Cryptography, Digital Signature and Network Security

Compiled By :- Er. Nagendra Karn

What is Cryptography

- Cryptography
  - In a narrow sense
    - Mangling information into apparent unintelligibility
    - Allowing a secret method of un-mangling
  - In a broader sense
    - Mathematical techniques related to information security
    - About secure communication in the presence of adversaries
- Cryptanalysis
  - The study of methods for obtaining the meaning of encrypted information without accessing the secret information
- Cryptology
  - Cryptography + cryptanalysis

BASIC TERMINOLOGIES

- Encryption
  - Encryption is the process of encoding a message so that its meaning is not obvious
- Decryption
  - Decryption is the reverse process, transforming an encrypted message back into its normal, original form
- Cryptosystem
  - A system for encryption and decryption is called a cryptosystem.

BASIC TERMINOLOGIES

- Plaintext
- Cipher text
- Key – key refers to a sequence of symbols or a numerical value used by an algorithm to alter information & making that information secure
- Encryption algorithm
  - The cryptosystem involves a set of rules for how to encrypt the plaintext and how to decrypt the cipher text.
- Cryptanalysis
  - Cryptanalysis is an attempt to break the cipher text.

TECHNIQUES OF CRYPTOGRAPHY

- Substitution Technique
  - Caesar Cipher
  - Monoalphabetic Cipher
  - Playfair Cipher
  - Polyalphabetic Cipher
- Transposition Technique
  - Rail Fence Technique
  - Vernam Cipher(One -time Pads)
  - Simple Columnar Cipher

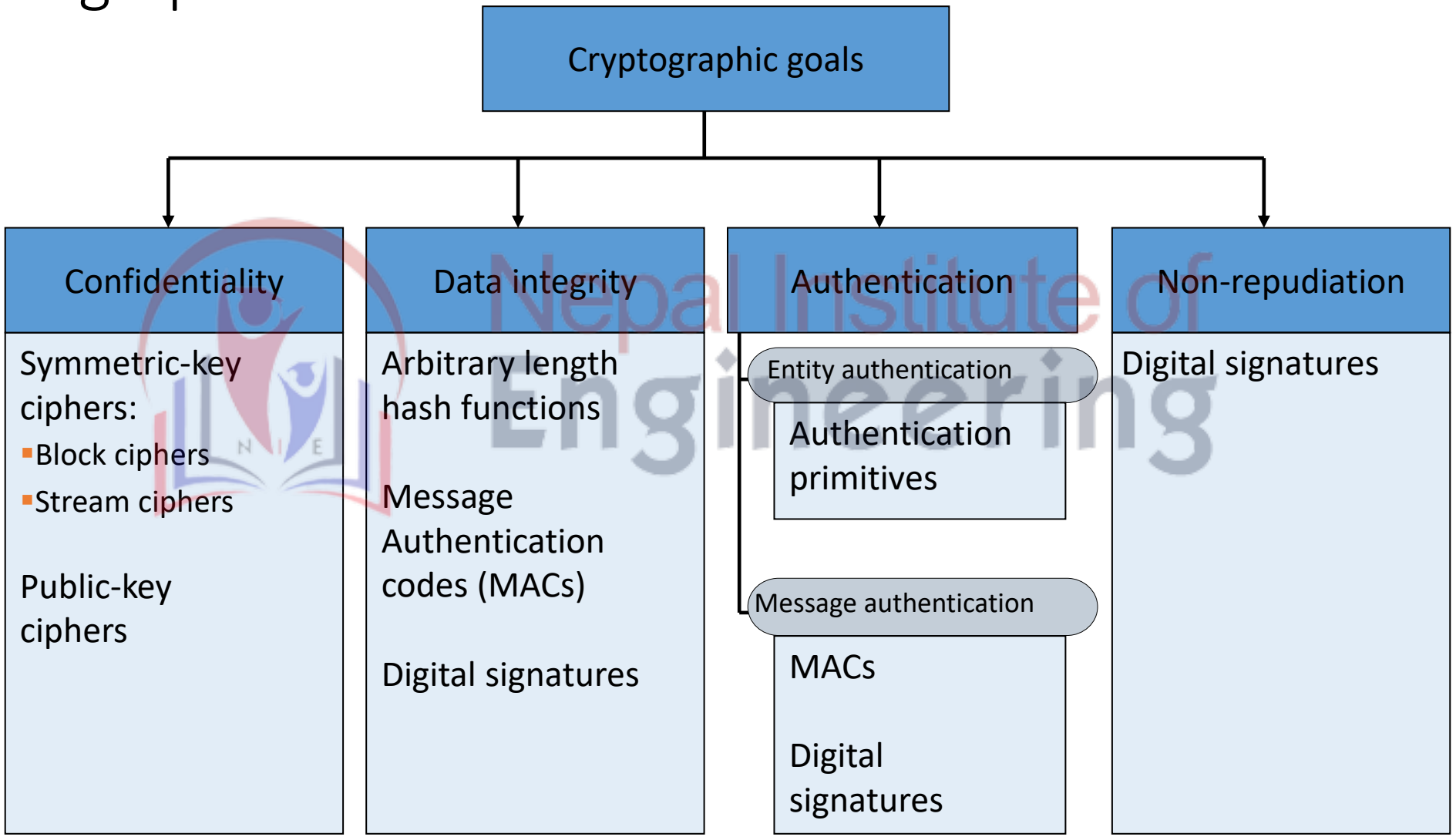
Keys

- Symetric Keys
  - Both parties share the same secret key
  - Problem is securely distributing the key
  - DES - 56 bit key considered unsafe for financial purposes since 1998
  - 3 DES uses three DES keys
- Public/Private keys
  - One key is the mathematical inverse of the other
  - Private keys are known only to the owner
  - Public key are stored in public servers, usually in a X.509 certificate.
  - RSA (patent expires Sept 2000), Diffie-Hellman, DSA

NEED OF ENCRYPTION

- Confidentiality
- Integrity
- Authentication
- Nonrepudiation
- Access Control
- Availability

Cryptographic Goals



ENCRYPTION ALGORITHM

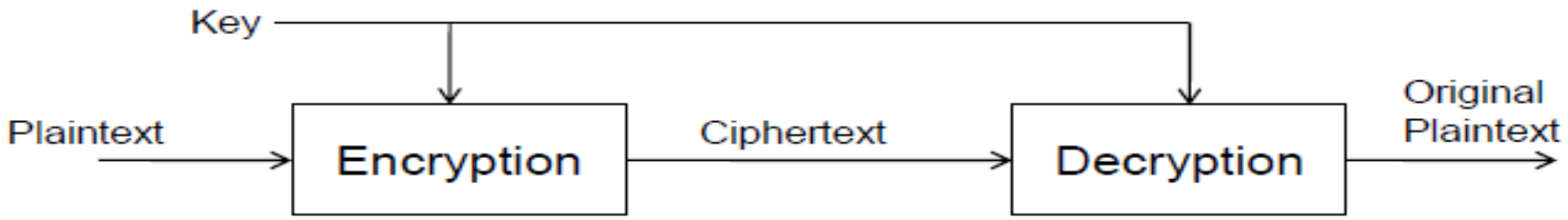
- Symmetric
  - Same key for encryption and decryption
  - Key distribution problem
- Asymmetric
  - Key pairs for encryption and decryption
  - Public and private keys

Cryptography

- Private-Key Cryptography
- Public-Key Cryptography

Private-Key Cryptography

- Secret Key Cryptography
- traditional **private/secret/single key** cryptography uses **one** key
- **shared** by both sender and receiver
- if this key is disclosed communications are compromised
- also is **symmetric**, parties are equal
- hence does not protect sender from receiver forging a message & claiming is sent by sender.
- Single key used for both encrypt & decrypt



Symmetric Cryptosystem

Private-Key/symmetric Cryptography

- Data Encryption Standard (DES):
  - 56 bits key
- Advance Encryption Standard (AES):
  - 128, 192 or 256 bits key
- International Data Encryption Algorithm(IDEA):
  - 128 bits key

DES (Data Encryption Standard)

- Authors: NSA & IBM, 1977

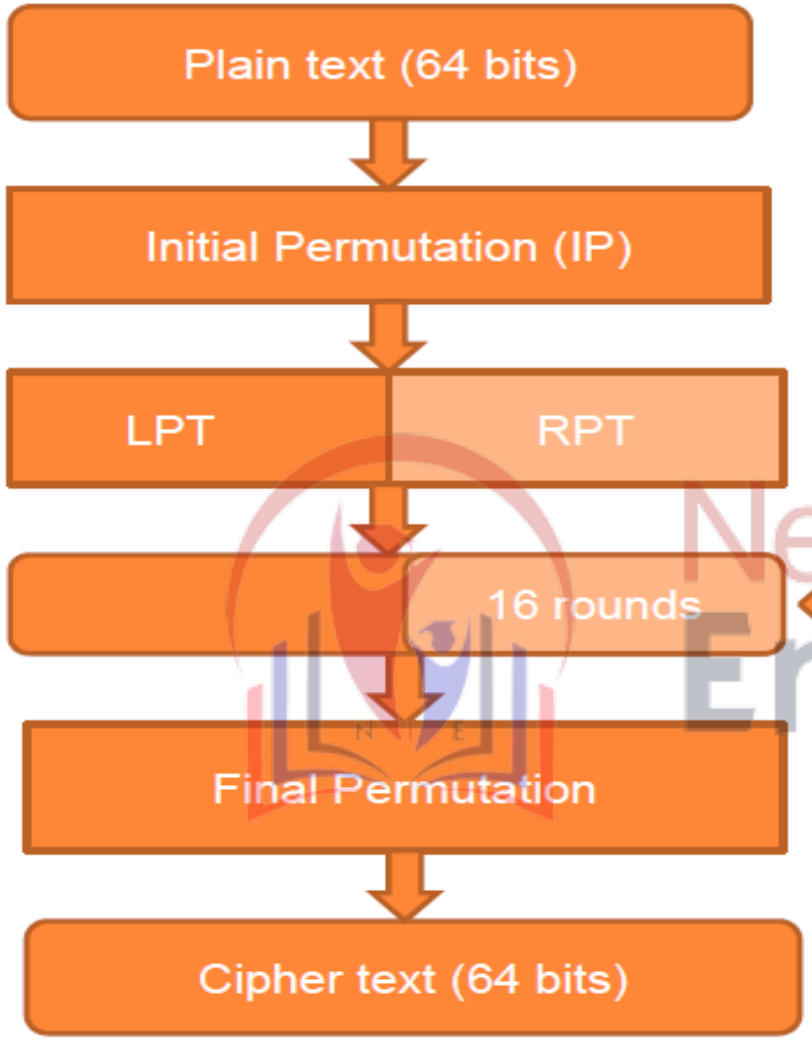
- Data block size: 64-bit (64-bit input, 64-bit output)
- Key size: 56-bit key

- Encryption is fast
  - DES chips
  - DES software: a 500-MIP CPU can encrypt at about 30K octets per second

- Security
  - No longer considered secure: 56 bit keys are vulnerable to exhaustive search

DATA ENCRYPTION STANDARD(DES)

- Developed by IBM and it is known as the Data Encryption Standard
- It is also known as Data Encryption Algorithm
- The DES algorithm is a careful and complex combination of two fundamental building blocks of encryption:
  - Substitution and
  - Transposition
- DES uses only standard arithmetic and logical operations on numbers up to 64 bits long



BROAD LEVEL STEPS IN DES

DATA ENCRYPTION STANDARD

- 1st 64 bit plain text is handed over to initial permutation function.
- IP is performed over the plain text.
- IP produces two halves of the permuted blocks left plain text (LPT) & right plain text (RPT).
- Now LPT & RPT goes 16 rounds of encryption process, each with its own key.
- Now LPT & RPT are rejoined and FINAL PERMUTATION (FP) is performed on the combined block.
- The result is 64 bit cipher text.

Triple-DES (3DES)

- $C = DES_{k3}(DES_{k2}(DES_{k1}(P)))$.

- Data block size: 64-bit
- Key size: 168-bit key; effective key size: 112 (due to man-in-the-middle attack)

- Encryption is slower than DES

- Securer than DES

IDEA (International Data Encryption Algorithm)

- Authors: Lai & Massey, 1991

- Data block size: 64-bit
- Key size: 128-bit

- Encryption is slower than DES
- Security
  - Nobody has yet published results on how to break it

- Having patent protection

AES (Advanced Encryption Standard)

- Authors: Daemen & Rijmen

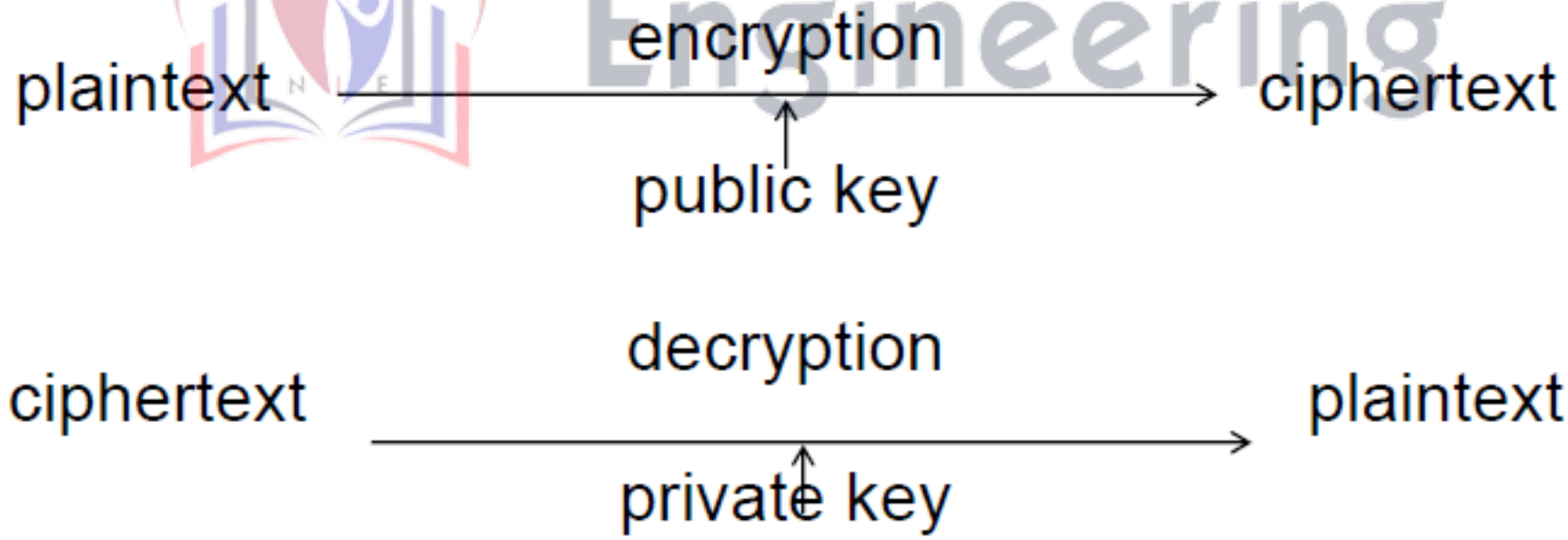
- Block size:128-bit
- Key size: 128-bit, 192-bit, 256-bit

- Encryption is fast

- Security
  - As of 2005, no successful attacks are recognized.
  - NSA stated it secure enough for non-classified data.

Public-Key Cryptography

- probably most significant advance in the 3000 year history of cryptography
- uses **two** keys – a public & a private key
- **asymmetric** since parties are **not** equal
- uses clever application of number theoretic concepts to function
- complements **rather than** replaces private key crypto.



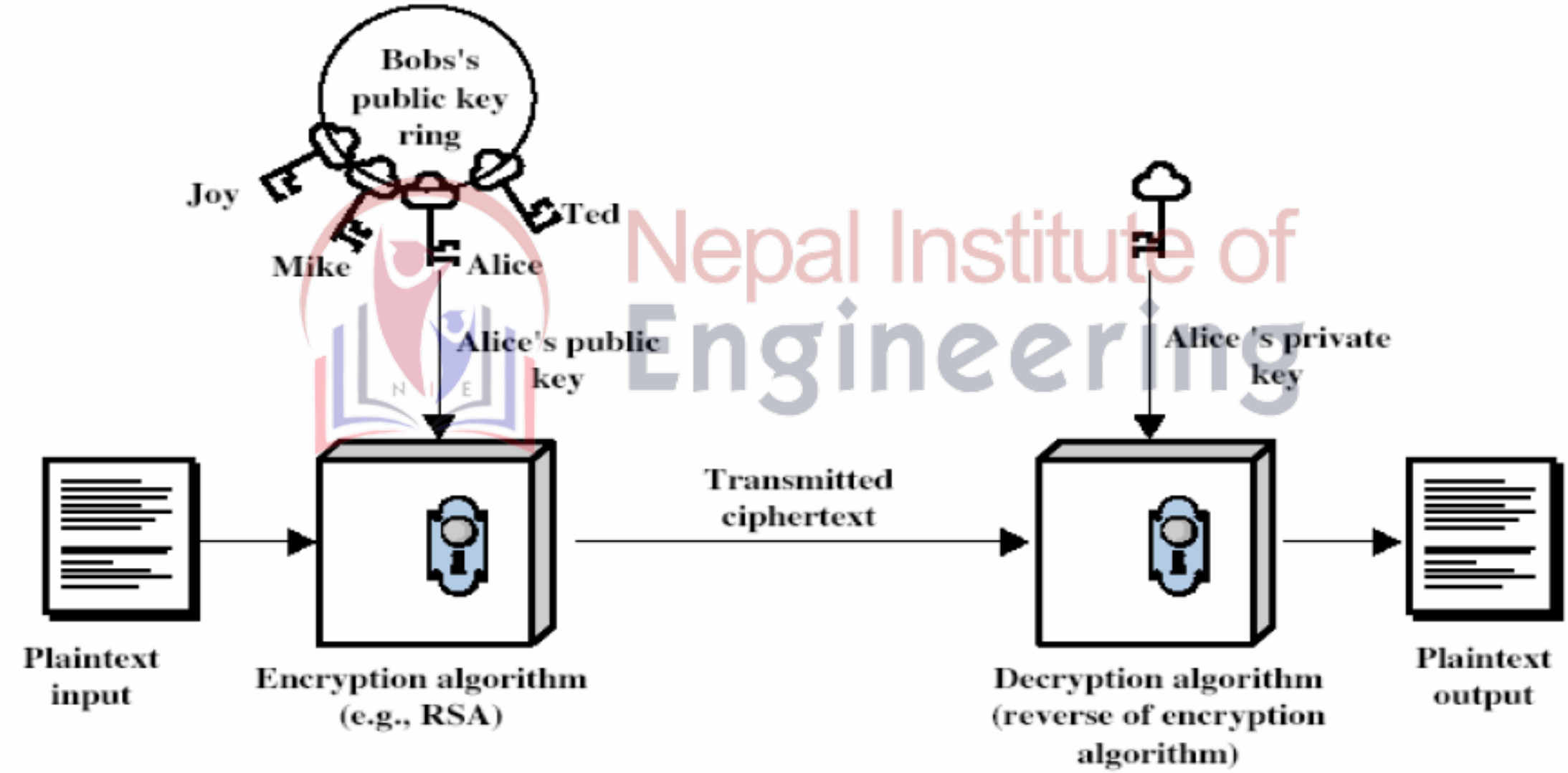
Public-Key Cryptography

- **public-key/two-key/asymmetric** cryptography involves the use of **two** keys:
  - a **public-key**, which may be known by anybody, and can be used to **encrypt messages**, and **verify signatures**
  - a **private-key**, known only to the recipient, used to **decrypt messages**, and **sign** (create) **signatures**
- is **asymmetric** because
  - those who encrypt messages or verify signatures **cannot** decrypt messages or create signatures

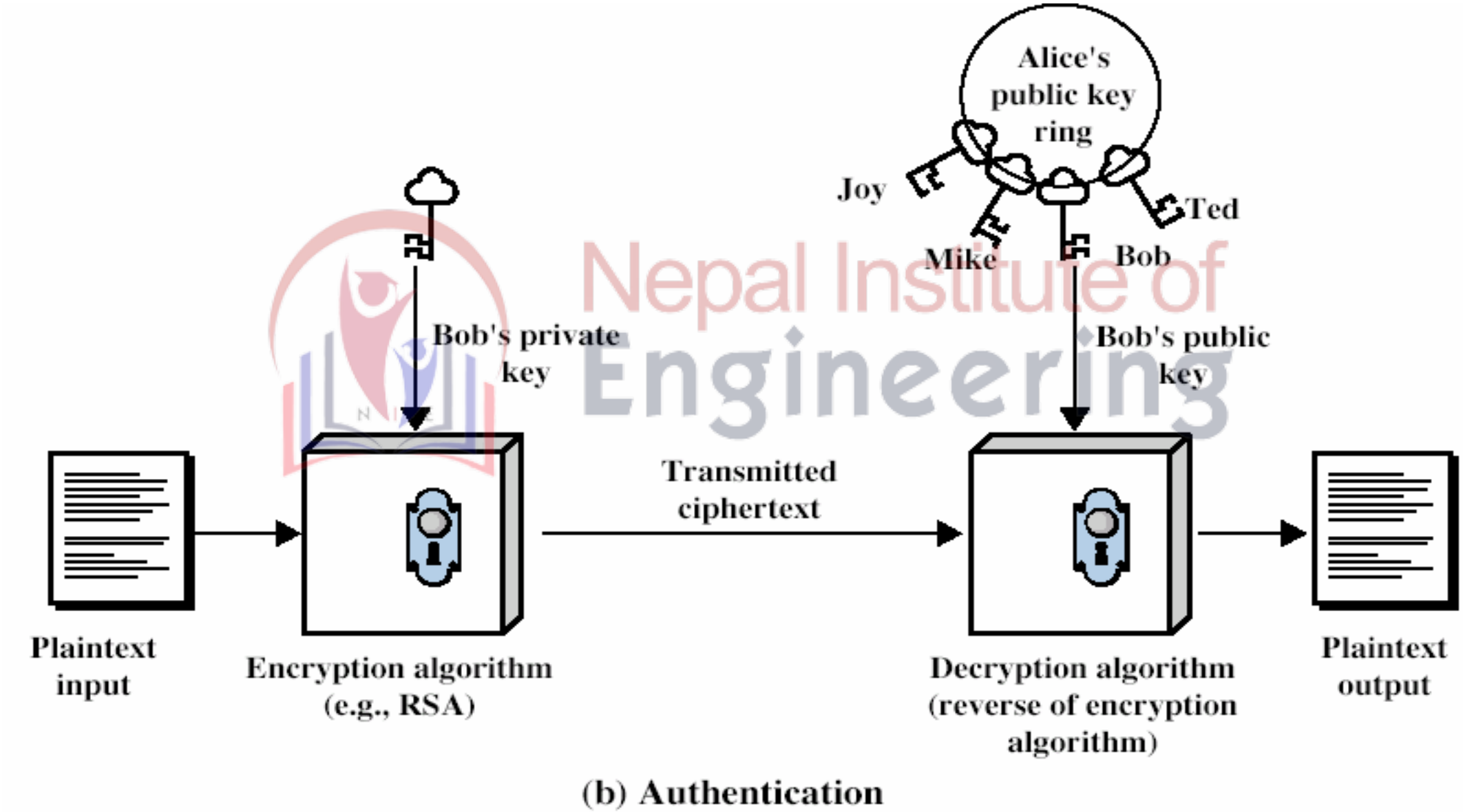
Why Public-Key Cryptography?

- developed to address two key issues:
  - **key distribution** – how to have secure communications in general without having to trust a KDC with your key
  - **digital signatures** – how to verify a message comes intact from the claimed sender
- public invention due to Whitfield **Diffie** & Martin **Hellman** at Stanford Uni in 1976
  - known earlier in classified community

Public-Key Cryptography- Encryption



Public-Key Cryptography- Authentication



(b) Authentication

Conventional Encryption

Needed to Work:

1. The same algorithm with the same key is used for encryption and decryption.
2. The sender and receiver must share the algorithm and the key.

Needed for Security:

1. The key must be kept secret.
2. It must be impossible or at least impractical to decipher a message if no other information is available.
3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.

Public-Key Encryption

Needed to Work:

1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption.
2. The sender and receiver must each have one of the matched pair of keys (not the same one).

Needed for Security:

1. One of the two keys must be kept secret.
2. It must be impossible or at least impractical to decipher a message if no other information is available.
3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

Public-Key Characteristics

- Public-Key algorithms rely on two keys with the characteristics that it is:
- computationally infeasible to find decryption key knowing only algorithm & encryption key
- computationally easy to en/decrypt messages when the relevant (en/decrypt) key is known
- either of the two related keys can be used for encryption, with the other used for decryption (in some schemes)

Public-Key Applications

- can classify uses into 3 categories:
  - **encryption/decryption** (provide secrecy)
  - **digital signatures** (provide authentication)
  - **key exchange** (of session keys)
- some algorithms are suitable for all uses, others are specific to one

Table 9.2 Applications for Public-Key Cryptosystems

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No

Security of Public Key Schemes

- like private key schemes brute force **exhaustive search** attack is always theoretically possible
- but keys used are too large (>512bits)
- security relies on a **large enough** difference in difficulty between **easy** (en/decrypt) and **hard** (cryptanalyse) problems
- more generally the **hard** problem is known, its just made too hard to do in practise
- requires the use of **very large numbers**
- hence is **slow** compared to private key schemes

The RSA Algorithm

- by Rivest, Shamir & Adleman of MIT in 1977
- Based on factoring the product of large prime numbers
- best known & widely used public-key scheme
- RSA has been the subject of extensive cryptanalysis, and no serious flaws have yet been found.
- based on exponentiation in a finite (Galois) field over integers modulo a prime
  - nb. exponentiation takes O((log n)3) operations (easy)
- uses large integers (eg. 1024/2048 bits)
- security due to cost of factoring large numbers
  - nb. factorization takes O(e log n log log n) operations(hard)

The encryption algorithm is based on the underlying problem of factoring large numbers

- RSA Key Setup: each user generates a public/private key pair by:
  - selecting two large primes at random: p, q.
  - computing their system modulus $N=p \times q$
    - note $\phi(N)=(p-1)\times(q-1)$
  - selecting at random the encryption key e
    - where $1<e<\phi(N)$, $\gcd(e,\phi(N))=1$
  - solve following equation to find decryption key d
    - $e\times d=1 \bmod \phi(N)$ and $0\leq d\leq N$
  - publish their public encryption key: $KU=\{e,N\}$
  - keep secret private decryption key: $KR=\{d,p,q\}$.

- to encrypt a message M the sender:
  - obtains **public key** of recipient $KU=\{e,N\}$
  - computes: $C=M^e \mod N$, where $0 \leq M < N$
- to decrypt the ciphertext C the owner:
  - uses their private key $KR=\{d,p,q\}$
  - computes: $M=C^d \mod N$
- note that the message M must be smaller than the modulus N (block if needed).

- RSA Example

1. Select primes: $p=17$ & $q=11$
2. Compute $n = pq = 17 \times 11 = 187$
3. Compute $\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$
4. Select e : $\gcd(e, 160) = 1$; choose $e=7$
5. Determine d: $de = 1 \bmod 160$ and $d < 160$
   Value is $d=23$ since $23 \times 7 = 161 = 10 \times 160 + 1$
6. Publish public key $KU = \{7, 187\}$
7. Keep secret private key $KR = \{23, 17, 11\}$

- sample RSA encryption/decryption is:
  - given message $M = 88$ (nb. $88<187$)
  - encryption:

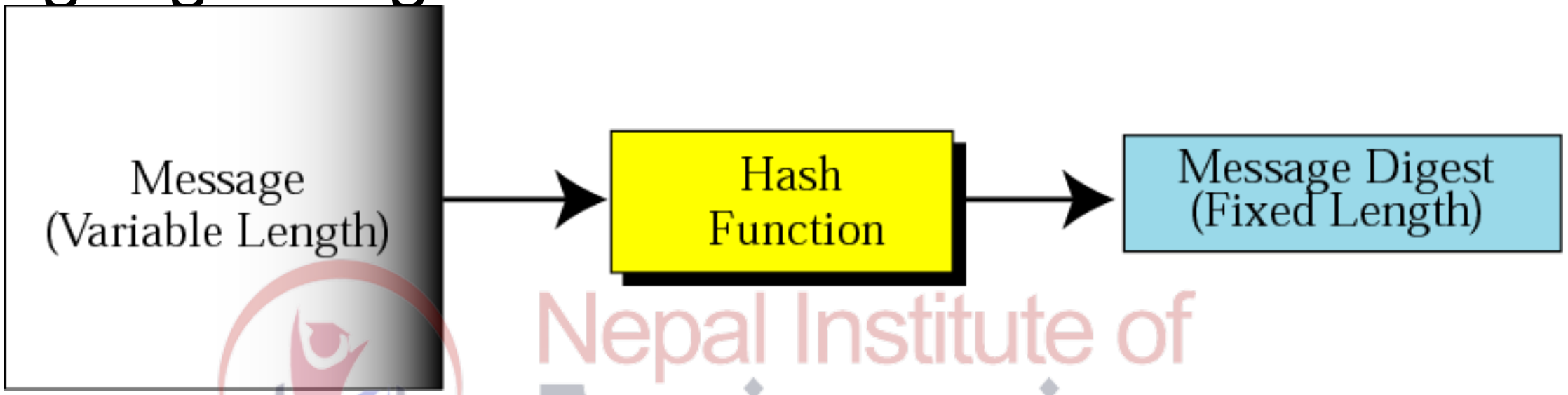
    $C = 88^7 \bmod 187 = 11$
  - decryption:

    $M = 11^{23} \bmod 187 = 88.$

DIGITAL SIGNATURE

- a digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted document to verify its contents and the sender's identity.
- When an author signs a document, it cannot be changed.
- When you send a document electronically, you can also sign it.

Signing the digest

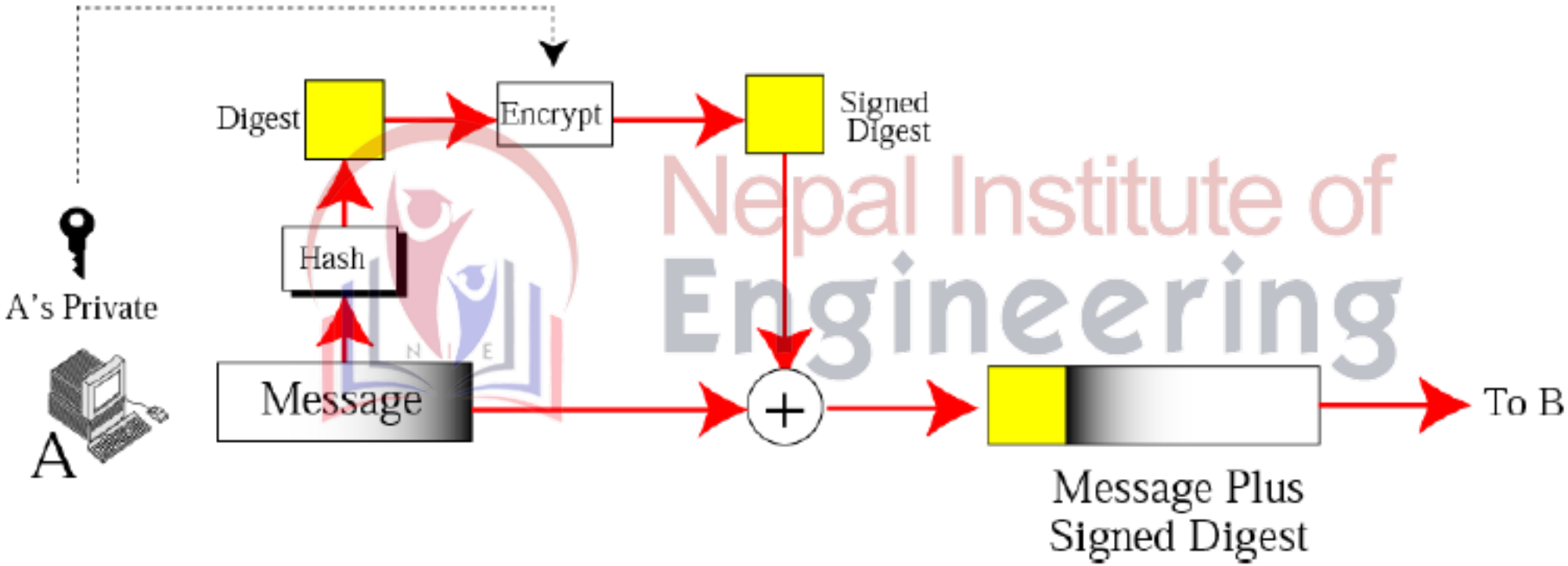


- The two most common hash functions are:
  - Message digest 5 (MD5)
  - Secure hash algorithm (SHA-1,2)
- The properties of hash function
  - One-way: the digest can only be created from the message, but not vice versa
  - One-to-one: be very difficult to find two messages that create the same digest.

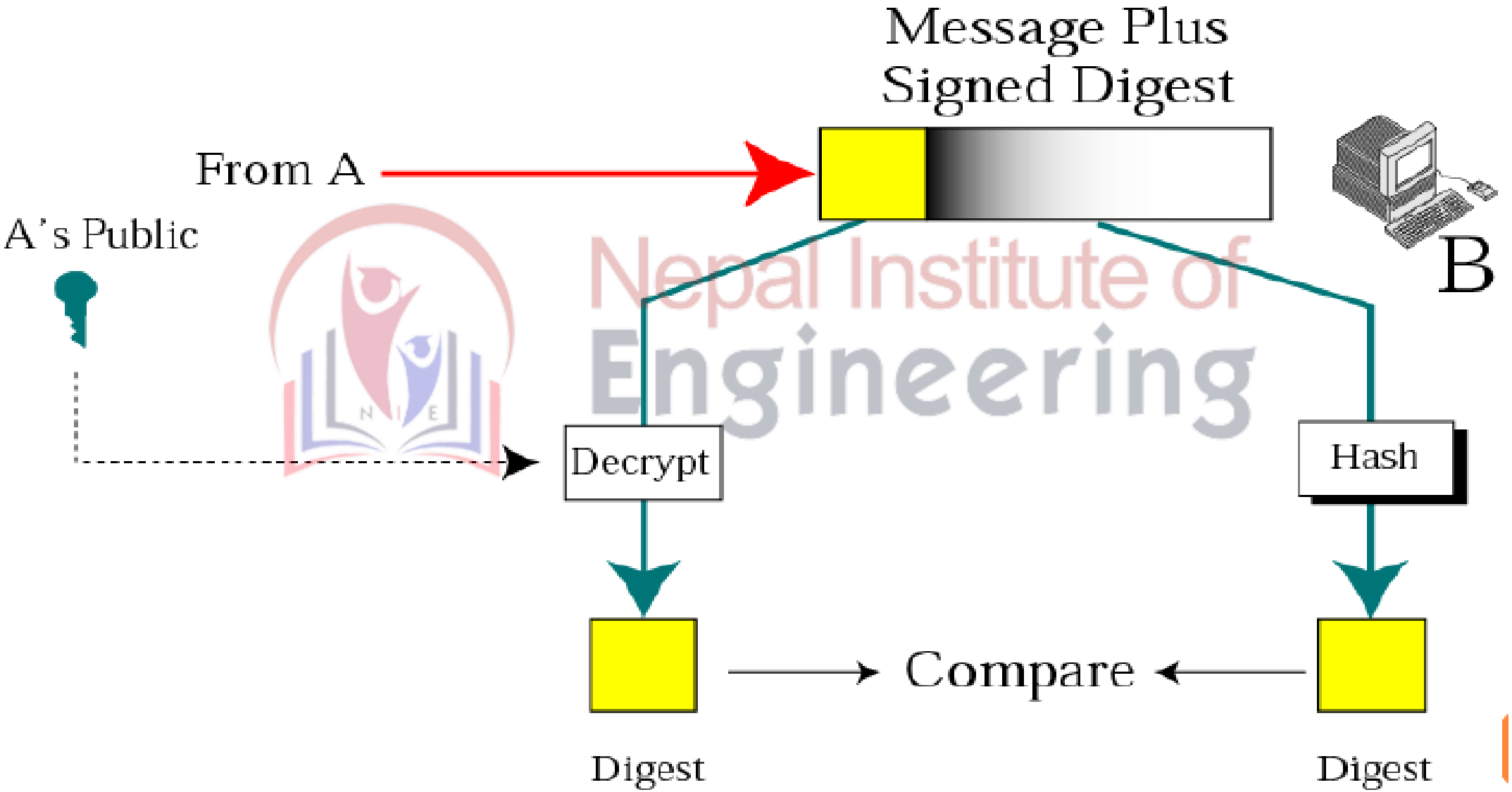
Digital Signatures

- Combines a hash with a digital signature algorithm
- To sign
  - hash the data
  - encrypt the hash with the sender's private key
  - send data signer’s name and signature
- To verify
  - hash the data
  - find the sender’s public key
  - decrypt the signature with the sender's public key
  - the result of which should match the hash

Sender site



Receiver site



Non-repudiation

m is *a* signed message

s is a valid signature for m

Alice denies her signature if she finds:

$m' \neq m$: s is valid signature for m'

Public Key Infrastructure

- Three different formats of messages can be used in public-key cryptosystems: Encrypted message, Signed message, Signed and encrypted message.
- An infrastructure must be set-up to allow them to be undoubtedly trusted , as they are accessible via unsecured networks (Internet)
- PKI entities:
  - -CA (certification authority)
  - -RA (registration authority)
  - -Subscriber
  - -Relying Party
  - -Repository

Elements of PKI

- Certificate Authorities (CA)
  - OpenSSL, Netscape, Verisign, Entrust, RSA Keon
- Public/Private Key Pairs - Key management
- x.509 Identity Certificates - Certificate management
- LDAP servers

PKI basic entities and operations

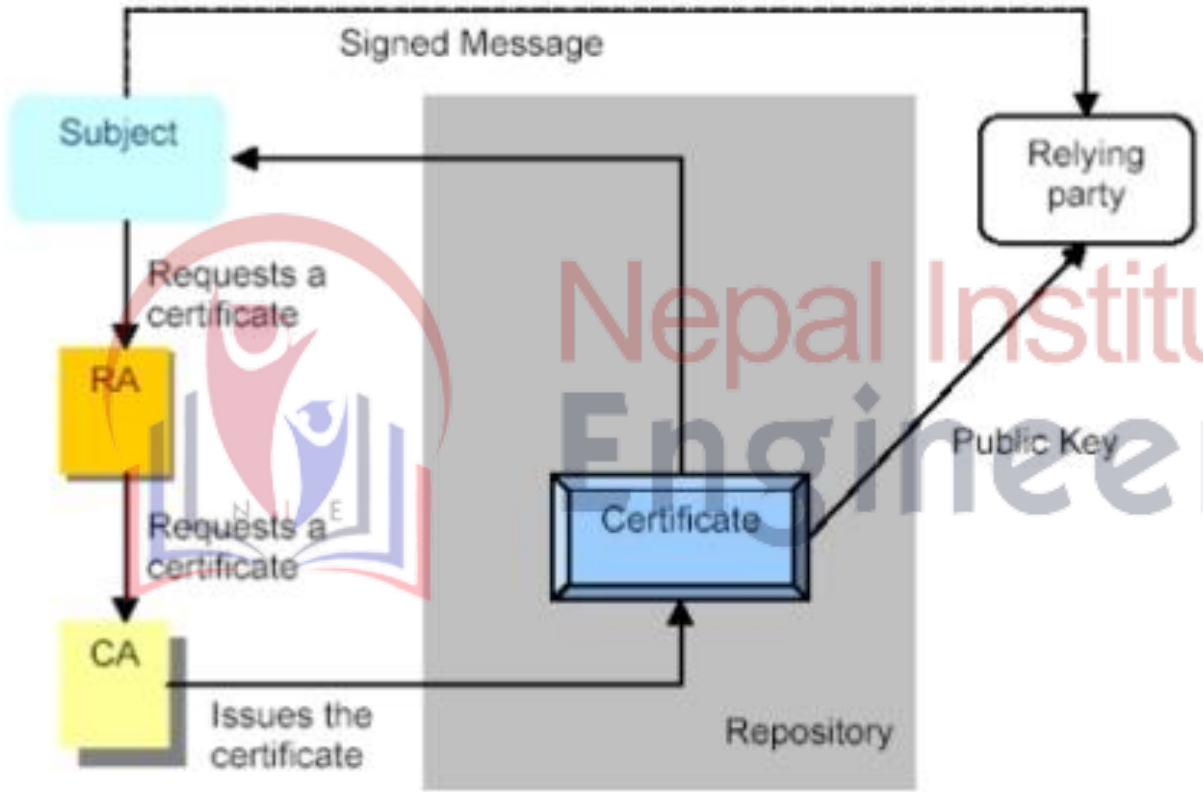


Figure 13 - PKI basic entities and operations

Certificate Authority

- A trusted third party - must be a secure server
- Signs and publishes X.509 Identity certificates
- Revokes certificates and publishes a Certification Revocation List (CRL)
- Many vendors
  - OpenSSL - open source, very simple
  - Netscape - free for limited number of certificates
  - Entrust - Can be run by enterprise or by Entrust
  - Verisign - Run by Verisign under contract to enterprise
  - RSA Security - Keon servers

LDAP server

- Lightweight Directory Access Protocol (IETF standard)
  - Evolved from DAP and X.500 Identities
- Used by CA's to store user's Identity Certificate
- Open source implementations
- Standard protocol for lookup, entry, etc.
- Access control is implemented by user, password.

X.509 Identity Certificates

- Distinguished Name of user
  - C=US, O=Lawrence Berkely National Laboratory, OU=DSD, CN=Mary R. Thompson
- DN of Issuer
  - C=US, O=Lawrence Berkely National Laboratory, CN=LBNL-CA
- Validity dates:
  - Not before <date>, Not after <date>
- User's public key
- V3- extensions
- Signed by CA
- Defined in ANS1 notation - language independent

Validation

- This is the process that ensures that the certificate information is still valid, as it can change over time.
- Either the user can ask the CA directly about the validity - every time it's used - or the CA may include a validity period in the certificate. This second alternative is also known as *offline* validation.

Related Technologies

- CMS - Cryptographic Message Syntax
- SSL
- Secure e-mail / S/MIME
- VPN (Virtual Private Network)
- PGP (Pretty Good Privacy)

Public Key Cryptography Standards - PKCS

- PKCS 7
  - Cryptographic Message Syntax Standard
- PKCS 10
  - Certification Request Syntax Standard - used by Netscape browser, IE, and SSL libraries
- PKCS 11
  - Cryptographic Token Interface Standard - An API for signing and verifying data by a device that holds the key
- PKCS 12
  - Personal Information Exchange Syntax Standard - file format for storing certificate and private key - used to move private information between browsers

SSL - OpenSSL

- Secure message passing protocol
- Developed by Netscape, now an IETF RFC (TLS Jan '99)
- Protocol for using one or two public/private keys
  - to authenticate a sever to a client
  - and by requiring a client key to authenticate the client to the server
  - establish a shared symetric key (the session key)
  - uses the session key to encypt or MAC all data over the secure channel
- Gives you authentication, message integrity and confidentiality
- Everything except authorizaton

Local Computing

- User sits down in front of the computer
- Responds to the login prompt with a user id and password.
- Machine has a list of all the users and their encrypted passwords
- Password never goes across the network
- Passwords are encrypted with a one-way code
- The crypt alogrithm of Unix has been around since mid 70's. Uses a salt to keep identical passwords from having the same encryption. Uses only 8 characters, case sensitive. Uses 25 iterations of DES.
- Typically broken by guessing and verifying guess or snooping the password.

Remote Access Computing

- User logs in to one or more remote machine(s)
- Each machine has its own copy of userid and password for each user
  - Changing a password on one machine does not affect the other machines
  - Each time a user connects to a different machine, she must login again
- In the standard Unix login or rsh commands, the user's password is sent in clear text over the network or else hosts trust users on the basis of their IP addresses
- Ssh
  - encrypts the password before sending it
  - or uses a user's key pair for establishing her identity

Single Domain Remote Access Computing

- User gets access to many machines in a single administrative domain.
- He has a single userid and password for all the machines
- Can login just once to a central trusted server
- Examples
  - Kerberos freeware from MIT Project Athena
  - NIS - Sun software with remote access comands

Kerberos

- User - password based authentication based on late-70's Needham - Schroeder algorithms.
- Kerberos Authentication Server aka KDC (Key Distribution Center) shares long-term secret (password) with each authorized user.
- User logs in and established a short term session key with the AS which can be used to establish his identity with other entities, e.g. file system, other hosts or services each of which trusts the authority server.
- The authorization mechanism needs to be integrated with the each function, e.g. file access, login, telnet, ftp, ...
- The central server is a single point of vulnerablity to attack and failure.
- Been in use for 20 years. We are now at version 5.

Hash Algorithms

- Reduce variable-length input to fixed-length (128 or 160bit) output
- Requirements
  - Can't deduce input from output
  - Can't generate a given output
  - Can't find two inputs which produce the same output
- Used to
  - Produce fixed-length fingerprint of arbitrary-length data
  - Produce data checksums to enable detection of modifications
  - Distill passwords down to fixed-length encryption keys
- Also called message digests or fingerprints

Message Authentication Code MAC

- Hash algorithm + key to make hash value dependant on the key
- Most common form is HMAC (hash MAC)
  - hash(key, hash(key, data))
- Key affects both start and end of hashing process
- Naming: hash + key = HMAC-hash
  - MD5 1 HMAC-MD5
  - SHA-1 1 HMAC-SHA (recommended)

Network Security

Nepal Institute of Engineering

Security Building Blocks

- Encryption provides
  - **confidentiality,** can provide authentication and integrity protection
- Checksums/hash algorithms provide
  - **integrity** protection, can provide authentication
- Digital signatures provide
  - **authentication**, integrity protection, and non-repudiation

Security Attacks

- Passive attacks
  - Obtain message contents
  - Monitoring traffic flows

- Active attacks
  - Masquerade of one entity as some other
  - Replay previous messages
  - Modify messages in transmit
  - Add, delete messages
  - Denial of service (DOS)
  - Distributed Denial of service (DDOS)

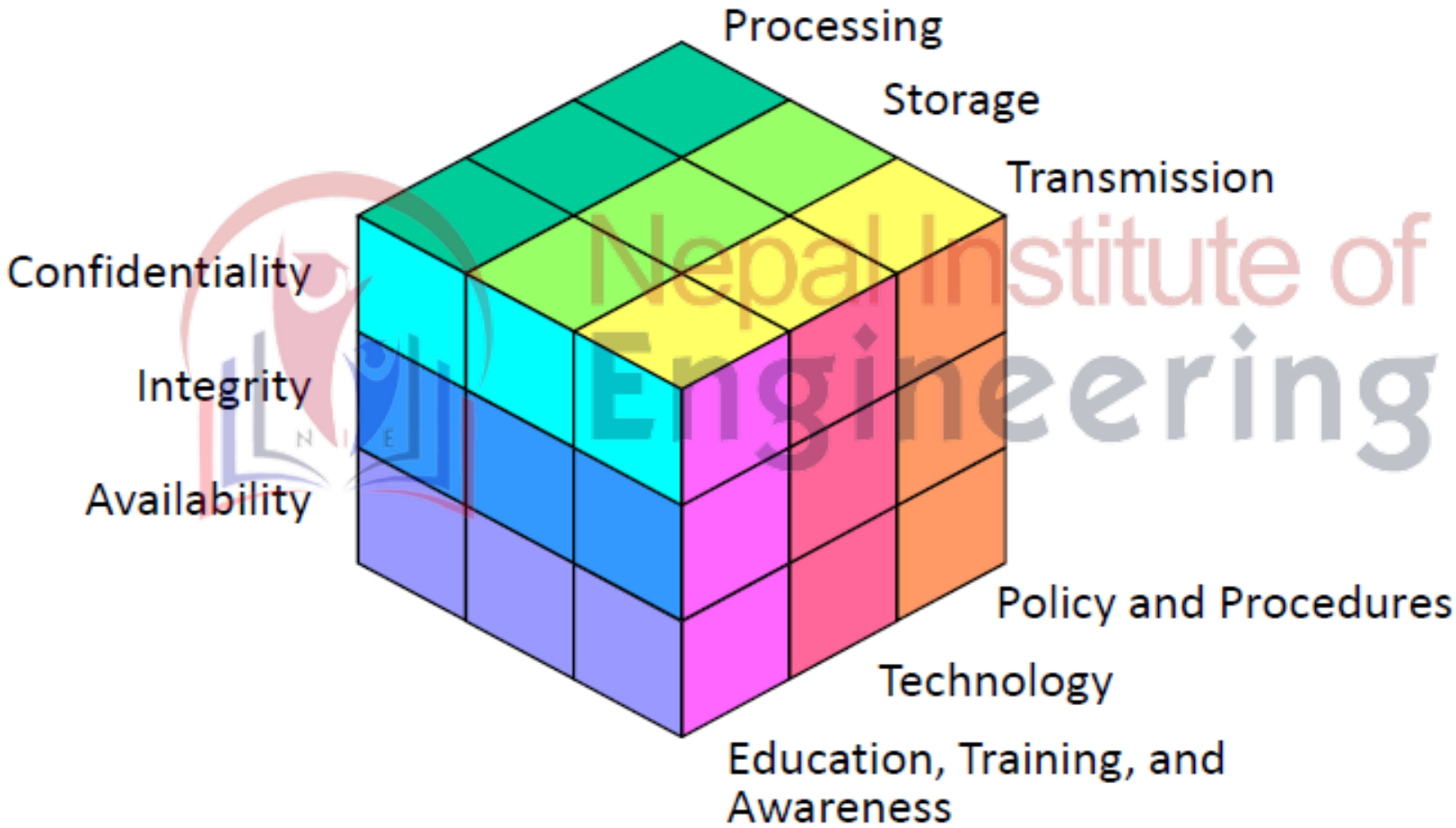
Objectives of Information Security

- Confidentiality (secrecy)
  - Only the sender and intended receiver should be able to understand the contents of the transmitted message
- Authentication
  - Both the sender and receiver need to confirm the identity of other party involved in the communication
- Data integrity
  - The content of their communication is not altered, either maliciously or by accident, in transmission.
- Availability
  - Timely accessibility of data to authorized entities.

Objectives of Information Security

- Non-repudiation
  - An entity is prevented from denying its previous commitments or actions
- Access control
  - An entity cannot access any entity that it is not authorized to.
- Anonymity
  - The identity of an entity if protected from others.

Information Security Model



Information Security Goals

- **Confidentiality**
  - Preserving authorized restrictions on information ***access*** and ***disclosure***, including means for protecting personal privacy and proprietary information.
- **Integrity**
  - Guarding against information ***modifications*** or ***destruction***, including ensuring information non-repudiation and authenticity.
- **Availability**
  - Ensuring timely and reliable access to and ***use*** of information

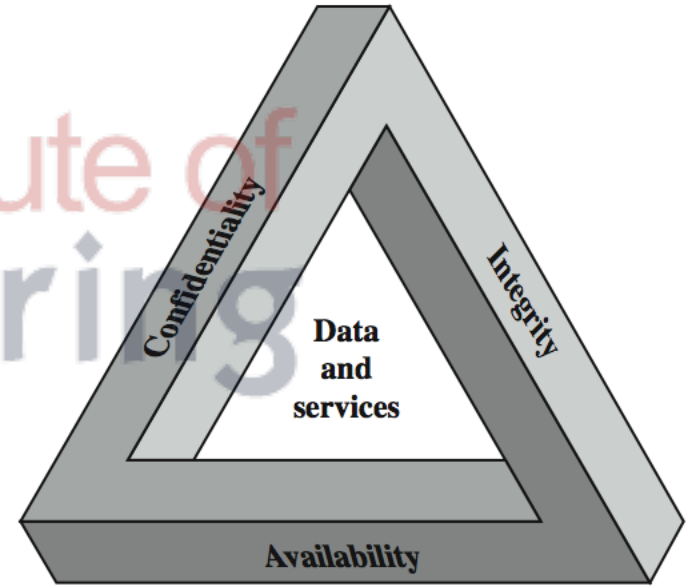


Figure 1.1 The Security Requirements Triad

Model for Network Security

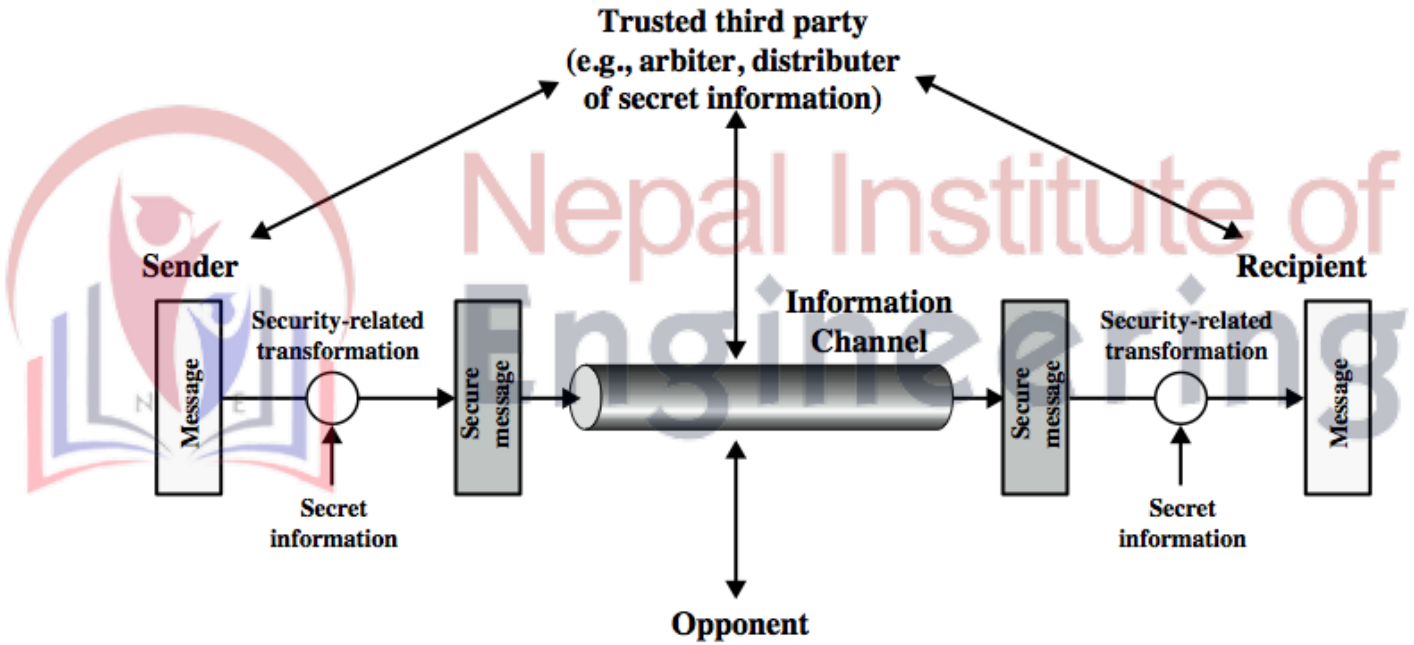
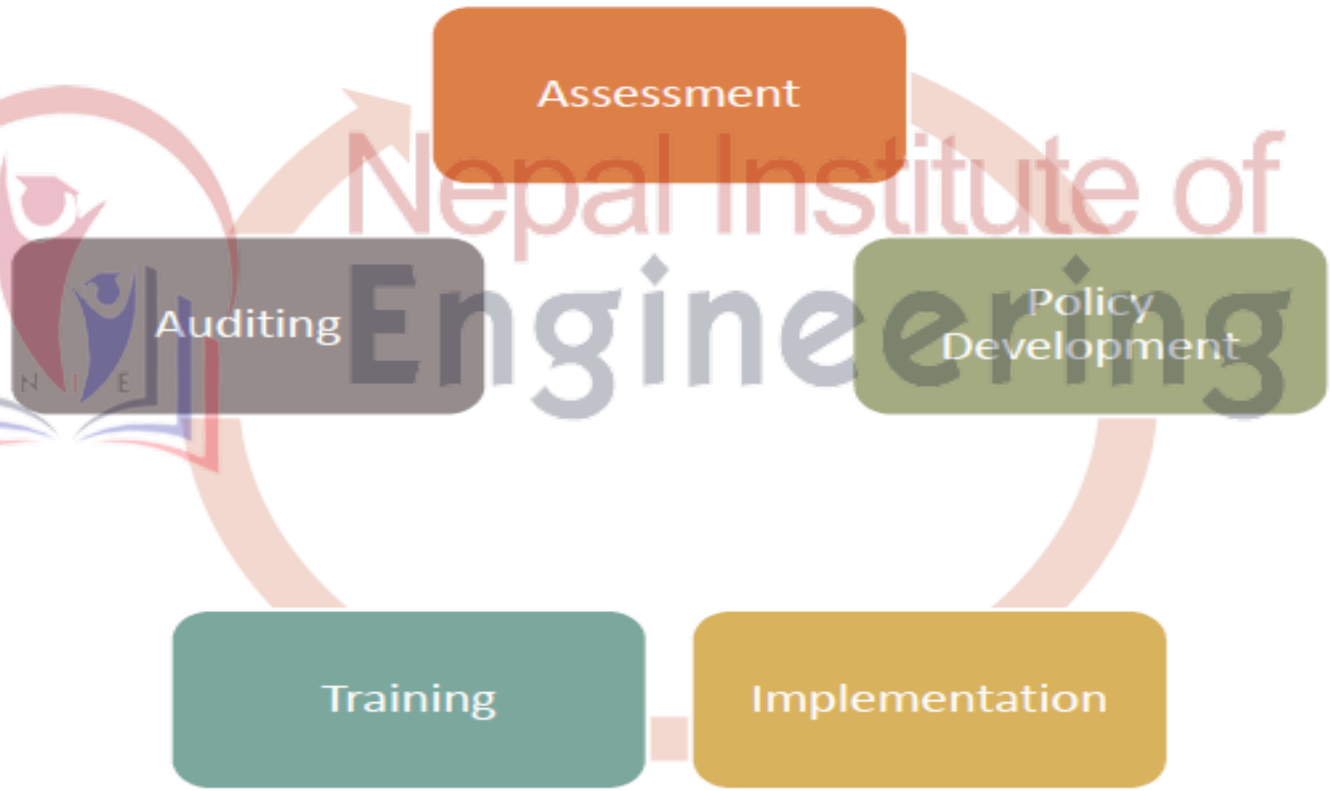
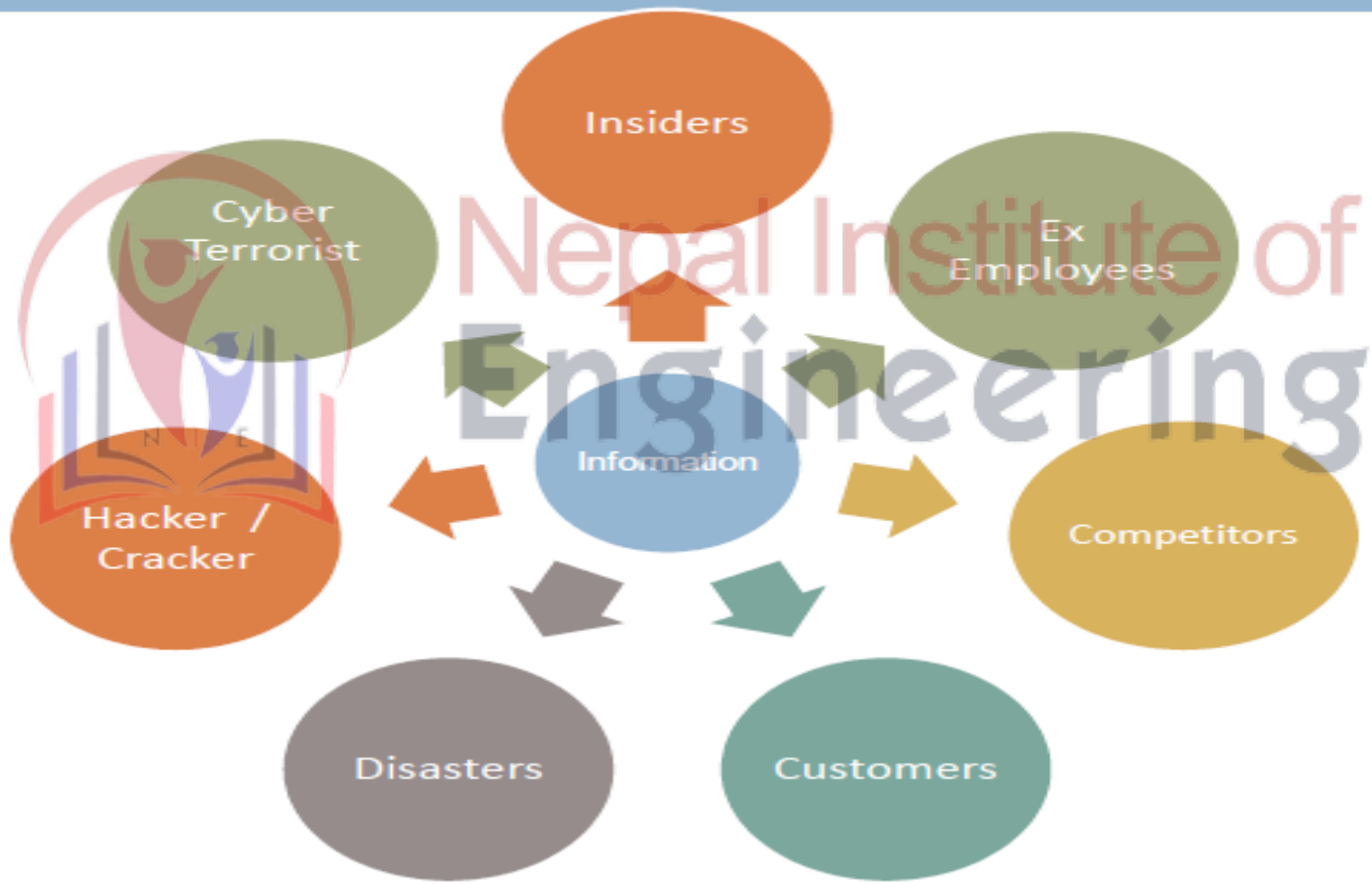


Figure 1.4 Model for Network Security

Information Security Life Cycle



Who Attacks on Information ??



Threats & Attacks

Table 1.1 Threats and Attacks (RFC 2828)

Threat A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.
Attack An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

… but *threat* and *attack* used nearly interchangeably

Security: Categories

- **Information Security**
- **Network Security**
- **Computer Security**
- **Internet Security**

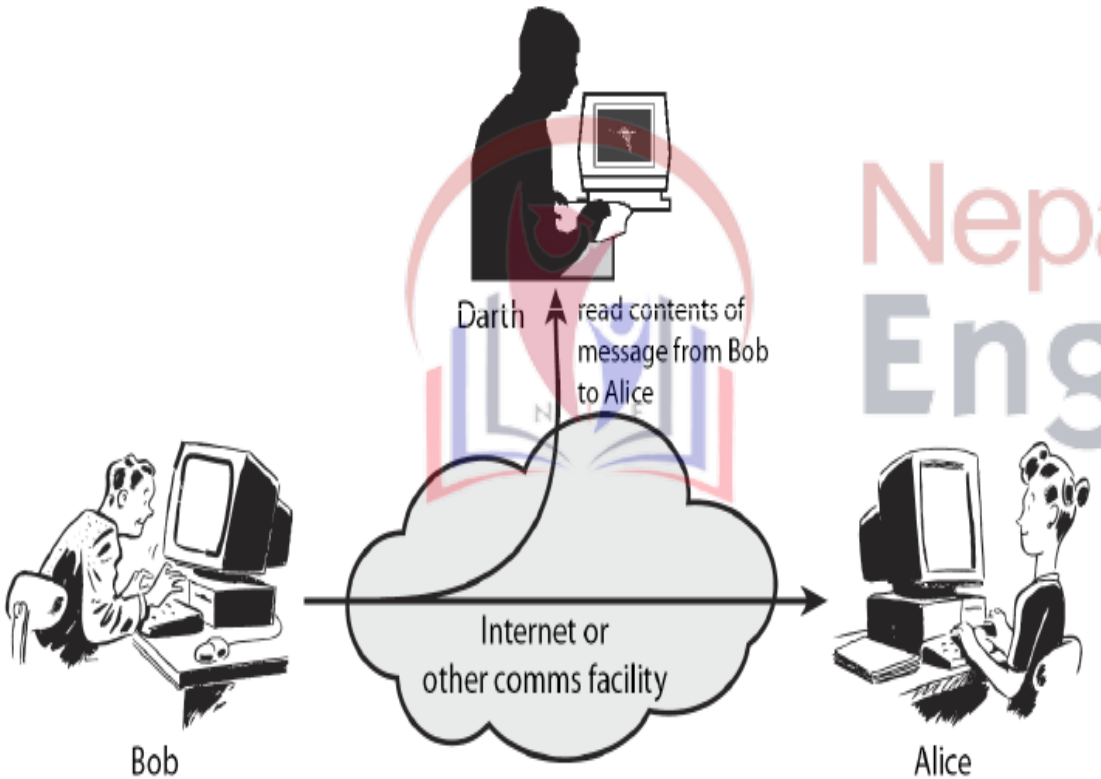
Security Attacks => Exploitation of Vulnerability

Types of Security Attacks.

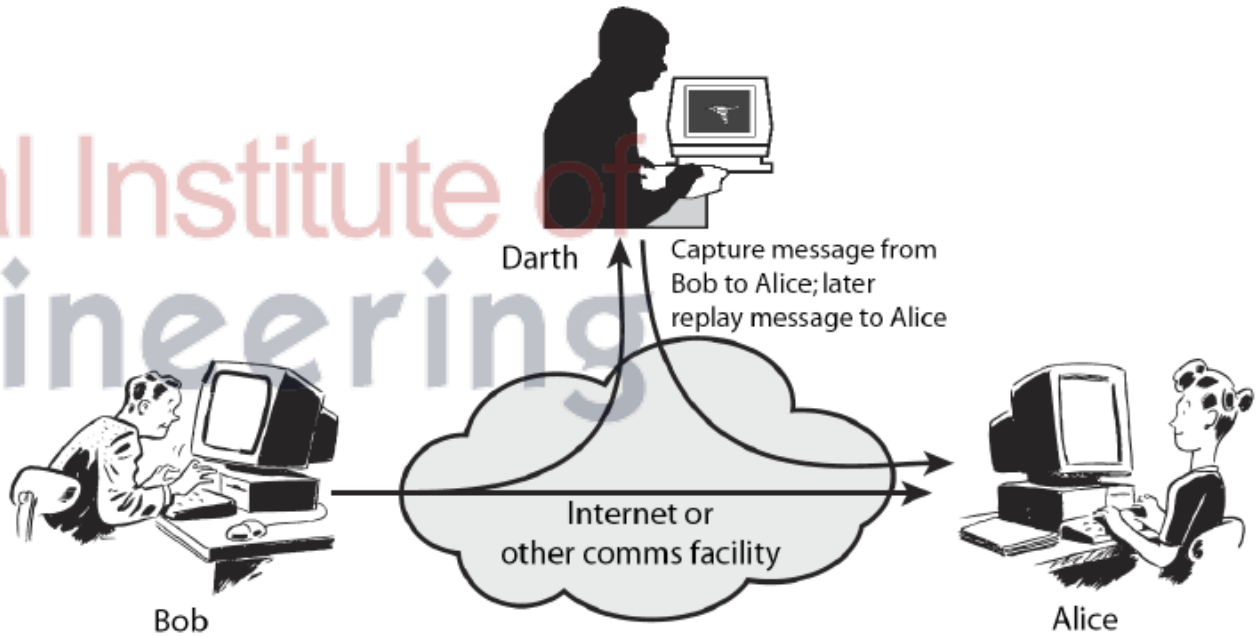
Passive Attacks

Active Attacks

Security Attacks: Passive Attacks



Security Attacks: Active Attacks



Vulnerability: What it is ??

- A network vulnerability is a weakness in a system, technology, product or policy
- Several organizations track, organize and test these vulnerabilities
- Each vulnerability is given an ID and can be reviewed by network security professionals over the Internet.
- The Common Vulnerability Exposure (CVE) list also publishes ways to prevent the vulnerability from being attacked. (http://cve.mitre.org)

Security Attacks : Categorization

Interruption

- This is an attack on availability.
- Example : Cutting of a communication line.

Interception

- This is an attack on confidentiality.
- Example : Wiretapping to capture data in a network.

Modification

- This is an attack of Integrity
- Example : Changing values in a data file.

Fabrication

- This is an attack on authenticity
- Example : Insertion of fake messages in a network.

Common security attacks and their countermeasures

- Finding a way into the network
  - Firewalls
- Exploiting software bugs, buffer overflows
  - Intrusion Detection Systems
- Denial of Service
  - Ingress filtering, IDS
- TCP hijacking
  - IPSec
- Packet sniffing
  - Encryption (SSH, SSL, HTTPS)
- Social problems
  - Education

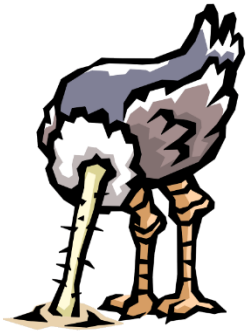
Intrusion Detection

- Used to monitor for “suspicious activity” on a network
  - Can protect against known software exploits, like buffer overflows
- Open Source IDS: Snort, www.snort.org
- Uses “intrusion signatures”
  - Well known patterns of behavior
    - Ping sweeps, port scanning, web server indexing, OS fingerprinting, DoS attempts, etc.

Dictionary Attack

- We can run a dictionary attack on the passwords
  - The passwords in /etc/passwd are encrypted with the crypt(3) function (one-way hash)
  - Can take a dictionary of words, crypt() them all, and compare with the hashed passwords
- This is why your passwords should be meaningless random junk!
  - For example, “sdfo839f” is a good password
    - That is not my andrew password
    - Please don’t try it either

Denial of Service

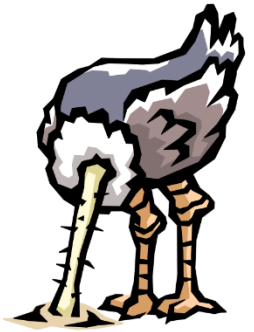


- Purpose: Make a network service unusable, usually by overloading the server or network
- Many different kinds of DoS attacks
  - SYN flooding
  - SMURF
  - Distributed attacks
  - Mini Case Study: Code-Red

Denial of Service

- SYN flooding attack
- Send SYN packets with bogus source address
  - Why?
- Server responds with SYN ACK and keeps state about TCP half-open connection
  - Eventually, server memory is exhausted with this state
- Solution: use “SYN cookies”
  - In response to a SYN, create a special “cookie” for the connection, and forget everything else
  - Then, can recreate the forgotten information when the ACK comes in from a legitimate connection

Denial of Service



- Distributed Denial of Service (DDOS)
  - Same techniques as regular DoS, but on a much larger scale
  - Example: Sub7Server Trojan and IRC bots
    - Infect a large number of machines with a “zombie” program
    - Zombie program logs into an IRC channel and awaits commands
    - Example:
      - Bot command: !p4 207.71.92.193
      - Result: runs ping.exe 207.71.92.193 -l 65500 -n 10000
      - Sends 10,000 64k packets to the host (655MB!)
    - Read more at: http://grc.com/dos/grcdos.htm

TCP Attacks

- If an attacker learns the associated TCP state for the connection, then the connection can be **hijacked**!
- Attacker can insert malicious data into the TCP stream, and the recipient will believe it came from the original source
  - Ex. Instead of downloading and running new program, you download a virus and execute it

Packet Sniffing

- How can we protect ourselves?
- SSH, not Telnet
  - Many people at CMU still use Telnet and send their password in the clear (use PuTTY instead!)
  - Now that I have told you this, please do not exploit this information
  - Packet sniffing is, by the way, prohibited by Computing Services
- HTTP over SSL
  - Especially when making purchases with credit cards!
- SFTP, not FTP
  - Unless you ***really*** don't care about the password or data
  - Can also use KerbFTP (download from MyAndrew)
- IPSec
  - Provides network-layer confidentiality

Example Systems

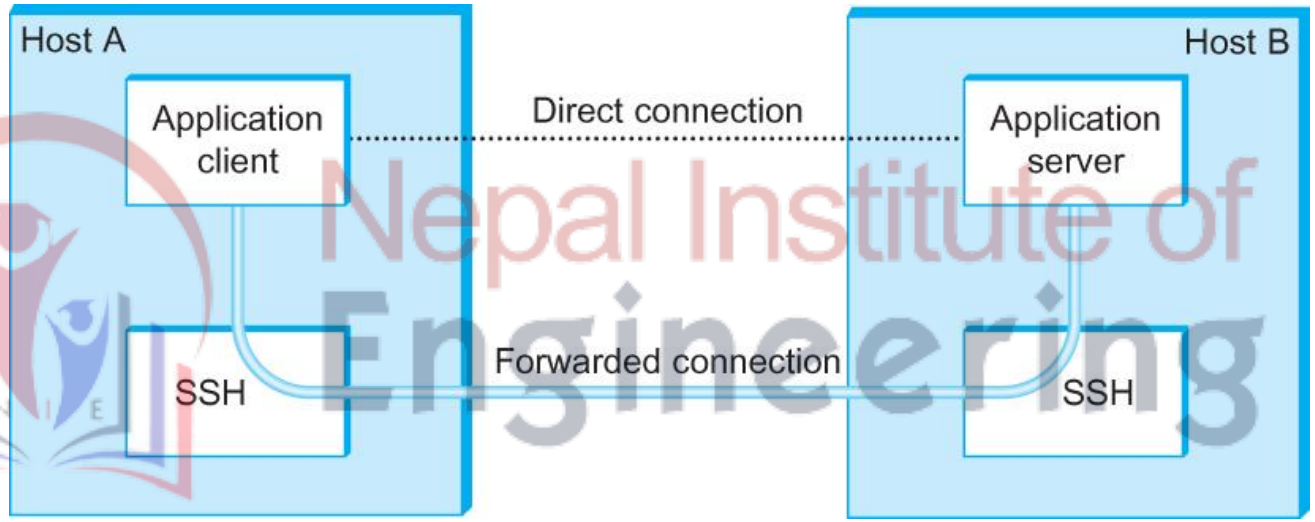
- Pretty Good Privacy (PGP)
  - Pretty Good Privacy (PGP) is a widely used approach to providing security for electronic mail. It provides authentication, confidentiality, data integrity, and nonrepudiation.
  - Originally devised by Phil Zimmerman, it has evolved into an IETF standard known as OpenPGP
  - PGP's confidentiality and receiver authentication depend on the receiver of an email message having a public key that is known to the sender.
  - To provide sender authentication and nonrepudiation, the sender must have a public key that is known by the receiver.
  - These public keys are pre-distributed using certificates and a web-of-trust PKI.
  - PGP supports RSA and DSS for public key certificates.

Example Systems

- Secure Shell (SSH)
  - The Secure Shell (SSH) protocol is used to provide a remote login service, and is intended to replace the less-secure Telnet and rlogin programs used in the early days of the Internet.
  - SSH is most often used to provide strong client/server authentication/ message integrity—where the SSH client runs on the user's desktop machine and the SSH server runs on some remote machine that the user wants to log into—but it also supports confidentiality.
  - Telnet and rlogin provide none of these capabilities.
  - Note that "SSH" is often used to refer to both the SSH protocol and applications that use it; you need to figure out which from the context.

Example Systems

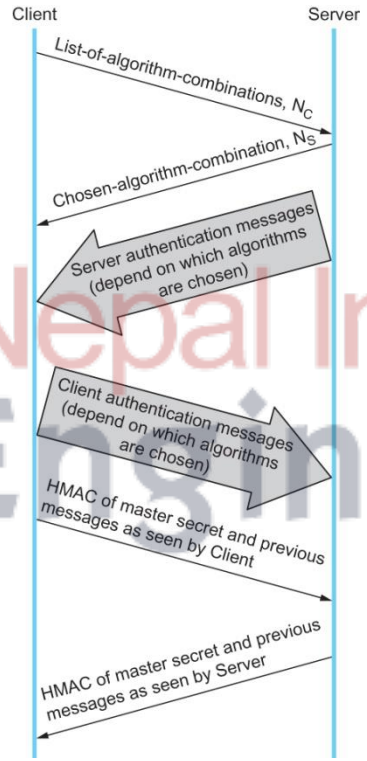
- Secure Shell (SSH)



Using SSH port forwarding to secure other TCP-based applications

Example Systems

- Transport Layer Security (TLS, SSL, HTTPS)



Handshake protocol to establish TLS session

Example Systems

- IP Security (IPSec)
  - Support for IPsec, as the architecture is called, is optional in IPv4 but mandatory in IPv6.
  - IPsec is really a framework (as opposed to a single protocol or system) for providing all the security services discussed throughout this chapter.
  - IPsec provides three degrees of freedom.
    - First, it is highly modular, allowing users (or more likely, system administrators) to select from a variety of cryptographic algorithms and specialized security protocols.
    - Second, IPsec allows users to select from a large menu of security properties, including access control, integrity, authentication, originality, and confidentiality.
    - Third, IPsec can be used to protect “narrow” streams (e.g., packets belonging to a particular TCP connection being sent between a pair of hosts) or “wide” streams (e.g., all packets flowing between a pair of routers).

Example Systems

- IP Security (IPSec)
  - When viewed from a high level, IPsec consists of two parts.
  - The first part is a pair of protocols that implement the available security services.
    - They are the Authentication Header (AH), which provides access control, connectionless message integrity, authentication, and antireplay protection, and the Encapsulating Security Payload (ESP), which supports these same services, plus confidentiality.
    - AH is rarely used so we focus on ESP here.
  - The second part is support for key management, which fits under an umbrella protocol known as ISAKMP:
    - Internet Security Association and Key Management Protocol.

Example Systems

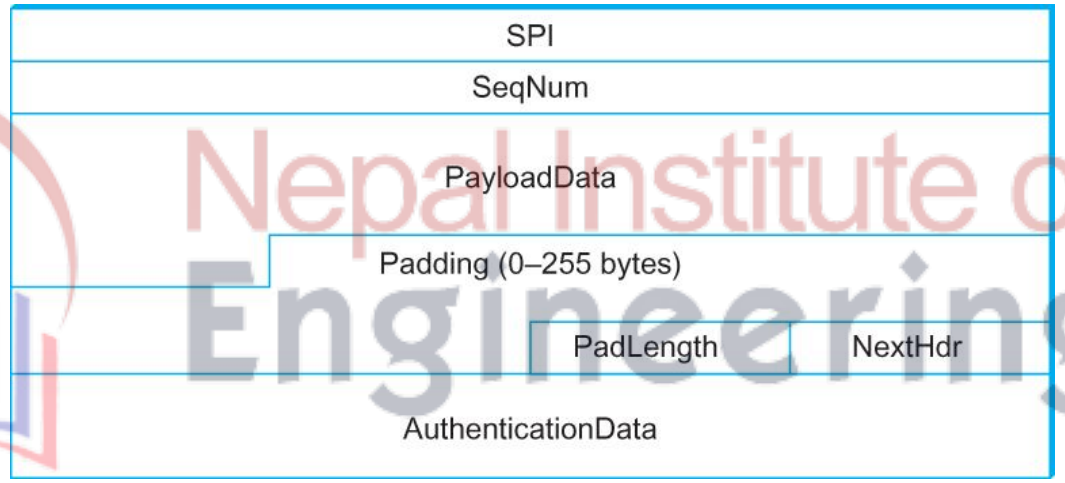
- IP Security (IPSec)
  - The abstraction that binds these two pieces together is the *security association (SA).*
  - *An SA is a simplex (one-way) connection with one or more of the available* security properties.
  - Securing a bidirectional communication between a pair of hosts—corresponding to a TCP connection, for example—requires two SAs, one in each direction.
  - Although IP is a connectionless protocol, security depends on connection state information such as keys and sequence numbers.
  - When created, an SA is assigned an ID number called a *security parameters index (SPI) by the receiving machine*

Example Systems

- IP Security (IPSec)
  - IPsec supports a *tunnel mode as well as the more straightforward transport mode.*
  - Each SA operates in one or the other mode.
  - In a transport mode SA, ESP's payload data is simply a message for a higher layer such as UDP or TCP.
    - In this mode, IPsec acts as an intermediate protocol layer, much like SSL/TLS does between TCP and a higher layer.
    - When an ESP message is received, its payload is passed to the higher level protocol.
  - In a tunnel mode SA, however, ESP's payload data is itself an IP packet

Example Systems

- IP Security (IPSec)



IPsec's ESP format

Example Systems

- IP Security (IPSec)

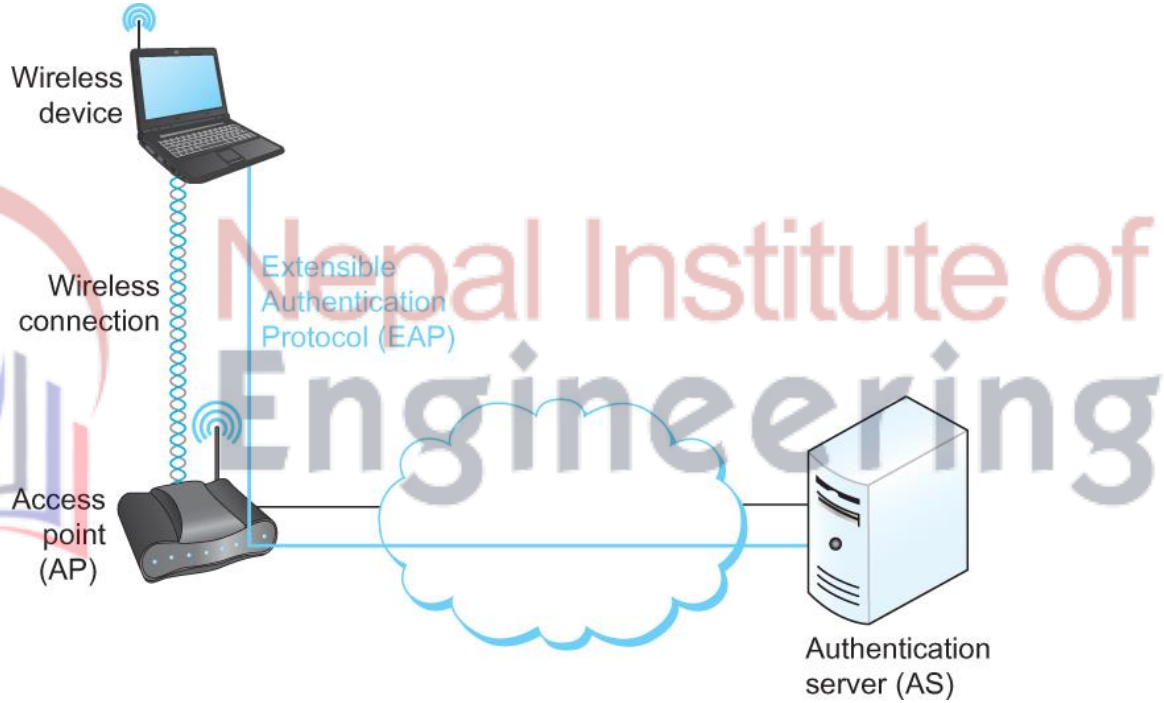
An IP packet with a nested IP packet encapsulated using ESP in tunnel mode. Note that the inner and outer packets have different addresses

Example Systems

- Wireless Security (IEEE 802.11i)
  - The IEEE 802.11i standard provides authentication, message integrity, and confidentiality to 802.11 (Wi-Fi) at the link layer.
  - *WPA2 (Wi-Fi Protected Access 2) is often* used as a synonym for 802.11i, although it is technically a trademark of The Wi-Fi Alliance that certifies product compliance with 802.11i.
  - 802.11i authentication supports two modes. In either mode, the end result of successful authentication is a shared Pairwise Master Key.
    - *Personal mode, also known* as *Pre-Shared Key (PSK) mode, provides weaker security but is more convenient and* economical for situations like a home 802.11 network.
    - The wireless device and the Access Point (AP) are preconfigured with a shared *passphrase—essentially a very long* password—from with the Pairwise Master Key is cryptographically derived.

Example Systems

- Wireless Security (IEEE 802.11i)



Use of an Authentication Server in 802.11i

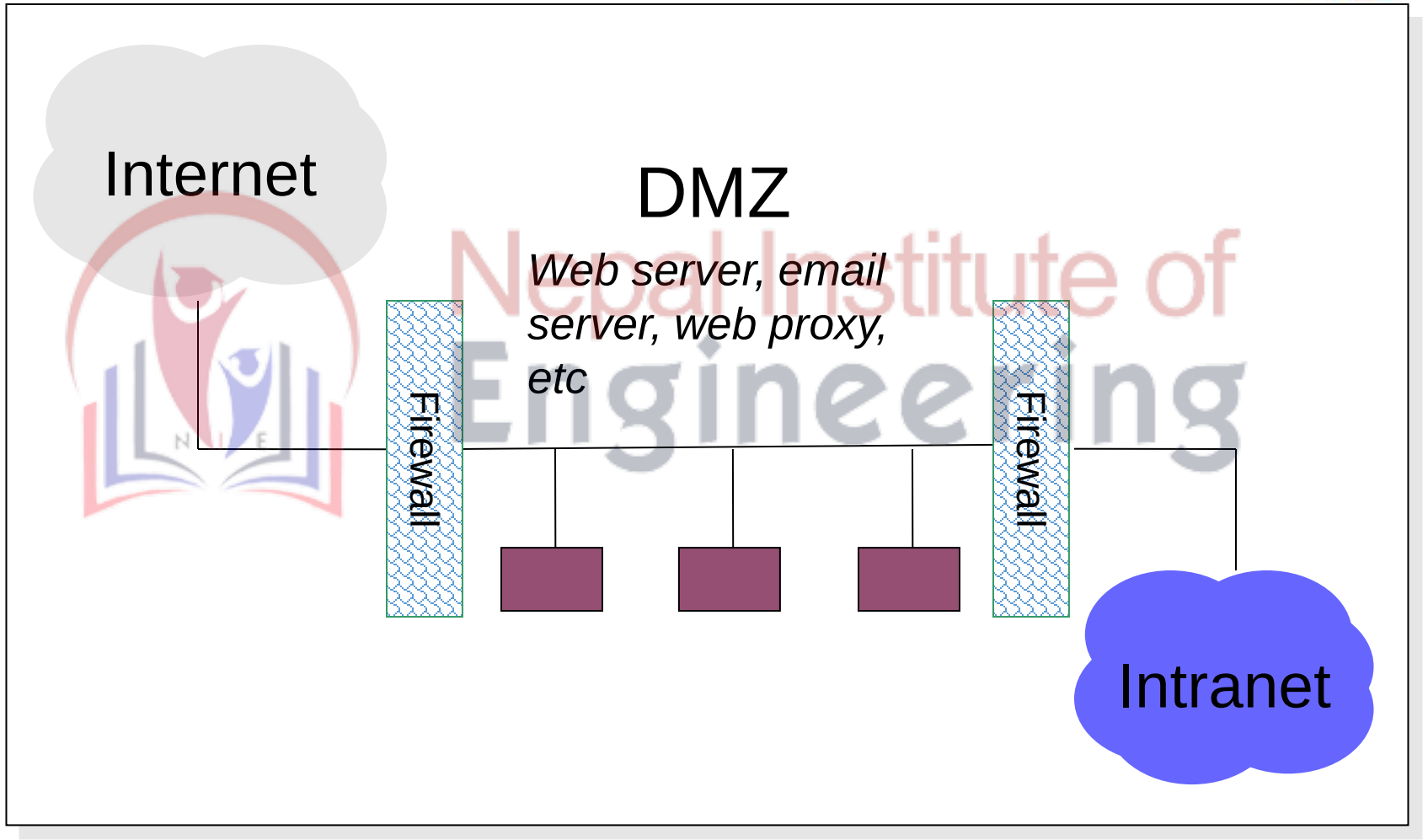
Firewalls

- A firewall is a system that typically sits at some point of connectivity between a site it protects and the rest of the network.
- It is usually implemented as an “appliance” or part of a router, although a “personal firewall” may be implemented on an end user machine.
- Firewall-based security depends on the firewall being the only connectivity to the site from outside; there should be no way to bypass the firewall via other gateways, wireless connections, or dial-up connections.

Firewalls

- A firewall is like a castle with a drawbridge
  - Only one point of access into the network
  - This can be good or bad
- Can be hardware or software
  - Ex. Some routers come with firewall functionality
  - ipfw, ipchains, pf on Unix systems, Windows XP and Mac OS X have built in firewalls

Firewalls



Firewalls

- In effect, a firewall divides a network into a more-trusted zone internal to the firewall, and a less-trusted zone external to the firewall.
- This is useful if you do not want external users to access a particular host or service within your site.
- Firewalls may be used to create multiple *zones of trust, such as a hierarchy of* increasingly trusted zones.
- A common arrangement involves three zones of trust: the internal network; the *DMZ ("demilitarized zone");* and the rest of the Internet.

Firewalls

- Firewalls filter based on IP, TCP, and UDP information, among other things.
- They are configured with a table of addresses that characterize the packets they will, and will not, forward.
- By addresses, we mean more than just the destination's IP address, although that is one possibility.
- Generally, each entry in the table is a 4-tuple: It gives the IP address and TCP (or UDP) port number for both the source and destination.

Protection Methods

- Packet Filtering
  - Rejects TCP/IP packets from unauthorized hosts and/or connection attempts bt unauthorized hosts
- Network Address Translation (NAT)
  - Translates the addresses of internal hosts so as to hide them from the outside world
  - Also known as IP masquerading
- Proxy Services
  - Makes high level application level connections to external hosts on behalf of internal hosts to completely break the network connection between internal and external hosts

Other common Firewall Services

- Encrypted Authentication
  - Allows users on the external network to authenticate to the Firewall to gain access to the private network
- Virtual Private Networking
  - Establishes a secure connection between two private networks over a public network
    - This allows the use of the Internet as a connection medium rather than the use of an expensive leased line

Additional services sometimes provided

- Virus Scanning
  - Searches incoming data streams for virus signatures so theey may be blocked
  - Done by subscription to stay current
    - McAfee / Norton
- Content Filtering
  - Allows the blocking of internal users from certain types of content.
    - Usually an add-on to a proxy server
    - Usually a separate subscription service as it is too hard and time consuming to keep current

Network Address Translation

- Single host makes requests on behalf of all internal users
  - hides the internal users behind the NAT's IP address
  - internal users can have any IP address
    - should use the reserved ranges of 192.168.n.m or 10.n.m.p to avoid possible conflicts with duplicate external addresses
- Only works at the TCP/IP level
  - doesn't do anything for addresses in the payloads of the packets

Virtual Private Networks (VPN)

- Used to connect two private networks via the internet
  - Provides an encrypted tunnel between the two private networks
  - Usually cheaper than a private leased line but should be studied on an individual basis
  - Once established and as long as the encryption remains secure the VPN is impervious to exploitation
  - For large organizations using VPNs to connect geographically diverse sites, always attempt to use the same ISP to get best performance.
    - Try to avoid having to go through small Mom-n-Pop ISPs as they will tend to be real bottlenecks

VPNs (more)

- Many firewall products include VPN capabilities
- But, most Operating Systems provide VPN capabilities
  - Windows NT provides a point-to-point tunneling protocol via the Remote Access server
  - Windows 2000 provides L2TP and IPSec
  - Most Linux distributions support encrypted tunnels one way or another
    - Point-to-Point Protocol (PPP) over Secure Sockets Layer (SSL)
- Encrypted Authentication
  - Many enterprises provide their employees VPN access from the Internet for work-at-home programs or for employees on-the-road
    - Usually done with a VPN client on portable workstations that allows encryption to the firewall
      - Good VPN clients disable connections to the internet while the VPN is running
      - Problems include:
        - A port must be exposed for the authentication
        - Possible connection redirection
        - Stolen laptops
        - Work-at-home risks

Proxies

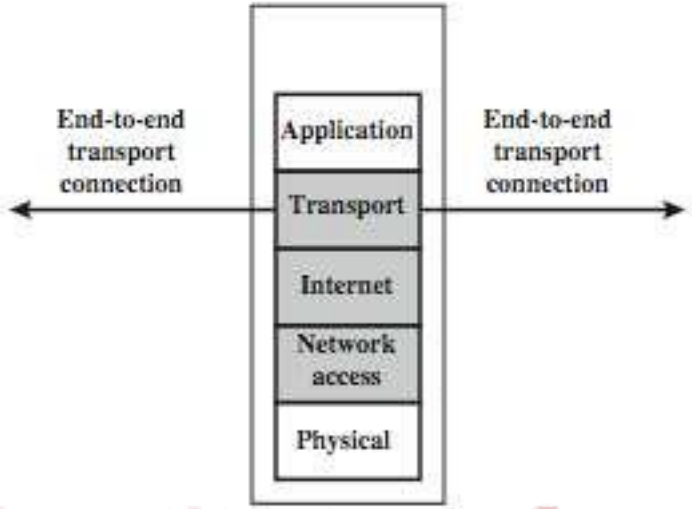
- Hides internal users from the external network by hiding them behind the IP of the proxy
- Prevents low level network protocols from going through the firewall eliminating some of the problems with NAT
- Restricts traffic to only the application level protocols being proxied
- proxy is a combination of a client and a server; internal users send requests to the server portion of the proxy which then sends the internal users requests out through its client (keeps track of which users requested what, do redirect returned data back to appropriate user)

Types of Firewalls

- Packet filtering firewall
- Application proxy firewall
- Stateful inspection firewall
- Circuit – level proxy firewall

Packet Filtering Firewall

- packet filtering firewall applies a set of rules to each incoming
- and outgoing IP packet and then forwards or discards the packet.
- Filtering rules are based on information contained in a network packet.
  - Source IP address
  - Destination IP address
  - Source and destination transport level address
  - IP protocol field
  - Interface



Some possible attacks on firewall :

- **IP address spoofing**
- **Source routing attacks**
- **Tiny fragment attacks**

Advantage :

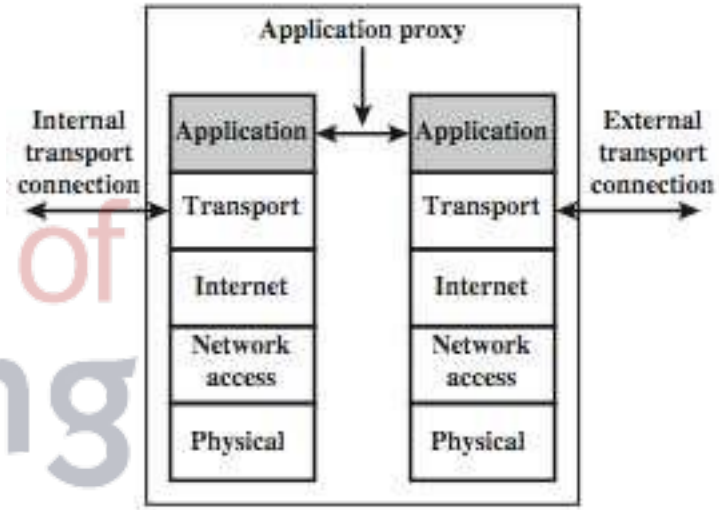
- Cost
- Low resource usage
- Best suited for smaller network

✓ **Disadvantage :**

- Can work only on the network layer
- Do not support complex rule based support
- Vulnerable to spoofing

Application Proxy Firewall

- An application – level gateway, also called an application proxy, acts as a rely of application – level traffic.
- user requests service from proxy.
- proxy validates request as legal.
- then actions request and returns result to user.
- can log / audit traffic at application level.



Advantage :

- More secure than packet filter firewalls
- Easy to log and audit incoming traffic

✓ **Disadvantage :**

- Additional processing overhead on each connection

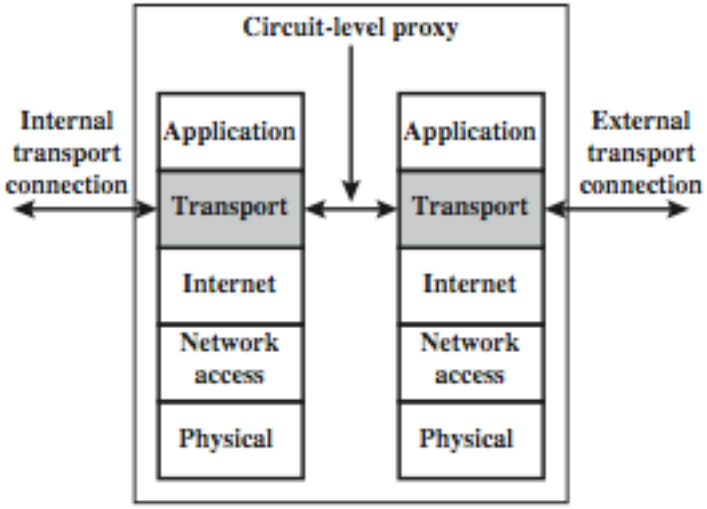
Stateful Inspection Firewall

- A stateful inspection packet firewall tightens up the rules for TCP traffic by creating a directory of outbound TCP connections.
- There is an entry for each currently established connection.
- The packet filter now allow incoming traffic to high – numbered ports only for those packets that fit the profile of one of the entries in this directory.
- A stateful packet inspection firewall reviews the same packet information as a packet filtering firewall, but also records information about TCP connections.

Advantage :

- can work on a transparent mode allowing direct connections between the client and the server
- can also implement algorithms and complex security models which are protocol specific, making the connections and data transfer more secure

Circuit Level Firewall



- This can be a stand – alone system or it can be a specialized functions performed by a gateway for certain applications.
- It does not permit an end – to – end TCP connection; rather, the gateway sets two TCP
- A typical use of the circuit – level gateway is a situation in which the system administrator trusts the internal users.
- The gateway can be configured to support application – level or proxy service on inbound connections and circuit – level functions for outbound connections.

✓ **Advantage :**

- comparatively inexpensive and provide Anonymity to the private network.

✓ **Disadvantage :**

- do not filter Individual Packets

Border Security Options

- Filtered packed services
- Single firewall with internal public servers
- Single firewall with external public servers
- Dual firewalls or DMZ firewalls
- Enterprise firewalls
- Disconnection

1. In cryptography, what is cipher?
a) **algorithm for performing encryption and decryption**
b) encrypted message
c) both (a) and (b)
d) none of the mentioned

2. In asymmetric key cryptography, the private key is kept by
a) sender
b) **receiver**
c) sender and receiver
d) all the connected devices to the network

5. What is data encryption standard (DES)?
a) **block cipher**
b) stream cipher
c) bit cipher
d) none of the mentioned

6. Cryptanalysis is used
a) to find some insecurity in a cryptographic scheme
b) to increase the speed
c) to encrypt the data
d) none of the mentioned

7. Which one of the following is a cryptographic protocol used to secure HTTP connection?
a) stream control transmission protocol (SCTP)
b) **transport layer security (TSL)**
c) explicit congestion notification (ECN)
d) resource reservation protocol

10. Cryptographic hash function takes an arbitrary block of data and returns
a) **fixed size bit string**
b) variable size bit string
c) both (a) and (b)
d) none of the mentioned

An HTTP connection uses port _____ whereas HTTPS uses port _____ and invokes SSL.
a) 40; 80
b) 60; 620
c**) 80; 443**
d) 620; 80

2. A(n) _____ algorithm transforms ciphertext to plaintext.
A) encryption
B) decryption
C) either (a) or (b)
D) neither (a) nor (b)

3. The _____ is the message after transformation.
A) ciphertext
B) plaintext
C) secret-text
D) none of the above

8. The _____ cipher reorders the plaintext characters to create a ciphertext.
A) substitution
B) transposition
C) either (a) or (b)
D) neither (a) nor (b)

7. A _____ cipher replaces one character with another character.
A) substitution
B) transposition
C) either (a) or (b)
D) neither (a) nor (b)

16. DES is a(n) _____ method adopted by the U.S. government.
A) symmetric-key
B) asymmetric-key
C) either (a) or (b)
D) neither (a) nor (b)

23. DES has an initial and final permutation block and _____ rounds.
A) 14
B) 15
C) 16
D) none of the above

1. Message_____ means that the data must arrive at the receiver exactly as sent.
A) confidentiality
B) integrity
C) authentication
D) none of the above

2. Message _____ means that the receiver is ensured that the message is coming from the intended sender, not an imposter.
A) confidentiality
B) integrity
C) authentication

3. A(n) _____function creates a message digest out of a message.
A) encryption
B) decryption
C) hash
D) none of the above

10. _____ means to prove the identity of the entity that tries to access the system's resources.
A) Message authentication
B) Entity authentication
C) Message confidentiality
D) none of the above

11. A _____ signature is included in the document; a _____ signature is a separate entity.
A) conventional; digital
B) digital; digital
C) either (a) or (b)
D) neither (a) nor (b)

13. Digital signature provides _____.
A) authentication
B) nonrepudiation
C) both (a) and (b)
D) neither (a) nor (b)

16. A(n) _____ can be used to preserve the integrity of a document or a message.
A) message digest
B) message summary
C) encrypted message
D) none of the above

19. A digital signature needs a(n)_____ system.
A) symmetric-key
B) asymmetric-key
C) either (a) or (b)
D) neither (a) nor (b)

11. SSL provides _____.
A) message integrity
B) confidentiality
C) compression
D) all of the above

20. A(n) _____is a federal or state organization that binds a public key to an entity and issues a certificate.
A) KDC
B) Kerberos
C) CA
D) none of the above

25. A(n) _____ is a hierarchical system that answers queries about key certification.
A) KDC
B) PKI
C) CA
D) none of the above

28. _____ is a popular session key creator protocol that requires an authentication server and a ticket-granting server.
A) KDC
B) Kerberos
C) CA
D) none of the above