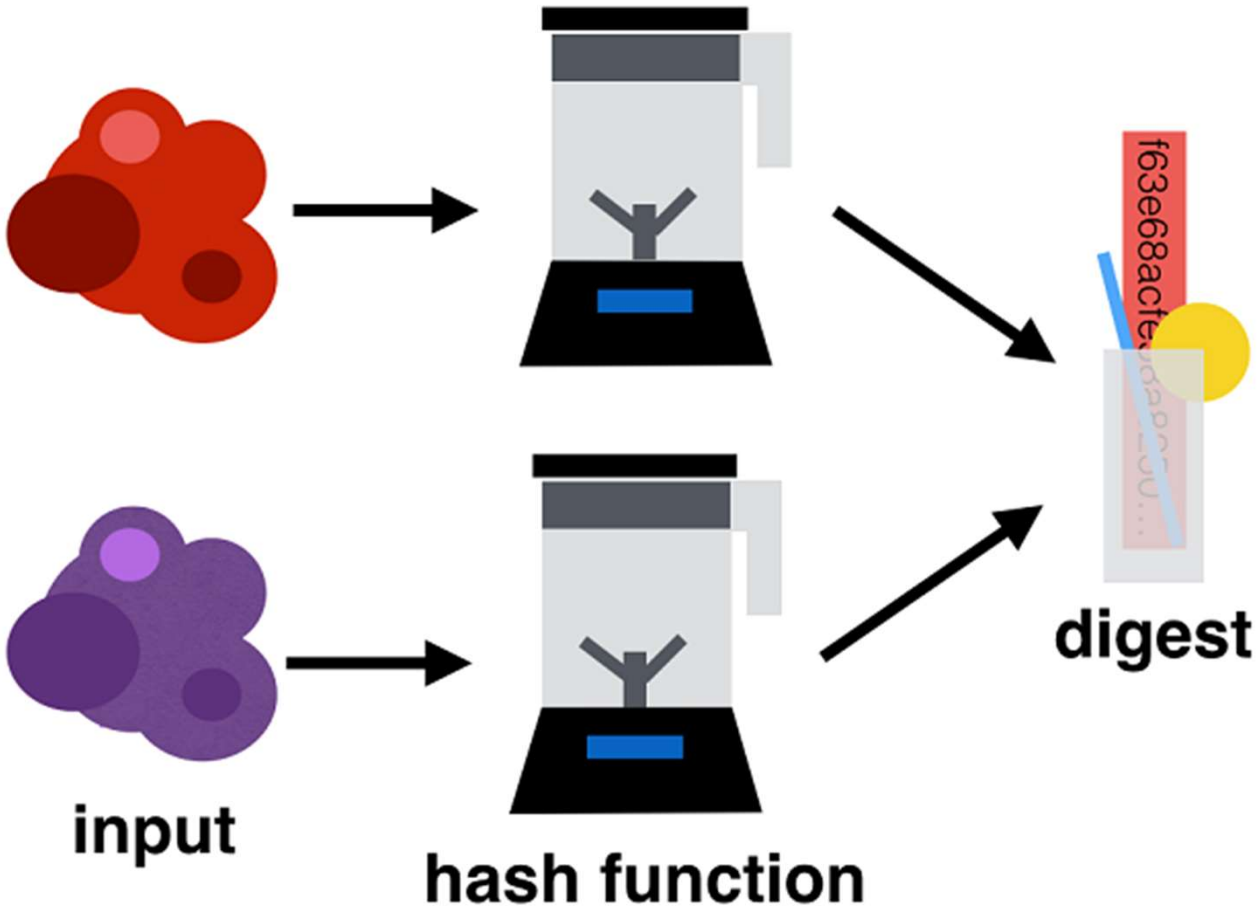
M: Message
Hash: Hash function
h(M): Digest

Find: M and M′ such that M ≠ M′, but h(M) = h(M′)

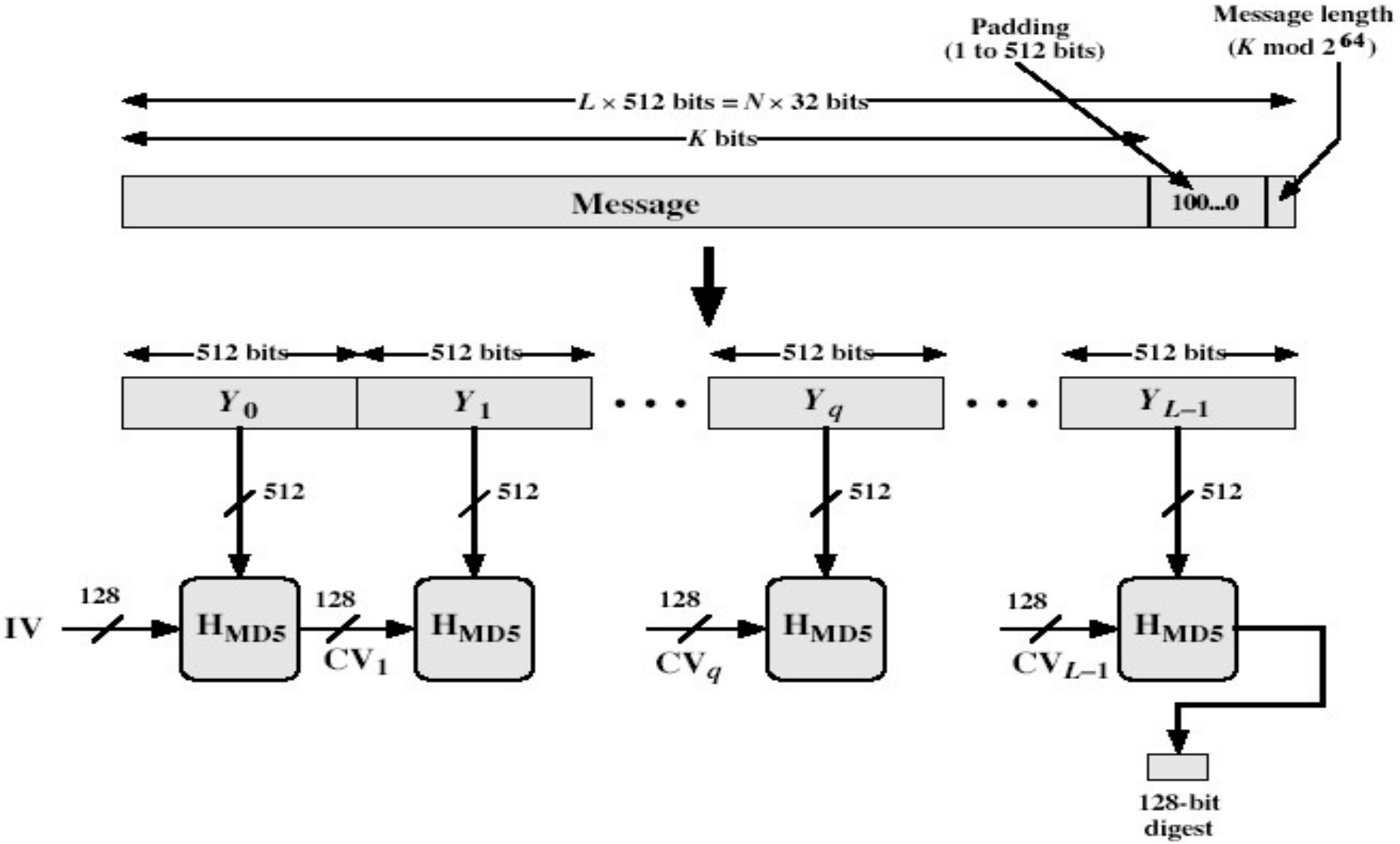


Can't find any two different messages with the same message digest

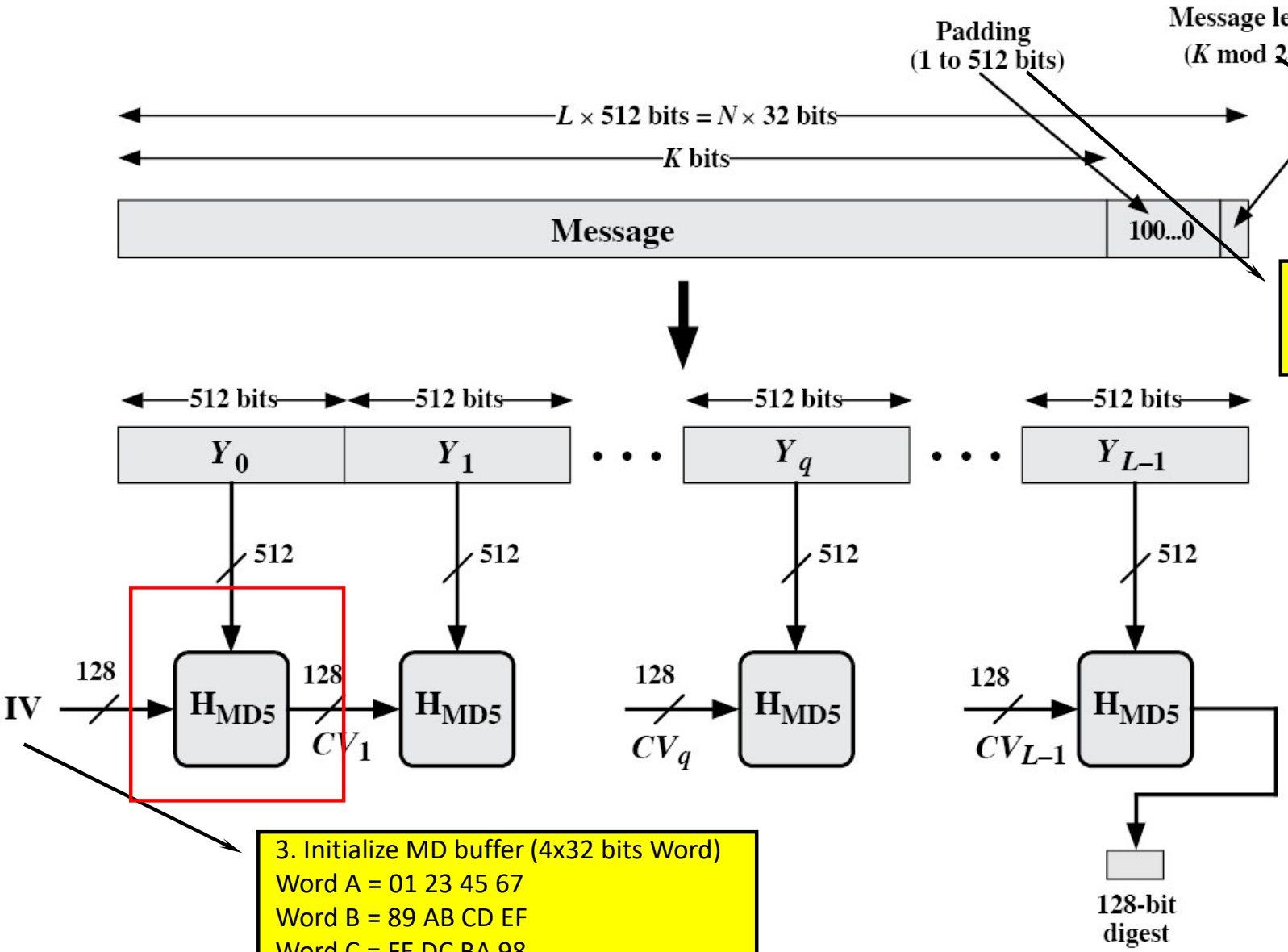
- Collision resistance implies second preimage resistance
- Collisions, if we could find them, would give signatories a way to repudiate their signatures


input
hash function
digest

MD5 Overview

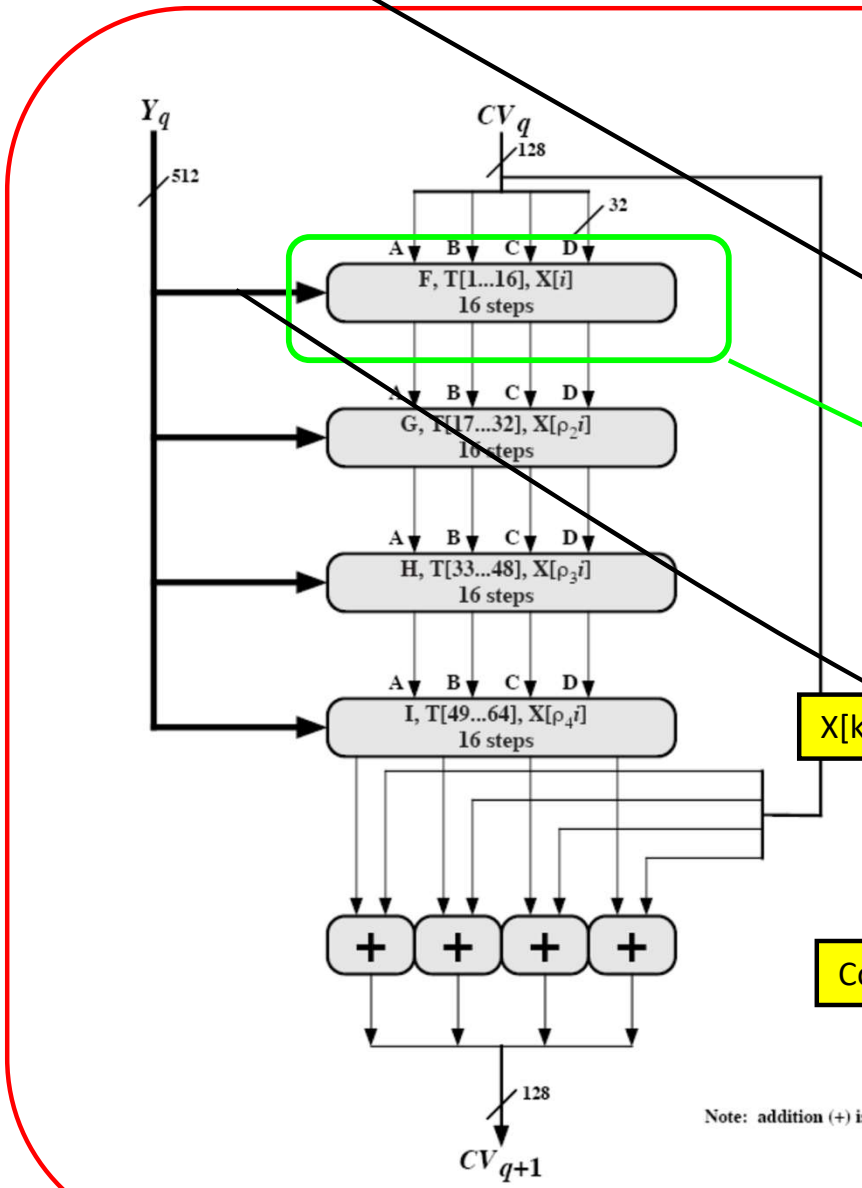


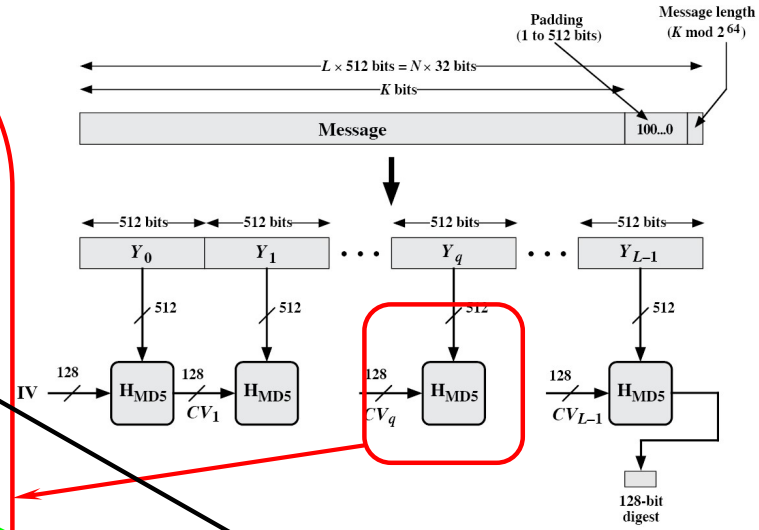
MD5 Overview



Hash Algorithm Design – MD5

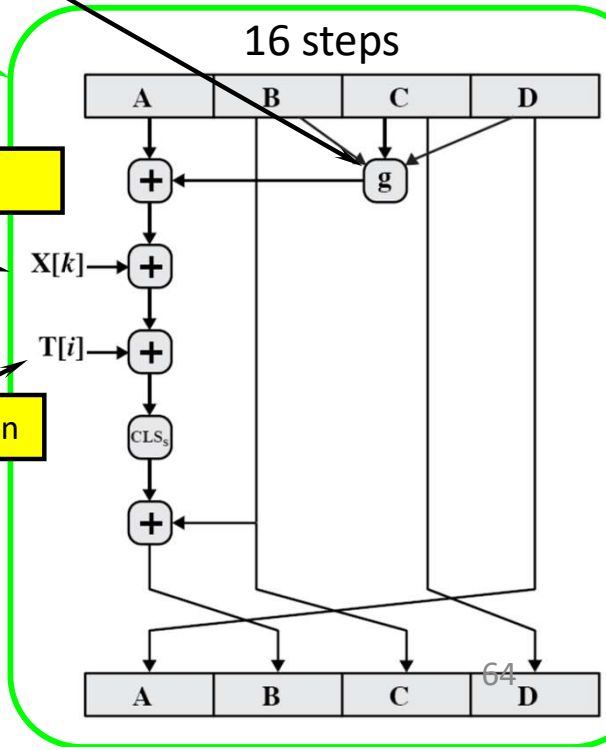
b	c	d	F	G	H	I
0	0	0	0	0	0	1
0	0	1	1	0	1	0
0	1	0	0	1	1	0
0	1	1	1	0	0	1
1	0	0	0	0	1	1
1	0	1	0	1	0	1
1	1	0	1	1	0	0
1	1	1	1	1	1	0





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

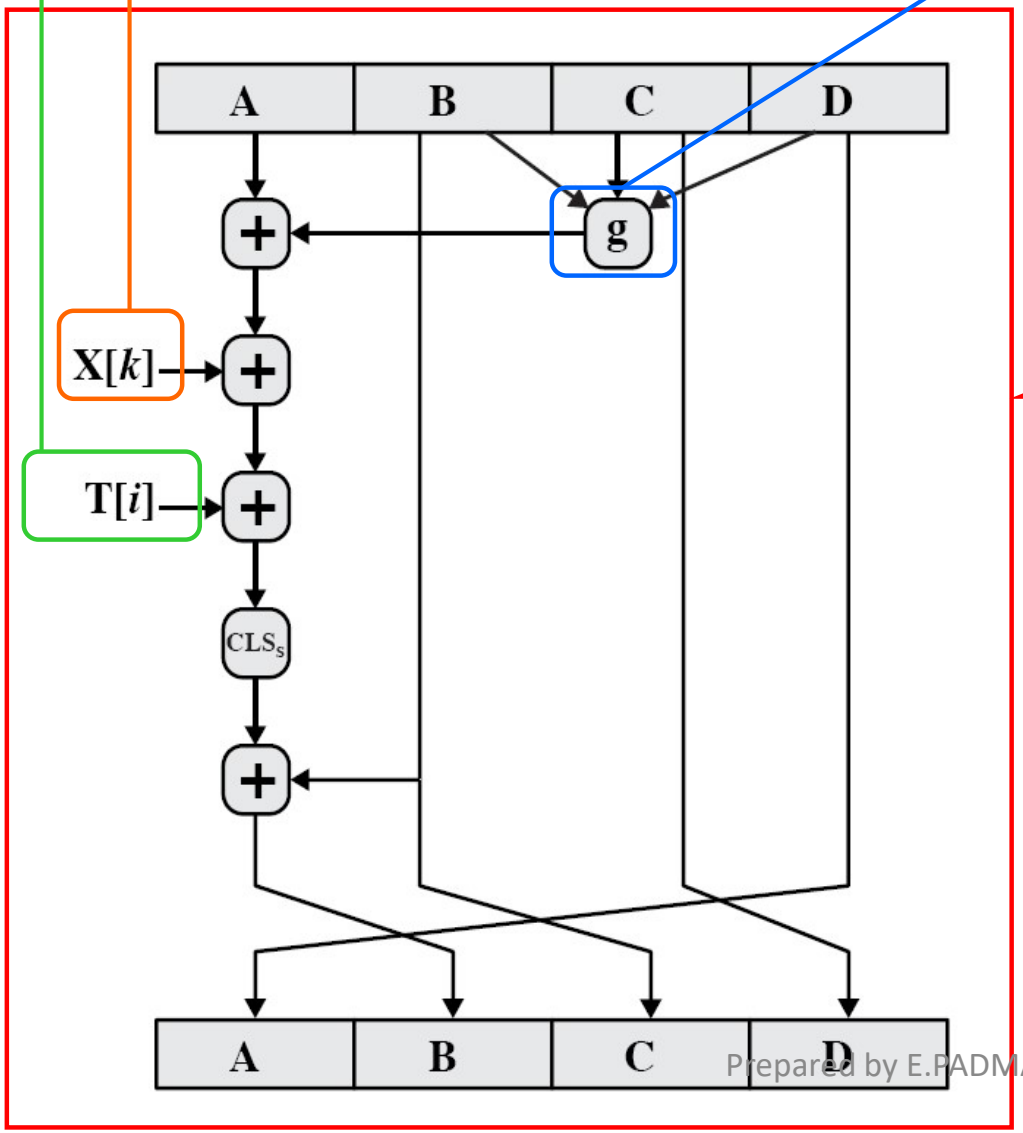
Constructed from sine function



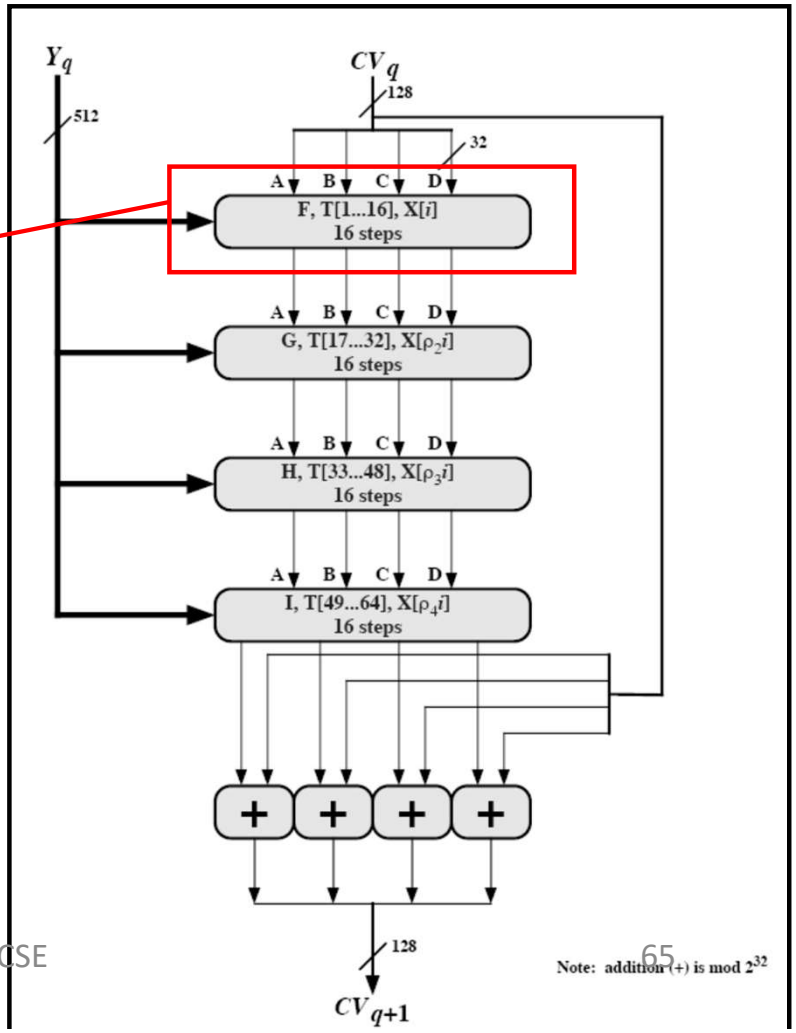
The ith 32-bit word in matrix T, constructed from the sine function

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

$$F(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z)$$
$$G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$$
$$H(X,Y,Z) = X \oplus Y \oplus Z$$
$$I(X,Y,Z) = Y \oplus (X \vee \neg Z)$$



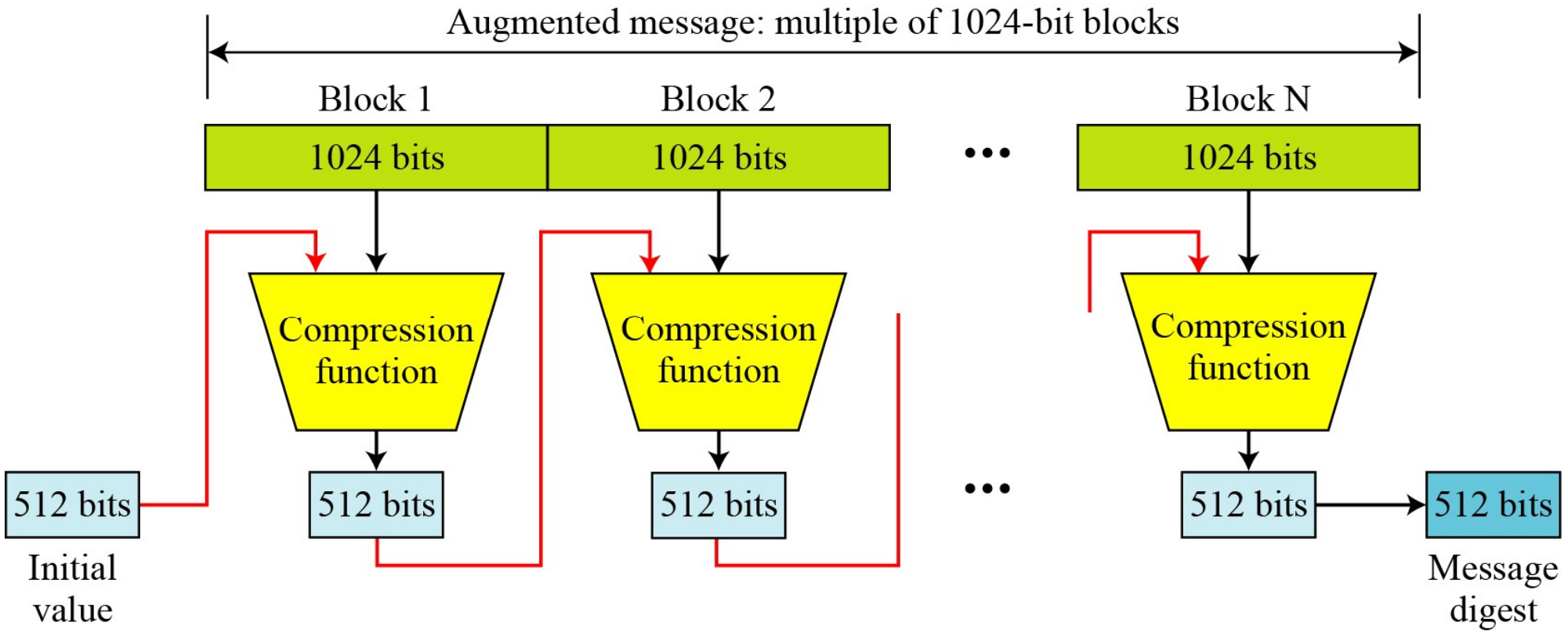
Single step



Secure Hash Algorithm:

- SHA originally designed by NIST & NSA in 1993
  - revised in 1995 as SHA-1
- US standard for use with DSA signature scheme
  - standard is FIPS 180-1 1995, also Internet RFC3174
  - based on design of MD4 with key differences
- produces 160-bit hash values
- recent 2005 results on security of SHA-1 have raised concerns on its use in future applications

SHA-512 Overview



UNIT IV

Authentication Applications

Objectives:

This course is to discuss

- E-mail Security(PGP,S/MIME)
- IPSec
- Key Management with Public Key Cryptography
- Web Security

Learning Outcomes:

- Use basic security tools to enhance email security.
- Develop basic security enhancements in stand-alone applications.
- The importance of Confidentiality and Authentication
- Ways to prevent network attacks and gaps in security policy

Prerequisites:

- Network security is one of the most important computer science issues today.

- It helps businesses meet mandatory compliance regulations, protect customer data, and reduce the risk of legal action.

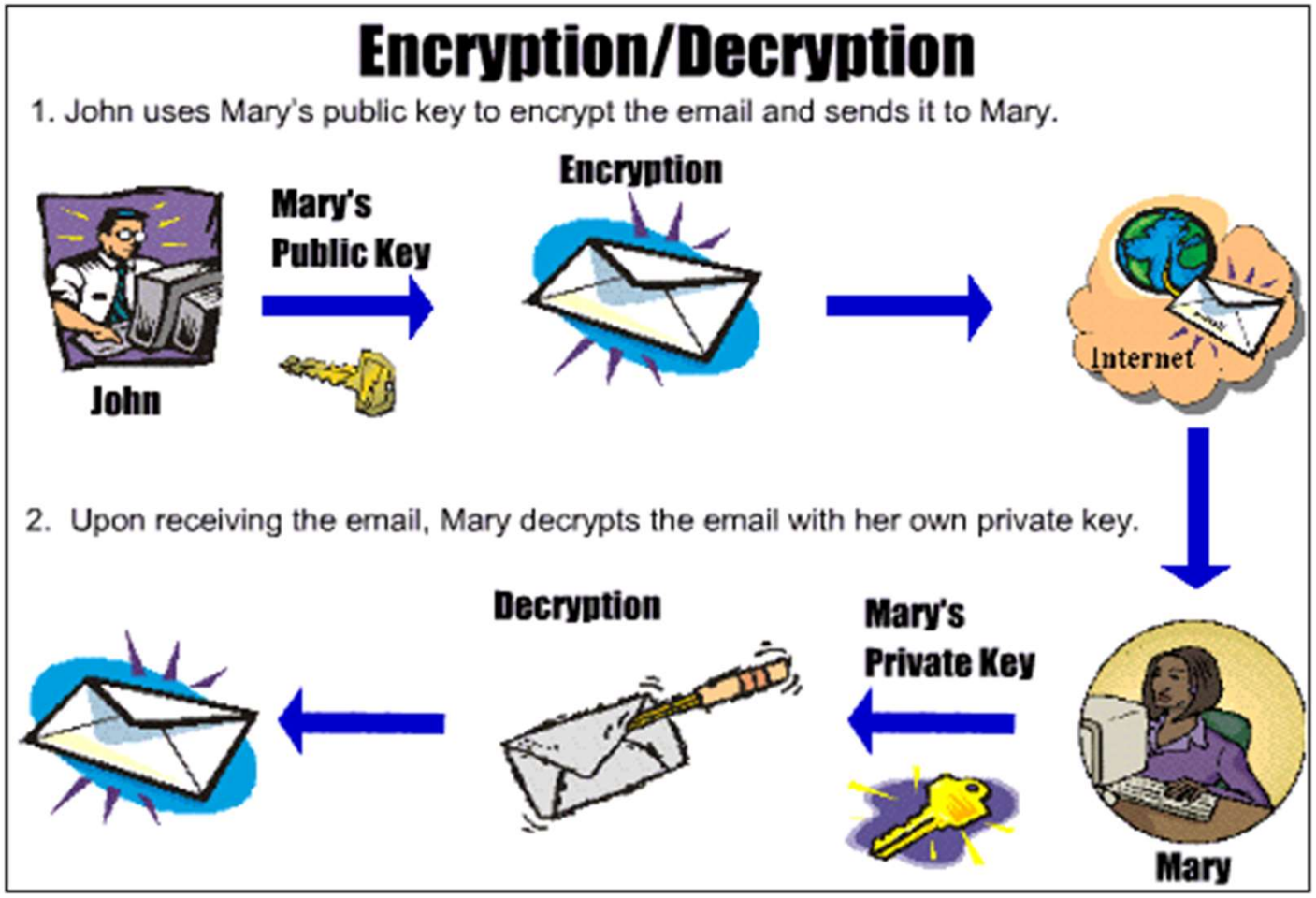
- Without a secure infrastructure and the expertise to remedy an issue, critical performance functions for users and computer programs may not be executable.

- This course covers the latest practices for building reliable and secure code to defend against various attack techniques, harmful viruses and threats.

Plan for the lecture delivery:

- Teaching aid both Blackboard and Presentation Via LCD
- Topic should be start with Definition, System Model as follows:
  - E-mail Security(PGP, S/MIME)
  - IP Security
  - Web Security

E-mail Security:



Working principle of e-mail security:

- Email encryption works by employing something called public key cryptography.
- Each person with an email address has a pair of keys associated with that email address, and these keys are required in order to encrypt or decrypt an email. ...
- This public key cannot be used to decrypt the sent message, only to encrypt it.
- When an email is sent, it is encrypted by a computer using the public key and the contents of the email are turned into a complex, indecipherable scramble that is very difficult to crack.
- This public key cannot be used to decrypt the sent message, only to encrypt it. Only the person with the proper corresponding private key has the ability to decrypt the email and read its contents.

There are various types of email encryption, but some of the most common encryption protocols are:

OpenPGP — a type of PGP encryption that utilizes a decentralized, distributed trust model and integrates well with modern web email clients

S/MIME — a type of encryption that is built into most Apple devices and utilizes a centralized authority to pick the encryption algorithm and key size

Common Security Issues and How to Fix Them:

- Code Injection. Hackers are sometimes able to exploit vulnerabilities in applications to insert malicious code. ...

- Data Breach. The cost of data breaches is well documented. ...
- Malware Infection. ...

- Distributed Denial of Service Attack. ..

- Malicious Insiders.

Confidentiality – Email Security:

Confidentiality:

- In simple terms, confidentiality means something that is secret and is not supposed to be disclosed to unintended people or entities.
- Confidentiality ensures that sensitive information is accessed only by an authorized person and kept away from those not authorized to possess them.
- Everyone has information which they wish to keep secret. Thus Protecting such information is an important part of information security.

Definition of IPSec:

IPSec stands for IP Security.

- It is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality.

- It also defines the encrypted, decrypted and authenticated packets.

IPSec Policy:

- An **IPsec policy** is a set of **rules** that determine which type of IP traffic needs to be secured using **IPsec** and how to secure that traffic.

- Only one **IPsec policy** is active on a computer at one time

Applications of IPSec:

IPsec is a framework of related protocols that secure communications at the network or packet processing layer. It can be used to protect one or more data flows between peers.

IPsec enables data confidentiality, integrity, origin authentication and anti-replay.

IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide **security** for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.

Services of IPSec:

Three security **services** that can be **provided by IPSec** are:

- message confidentiality
- message integrity
- traffic analysis protection.

Benefits of IPSec:

- Traffic within a company or workgroup does not incur the overhead of **security**-related processing.
- IPSec is below the transport layer (TCP, UDP), and is thus transparent to applications.
- There is no need to change software on a user or server system when IPSec is implemented in the firewall or router.

Authentication of IPSec:

- IPSec provides confidentiality, integrity, authenticity, and replay protection through two new protocols.
- These protocols are called Authentication Header (AH) and Encapsulated Security Payload (ESP).
- AH provides authentication, integrity, and replay protection (but not confidentiality).

Definition of Web Security:

- Web Security also known as Cyber Security relates to the securing of websites and servers from online risks.

- It is aimed at safeguarding the sensitive data by restricting, discovering and responding to attacks.

- A web security check informs the user of the online risks and advises solutions to address them. The first step to ensuring safety is by preventing and recognizing the risks.

- Malware virus threats are highly infectious and are capable enough to corrupt your data and damage your network and web security. Malware viruses silently trespass your system and execute lots of malicious activities that make your website and network non-responsive.

Application of Web Security:

- A website security tool scans websites at periodic intervals to find out if there is any questionable activity.

- When a suspicious activity is tracked, the website security tools immediately brings it to the notice of security experts.

- In simple, the website security tools aid in identifying, and removing of malware which is trying to affect or already lying unnoticed on the business website.

UNIT V

Intrusion Detection

Objectives:

This course is to discuss

- Viruses & Related Threats
- Trusted Systems
- Firewall Design Principles

Learning Outcomes:

- Use basic security tools to enhance Trusted System.
- Develop basic security enhancements in stand-alone applications.
- The importance of Confidentiality and Integrity
- Ways to prevent network attacks and gaps in security policy

Plan for the lecture delivery:

- Teaching aid both Blackboard and Presentation Via LCD
- Topic should be start with Definition, System Model as follows:
  - Virus Countermeasures
  - Trusted System
  - Firewall

Virus: A microorganism that is smaller than a bacterium that cannot grow or reproduce apart from a living cell.

Examples of viral illnesses range from the common cold, which can be caused by one of the rhinoviruses, to AIDS, which is caused by HIV. Viruses may contain either DNA or RNA as their genetic material.

Electronic threats are usually spread by opening infected email attachments and by downloading infected files.

Destroy or corrupt your files. Send copies of itself to all of your email contacts, potentially infecting them as well. Deactivate your antivirus software.

Threats can be classified into four different categories; direct, indirect, veiled, conditional.

The 8 Most Famous Computer Viruses of All Time:

CryptoLocker. When it comes to malware, ransomware is the new kid on the block. ...

ILOVEYOU. While ILOVEYOU sounds like a cheerful bon mot you might find printed on the inside of a Valentine's Day card, it's actually far, far more sinister than that. ...

MyDoom. ...

Storm Worm. ...

Anna Kournikova. ..

Slammer. ..

Stuxnet.

Data Access Control:

- Access matrix - An entity capable of accessing objects, the concept of subject associate with that of process (e.g. Application soft, e.g. read, write, execute)

- Access control list - Decomposition of the matrix by columns.

  One process , many program. E.g. CD Writer is one process in which writing is one program and data verification of write data is second program.

- Capability list - Decomposition of the matrix by rows A capability list specifies authorized objects and operations for a user.

A system that can provide such verifications (properties) is referred to as a trusted system

Concept of Trusted Systems :

- Reference Monitor is Controlling element in the hardware and operating system of a computer that regulates the access of subjects to objects on basis of security parameters. Multilevel security for a data processing system.

- The Reference monitor has access to a file (security kernel database) – The monitor enforces the security rules (no read up, no write down)

  No read up: A subject can only read an object of less or equal security level (Simple Security Property)

  No write down: A subject can only write into an object of greater or equal security level

Real time example – Trusted System:

Trusted Systems – Protection of data and resources on the basis of levels of security.

(e.g. military) – In military, information is categorize as unclassified , confidential , secret , top secret .

– Users can be granted clearances to access certain categories of data.

Multilevel security – In which a subject at high level may not convey information to a subject at low level

- Real Time Operating System (RTOS) had emerged in the market for the past few decades to provide solutions over various platforms that range from embedded devices to more sophisticated electronic system such nuclear plant and spacecraft.

- The evolution of the design of operating systems continues to endure the need of diverse applications that run on various platforms.

Properties of the Reference Monitor :

- Complete mediation: Security rules are enforced on every access
- Isolation: The reference monitor and database are protected from unauthorized modification
- Verifiability: The reference monitor's correctness must be provable (mathematically)

– i.e. it is possible to demonstrate mathematically that the reference monitor enforce the security rules and provides complete mediation and isolation.

Definition of Firewall:

- A choke point of control and monitoring interconnects networks with differing trust imposes restrictions on network services

  only authorized traffic is allowed auditing and controlling access
  can implement alarms for abnormal behavior implement VPNs using IPSec
  must be immune to penetration

Firewall Design Principles:

- Centralized data processing system, with a central mainframe supporting number of directly connected terminals.

- LAN's interconnected PCs and terminals to each other and the mainframe.

- Premises network that consisting of a number of LANs, interconnecting PCs , servers .

- Enterprise – wide network consisting of multiple , geographical distributed premises network interconnected by private WAN

Firewall Techniques for control Access:

Service control : The firewall types of Internet services can be accessed inbound or outbound.

Direction Control: It determines the direction in which particular service request may be initiated and allowed to flow through the firewall.

User Control : Controls access to a service according to which user wants to attempt and access the same. It is typically applied to local user only.

Behavior Control : The user may filter traffic on the basis of IP address. It determines the how particular service are used.

Firewall Limitations:

Firewall cannot protect from attacks bypassing it cannot protect against internal threats

– eg unhappy or plan employees cannot protect against transfer of all virus infected programs or files

Types of Firewalls:

1.Packet filtering router

2.Application level gateways

3.Circuit- level gateways

References:

- Third Edition by William Stallings
- Lecture Slides by Lawrie Brown
- Fifth Edition by William Stallings
- The Concept of Trusted Systems, Cryptography Lecture Notes (faadooengineers.com)

THANK YOU