3rd session on 8st Feb 2020

Information Systems Security

Cryptography

Prof. M. Chattopadhyay
IIM Raipur
IT & Systems

Learning Objective(s)

Explain how businesses apply

- cryptography in maintaining information security.
- Cyber security tools
- Some of the Important Tools and Technologies for Safeguarding Information Systems?
- Protecting Networks: Firewalls and Proxy Servers
- Encryption and Public Key Infrastructure
- Digital Certificates
- Tools Available to Achieve Site Security
- Protecting Internet communications (encryption)
- Securing channels of communication (SSL, S-HTTP, VPNs)

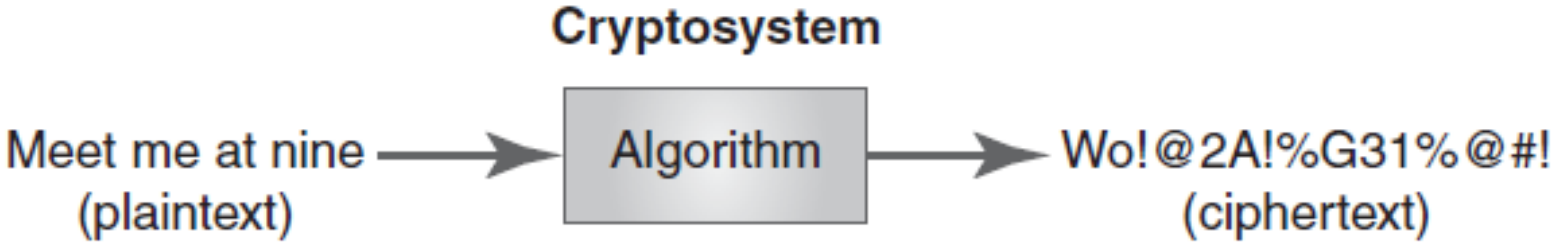
Key Concepts

- Basics of cryptography
- Business applications of cryptography
- Symmetric and asymmetric key cryptography
- Encryption mechanisms and techniques
- Certificate and key management

What Is Cryptography?

- **Unencrypted information**—Information in understandable form (plaintext or cleartext)
- **Encrypted information**—Information in scrambled form (ciphertext)
- **Encryption**—The process of scrambling plaintext into ciphertext
- **Decryption**—The process of unscrambling ciphertext into plaintext
- **Algorithm**—A repeatable process that produces the same result when it receives the same input
- **Cipher**—An algorithm to encrypt or decrypt information

A Cryptosystem at Work



Encryption Cipher Categories

- Those that use the same key to encrypt and decrypt are **private (symmetric) key** ciphers
- Those that use different keys to encrypt and decrypt are **public (asymmetric) key** ciphers

Basic Cryptographic Principles

- **Keyspace—**The number of possible keys to a cipher
- **Open ciphers—**Make it possible for experts around the world to examine the ciphers for weaknesses
- **Data Encryption Standard (DES)—**The most scrutinized cipher in history

A Brief History of Cryptography

- People have used cryptography to protect information for at least 4,000 years
- Steganography is the act of hiding information
- Cryptanalysis is breaking code
- Cryptography was used in WWI and WWII
- Symmetric and asymmetric key cryptography introduced in 1976

Cryptography's Role in Information Security

Confidentiality

- Keeps information secret from unauthorized users

Integrity

- Ensures that no one, even the sender, changes information after transmitting it

Authentication

- Confirms the identity of an entity

Nonrepudiation

- Enables you to prevent a party from denying a previous statement or action

Business and Security Requirements for Cryptography

Internal security

- Confidentiality, privacy, integrity, and authorization

Security in business relationships

- Message authentication, signature, receipt and confirmation, and nonrepudiation

Security measures that benefit everyone

- Anonymity, timestamping, revocation, and ownership

Information Security Objectives

Objective	Steps to Take
Privacy or confidentiality	Keep information secret from all unauthorized users.
Integrity	Ensure that unauthorized users or unknown processes have not altered information.
Entity authentication or identification	Corroborate the identity of an entity (that is, a person, a computer terminal, a credit card, etc.).
Message authentication	Corroborate the source of information; authenticate the data's origin.
Signature	Bind information to an entity.

Information Security Objectives (cont.)

Objective	Steps to Take
Authorization	Convey an official sanction to do or be something to another entity.
Validation	Provide timely authorization to use or manipulate information or resources.
Access control	Restrict access to resources to privileged entities.
Certification	Endorse information by a trusted entity.
Timestamping	Record the time a user created or accessed information.
Witnessing	Verify the action to create an object or verify an object's existence by an entity other than the creator.

Information Security Objectives (cont.)

Objective	Steps to Take
Receipt	Acknowledge that the recipient received information.
Confirmation	Acknowledge that the provider has provided services.
Ownership	Grant an entity the legal right to use or transfer a resource to others.
Anonymity	Conceal the identity of an entity involved in some process.
Nonrepudiation	Prevent an entity from denying previous commitments or actions.
Revocation	Retract certification or authorization.

Cryptographic Functions and Ciphers

- Each cipher has specific characteristics that make it desirable or undesirable
- When evaluating a cipher, consider its intended use
  - Are you trying to secure data in transit or data at rest?
  - Different ciphers solve different problems better than others
- After selecting a cipher, you must make additional decisions about key size, operational mode, etc.
- Many symmetric ciphers operate as either a stream cipher or a block cipher

Business-Security Implementations

General Classifications

- Authentication (non-PKI)
- Access control/authorization
- Assessment and audit
- Security management products
- Perimeter/network security/availability
- Content filtering
- Encryption
- Administration/education
- Outsource services/consultants

Cryptography Capabilities

- Privacy or confidentiality
- Integrity
- Entity authentication or identification
- Message authentication
- Signature
- Access control
- Certification
- Timestamping
- Witnessing
- Ownership
- Anonymity
- Nonrepudiation

Types of Ciphers

Transposition ciphers

- Rearranges characters or bits of data

Substitution ciphers

- Replaces bits, characters, or blocks of information with other bits, characters, or blocks

Transposition Ciphers

- Message—ATTACK AT DAWN
- Ciphertext—ACDTKATAWATN
- Key— {1,2,3,4}

1	2	3	4
A	T	T	A
C	K	A	T
D	A	W	N

Substitution Ciphers

- **Caesar cipher**—Each letter in the English alphabet a fixed number of positions, with Z wrapping back to A
- **Keyword mixed alphabet cipher**—Uses a cipher alphabet that consists of a keyword, minus duplicates, followed by the remaining letters of the alphabet
- **Vigenère** (*vee-zhen-AIR*) **cipher**—Encrypts every letter with its own substitution scheme
- **Simple substitution cipher**—Allows any letter to uniquely map to any other letter

Symmetric and Asymmetric Key Cryptography

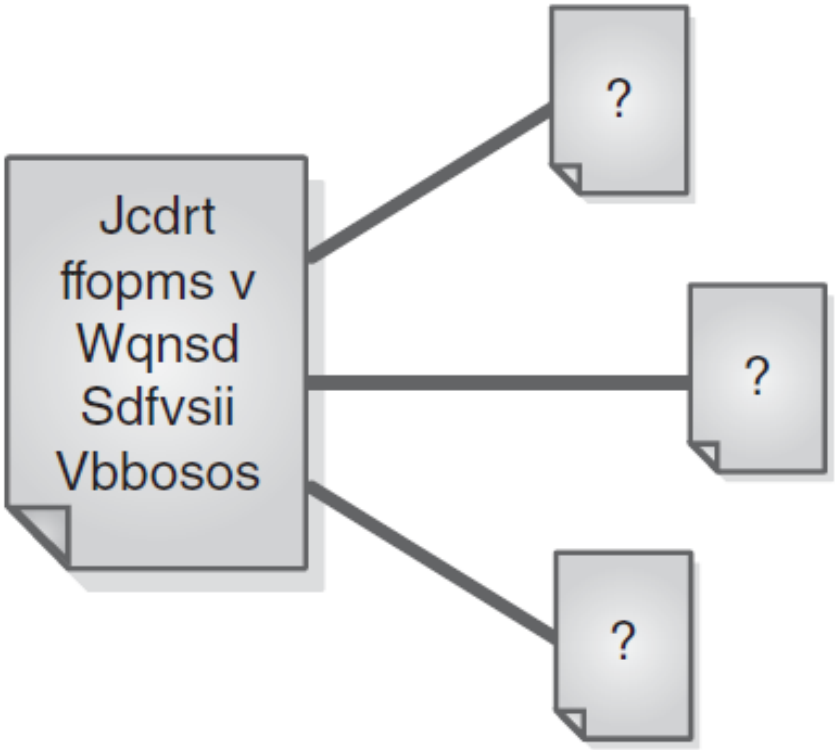
- Symmetric key ciphers use the same key to encrypt and decrypt
- Asymmetric key ciphers have four key properties:
  - Two associated algorithms that are inverses of each other exist
  - Each of these two algorithms is easy to compute
  - It is computationally infeasible to derive the second algorithm if you know the first algorithm
  - Given some random input, you can generate associated key pairs that are inverses of each other

Cryptanalysis and Public Versus Private Keys

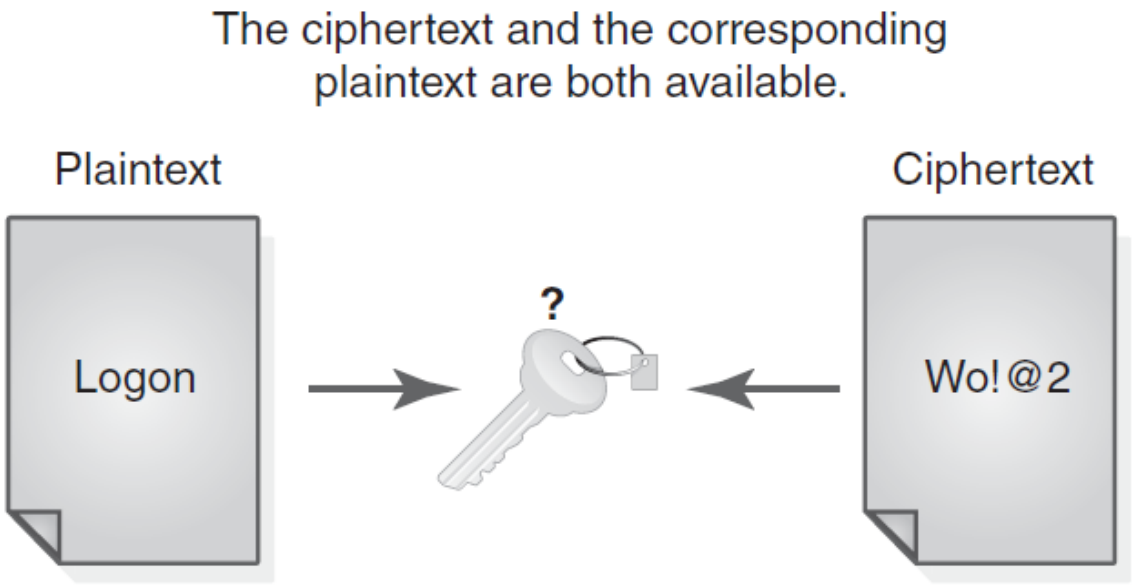
- You can break a cipher in two ways:
  - Analyzing the ciphertext to find the plaintext or key
  - Analyzing the ciphertext and its associated plaintext to find the key
- Four basic forms of cryptographic attack
  - Ciphertext-only attack (COA)
  - Known-plaintext attack (KPA)
  - Chosen-plaintext attack
  - Chosen-ciphertext attack

A Ciphertext-only Attack (COA)

The sample of ciphertext is available, but not the plaintext associated with it.



A Known-Plaintext Attack (KPA)



Keys, Keyspace, and Key Management

Key

- A value that is an input to a cryptosystem

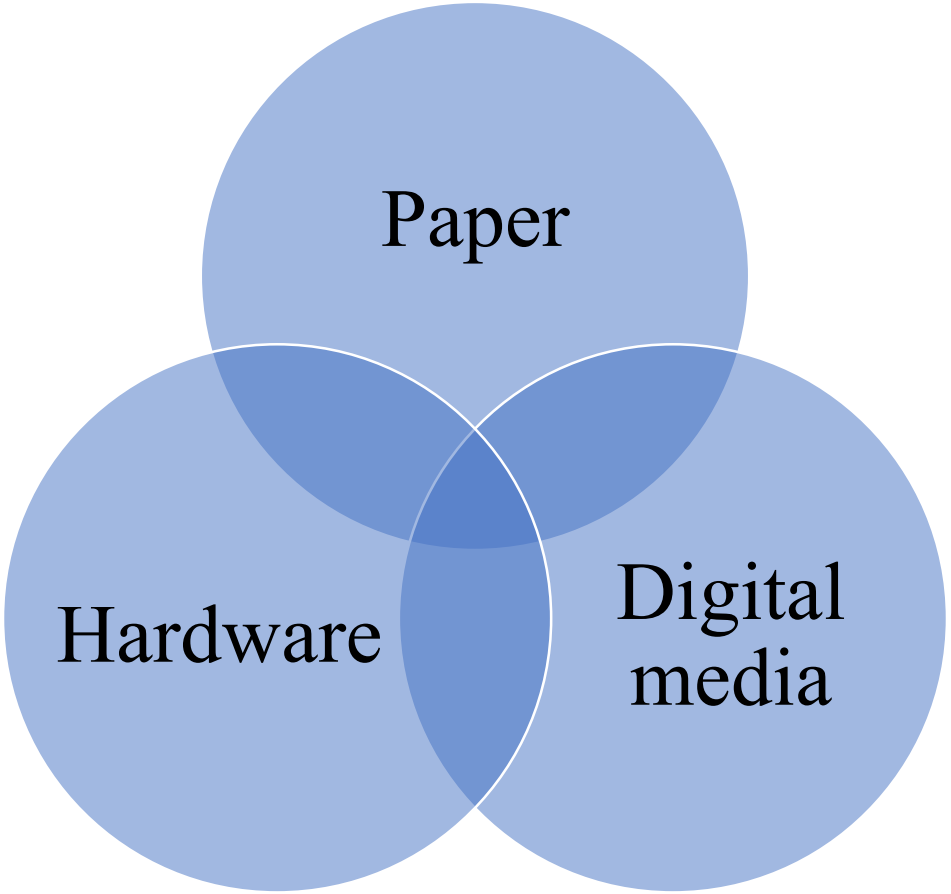
Keyspace

- The set of all possible keys

Key management

- One of the most difficult and critical parts of a cryptosystem

Key Distribution Techniques



Key Distribution Centers

- Rather than each organization creating the infrastructure to manage its own keys, a number of hosts could agree to trust a common **key-distribution center (KDC)**
- All parties must trust the KDC
- With a KDC, each entity requires only one secret key pair—between itself and the KDC
- Kerberos and ANSI X9.17 use the concept of a KDC

Tools Available to Achieve Site Security

Protecting Internet Communications: Encryption

- Encryption: Process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and receiver
- Purpose: Secure stored information and information transmission
- Provides:
  - Message integrity
  - Nonrepudiation
  - Authentication
  - Confidentiality

Symmetric Key Encryption

- Also known as secret key encryption
- Both the sender and receiver use the same digital key to encrypt and decrypt message
- Requires a different set of keys for each transaction
- Advanced Encryption Standard (AES): Most widely used symmetric key encryption today; offers 128-, 192-, and 256-bit encryption keys; other standards use keys with up to 2,048 bits

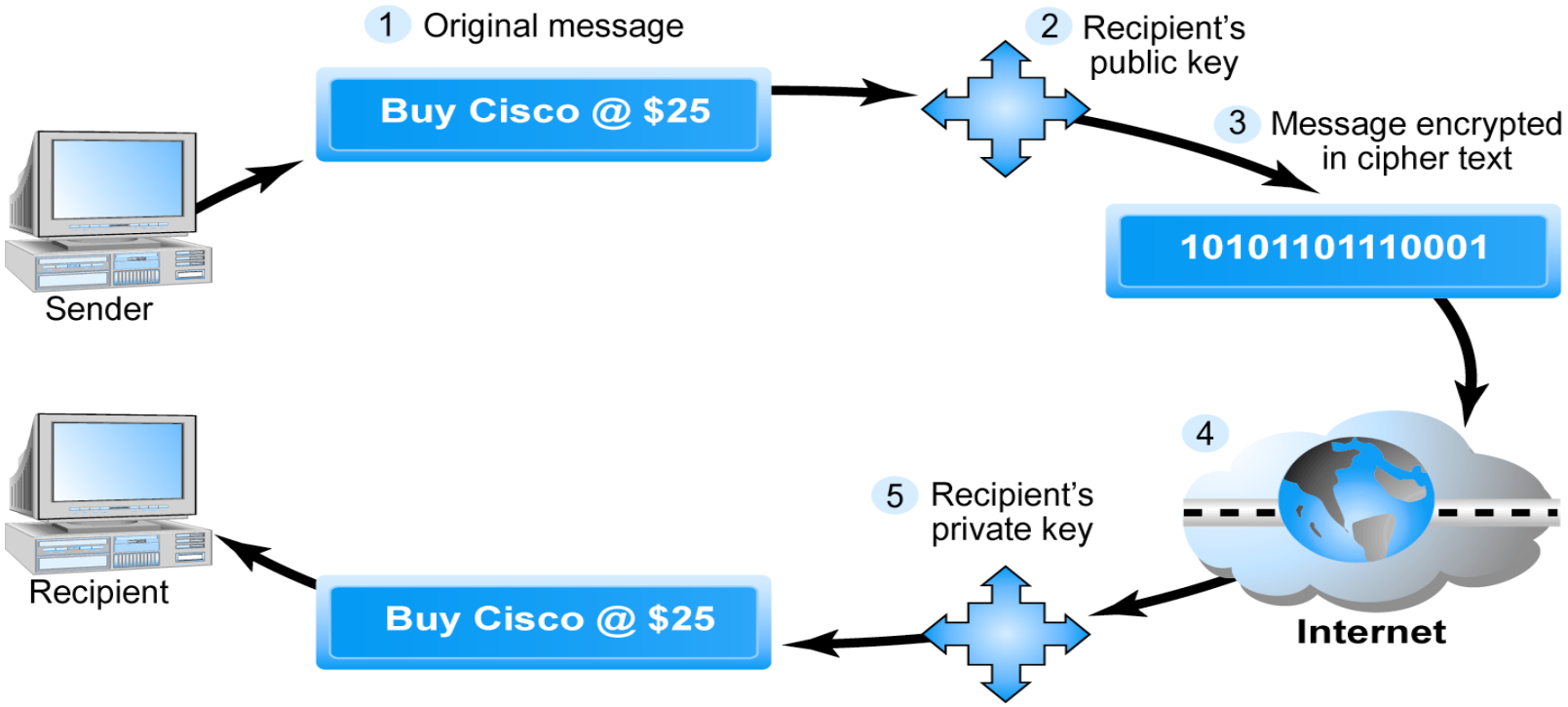
Symmetric Key Encryption

- Also known as secret key encryption
- Both the sender and receiver use the same digital key to encrypt and decrypt message
- Requires a different set of keys for each transaction
- Advanced Encryption Standard (AES): Most widely used symmetric key encryption today; offers 128-, 192-, and 256-bit encryption keys; other standards use keys with up to 2,048 bits

Public Key Encryption

- Solves symmetric key encryption problem of having to exchange secret key
- Uses two mathematically related digital keys – public key (widely disseminated) and private key (kept secret by owner)
- Both keys used to encrypt and decrypt message
- Once key used to encrypt message, same key cannot be used to decrypt message
- For example, sender uses recipient's public key to encrypt message; recipient uses his/her private key to decrypt it

Public Key Cryptography – A Simple Case

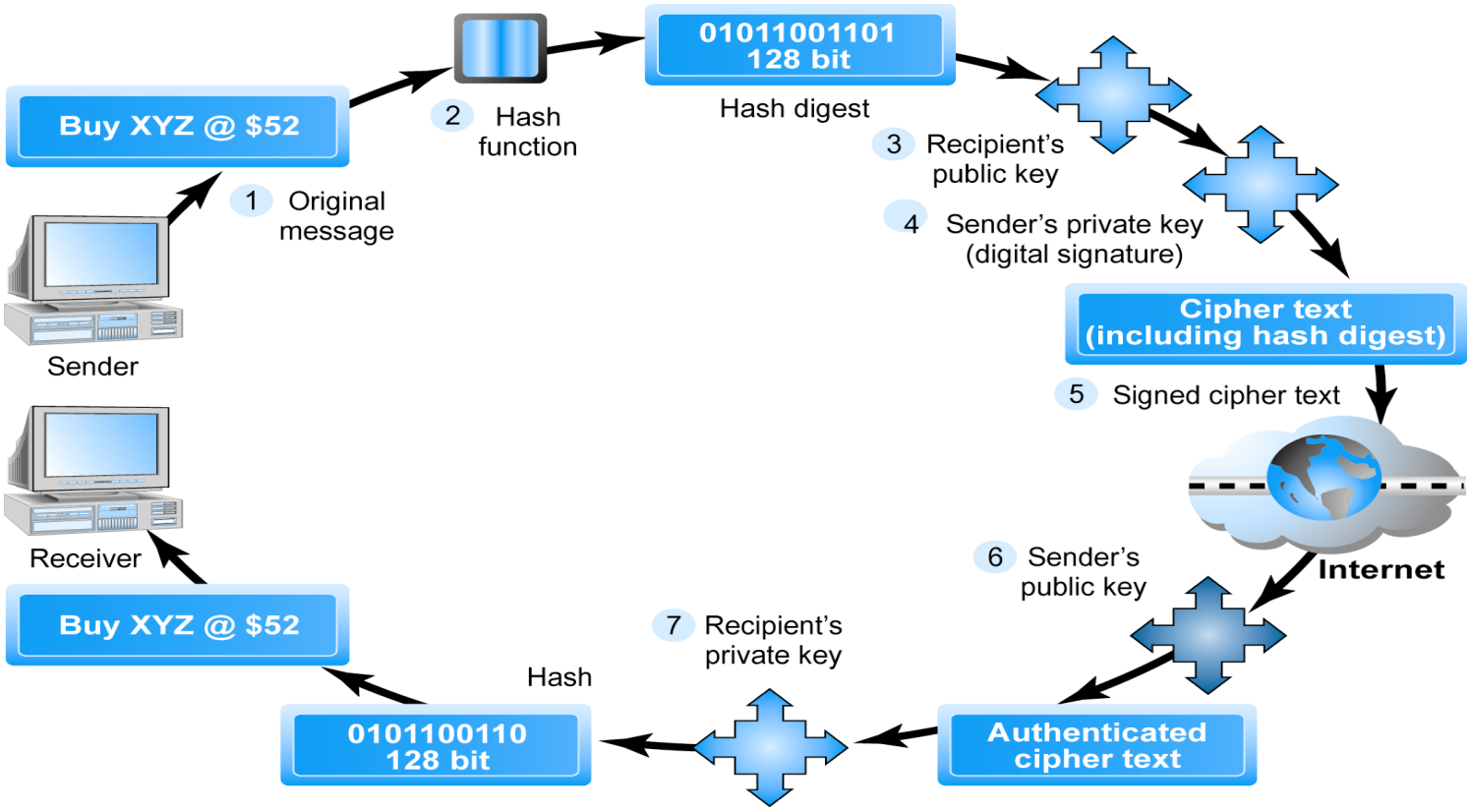


- Asymmetric key video

Public Key Encryption using Digital Signatures and Hash Digests

- Application of hash function (mathematical algorithm) by sender prior to encryption produces hash digest that recipient can use to verify integrity of data
- Double encryption with sender's private key (digital signature) helps ensure authenticity and nonrepudiation

Public Key Cryptography with Digital Signatures

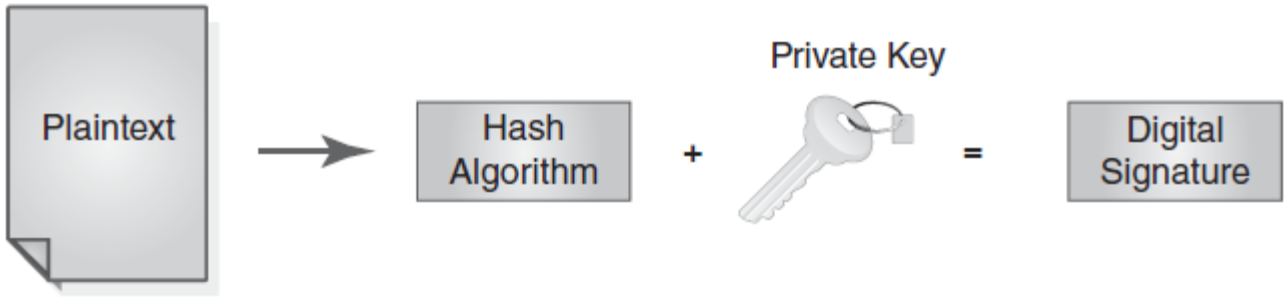


Hash Functions

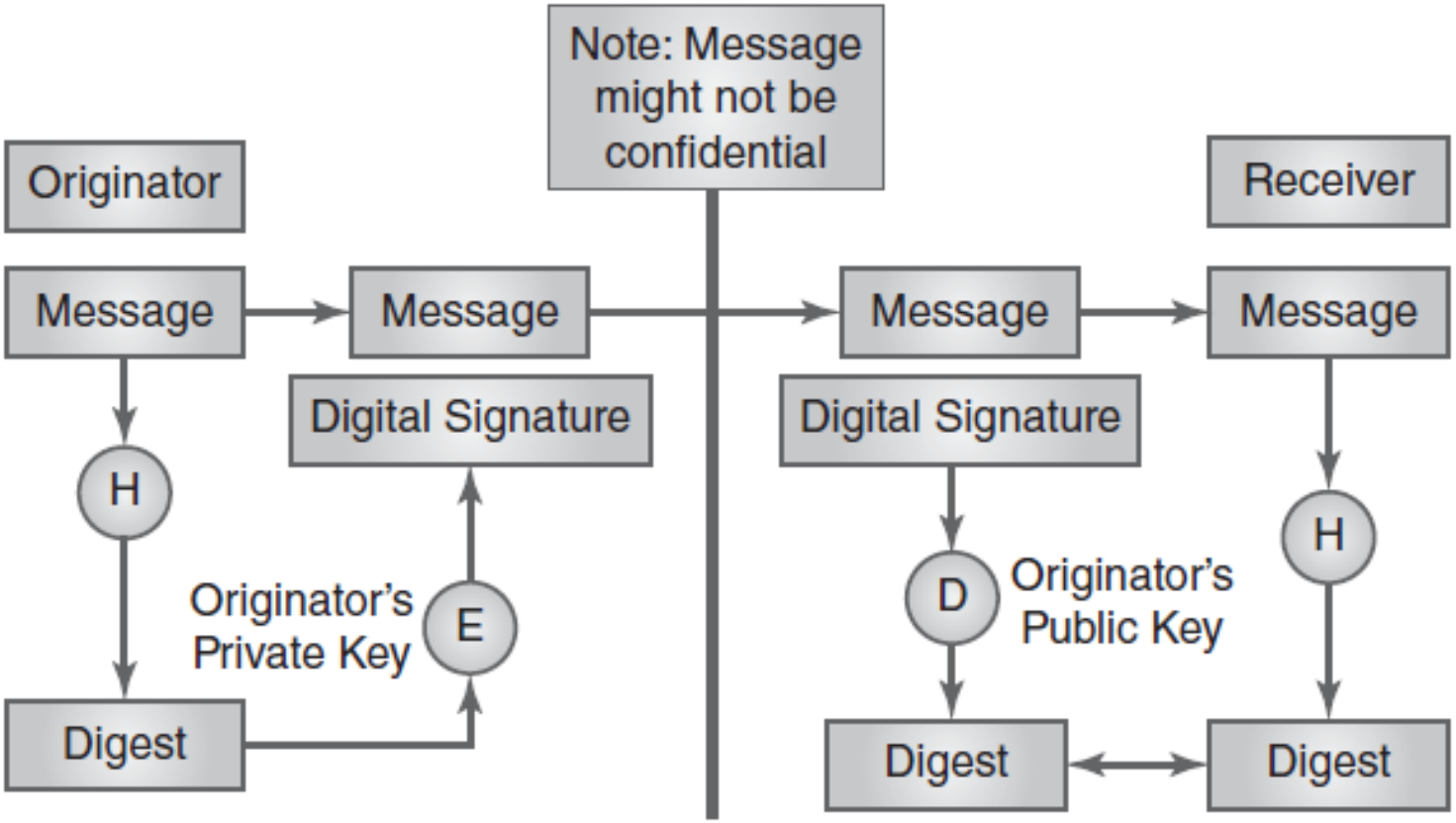
- Checksum
  - Summary information appended to a message to ensure that the values of the message have not changed
- Hash
  - Like a checksum but operates so that a forged message will not result in the same hash as a legitimate message
  - Is usually a fixed size
  - Acts as a fingerprint for data

Digital Signatures

- Bind the identity of an entity to a particular message or piece of information
- Ensure the integrity of a message and verify who wrote it
- Require asymmetric key cryptography



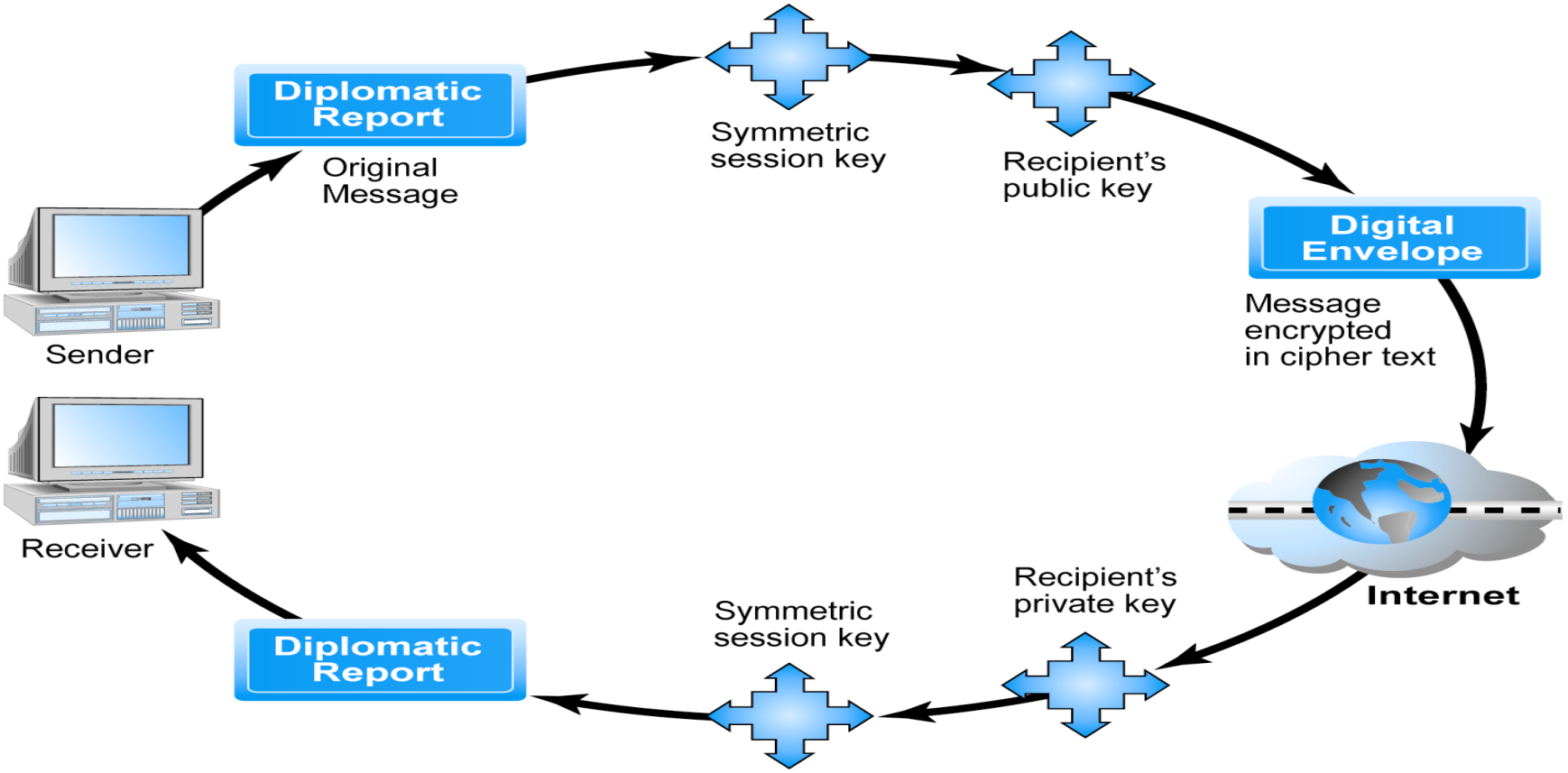
How a Digital Signature Works



Digital Envelopes

- Addresses weaknesses of public key encryption (computationally slow, decreases transmission speed, increases processing time) and symmetric key encryption (faster, but more secure)
- Uses symmetric key encryption to encrypt document but public key encryption to encrypt and send symmetric key

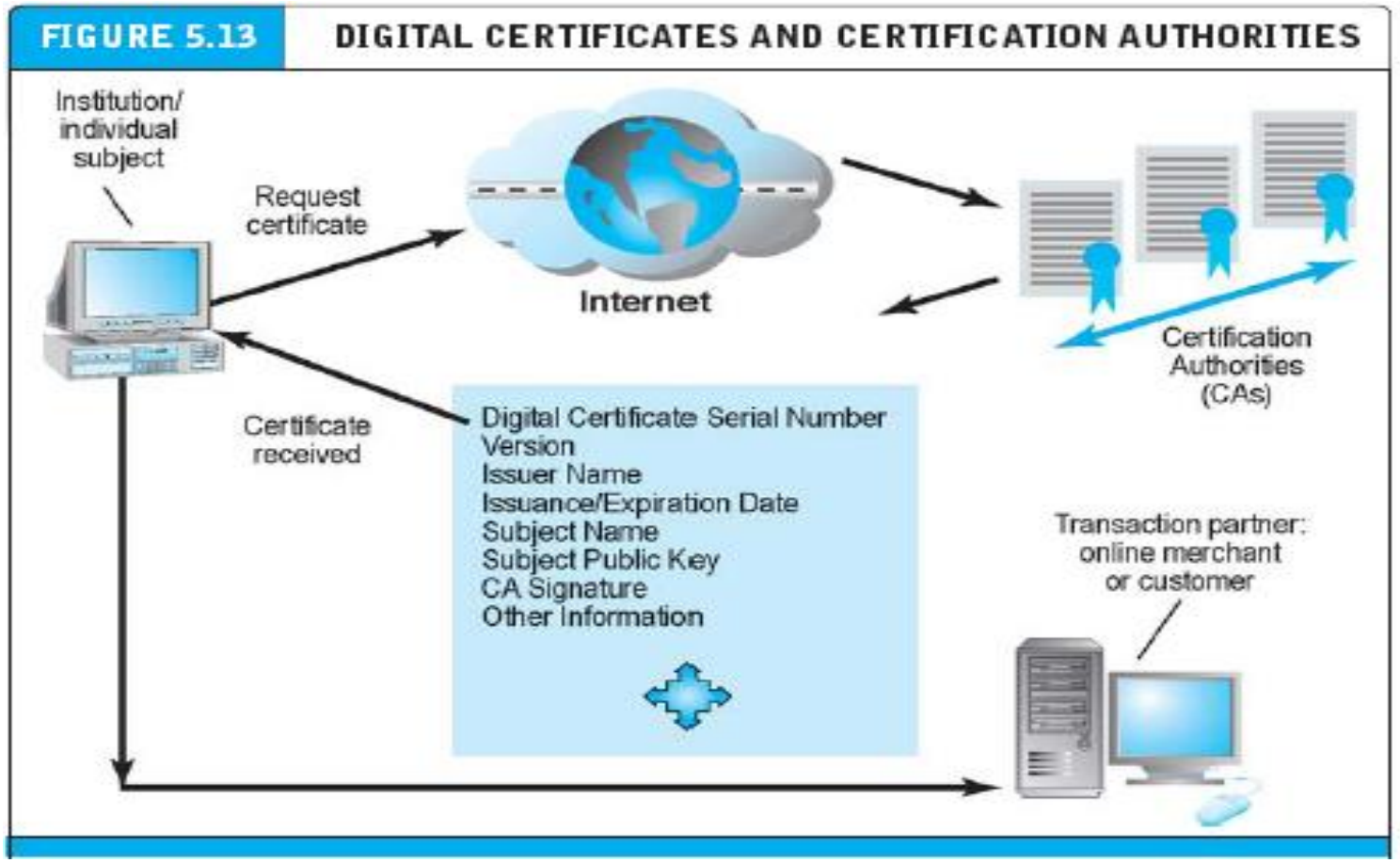
Public Key Cryptography: Creating a Digital Envelope



Digital Certificates and Public Key Infrastructure (PKI)

- Digital certificate includes:
  - Name of subject/company
  - Subject's public key
  - Digital certificate serial number
  - Expiration date
  - Issuance date
  - Digital signature of certification authority (trusted third party institution) that issues certificate
  - Other identifying information
- Public Key Infrastructure (PKI): refers to the CAs and digital certificate procedures that are accepted by all parties

Digital Certificates and Certification Authorities



Limits to Encryption Solutions

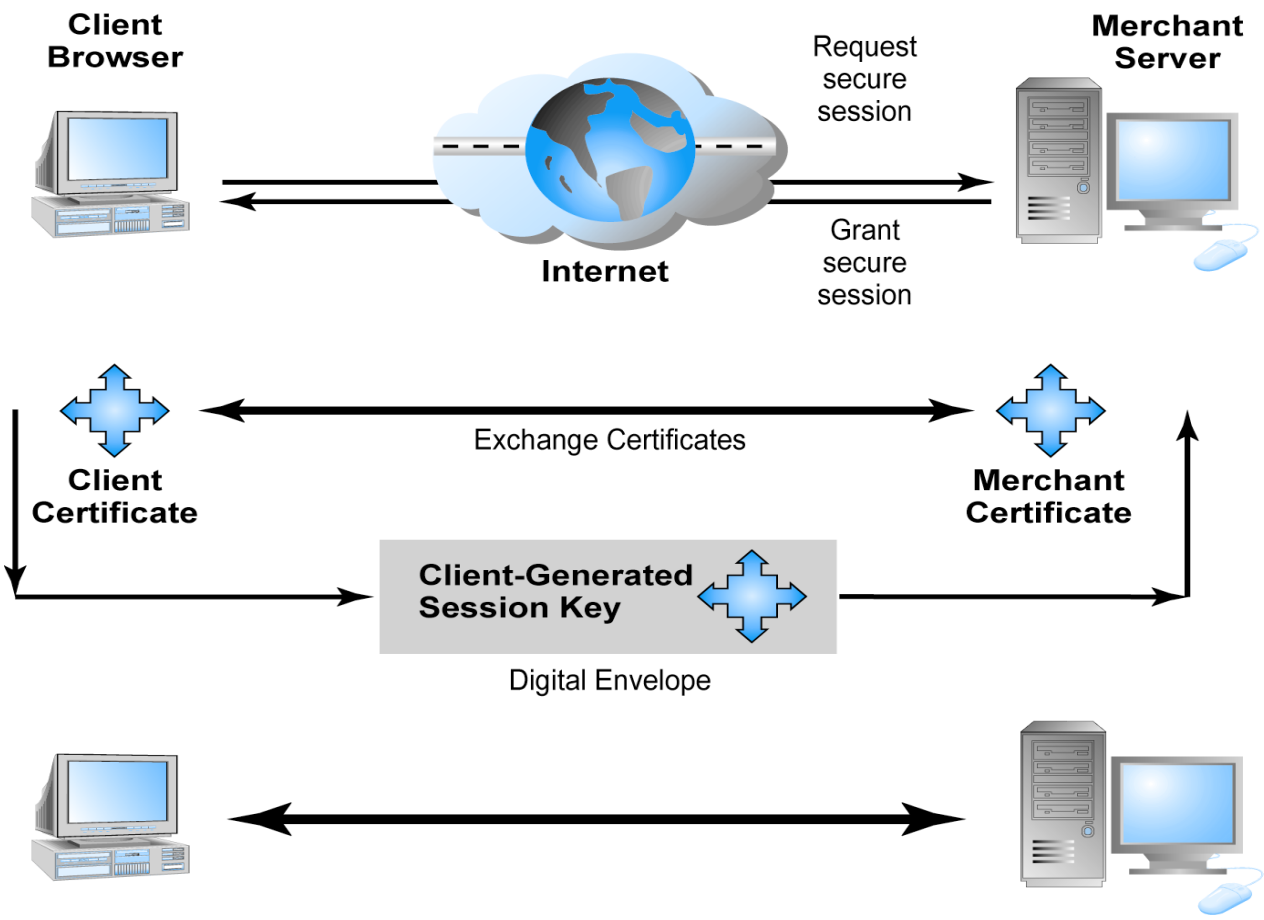
- PKI applies mainly to protecting messages in transit
- PKI is not effective against insiders
- Protection of private keys by individuals may be haphazard
- No guarantee that verifying computer of merchant is secure
- CAs are unregulated, self-selecting organizations

Securing Channels of Communication

- Secure Sockets Layer (SSL): Most common form of securing channels of communication; used to establish a secure negotiated session (client-server session in which URL of requested document, along with contents, is encrypted)
- S-HTTP: Alternative method; provides a secure message-oriented communications protocol designed for use in conjunction with HTTP
- Virtual Private Networks (VPNs): Allow remote users to securely access internal networks via the Internet, using Point-to-Point Tunneling Protocol (PPTP)

- Ssl video

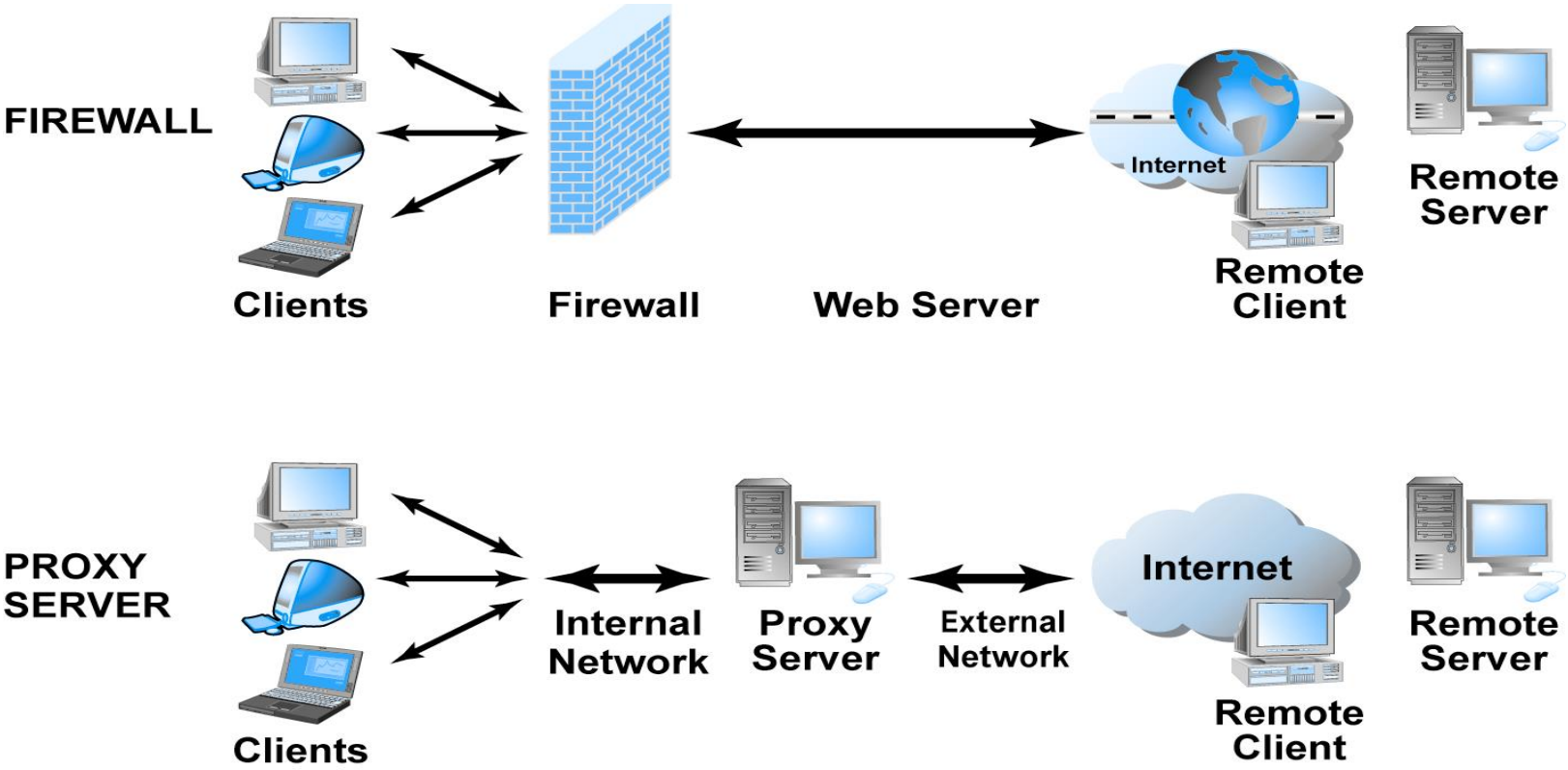
Secure Negotiated Sessions Using SSL



Protecting Networks: Firewalls and Proxy Servers

- **Firewall:** Hardware or software filters communications packets; prevents some packets from entering the network based on a security policy
- Firewall methods include:
  - Packet filters
  - Application gateways
- Proxy servers: Software servers that handle all communications originating from or being sent to the Internet

Firewalls and Proxy Servers



Cryptographic Applications and Uses in Information System Security

Security product and service categories:

- Anti-malware
- Forensics
- ID management
- Messaging safeguards
- Patch management
- Perimeter defenses
- Transaction security (digital certificates, secure file transfer)
- Wireless security

Cryptographic Applications and Uses in Information System Security

- Authentication tools include tokens, smart cards, biometrics, passwords, and password recovery
- Access control and authorization includes firewalls, timestamping, single sign-on, identity management, and mobile device security
- Assessment and auditing tools include vulnerability-assessment scanners, penetration testing tools, forensic software, and log analyzers

Cryptographic Applications and Uses in Information System Security

- Security management products include tools for enterprise security management, configuration and patch management, and security policy development
- Wireless security tools encrypt data to protect them in transit and to limit access to authorized people
- Encryption tools include line encryption, database security products, virtual private networks (VPNs), public key infrastructure (PKI), and crypto accelerators

Symmetric Key Standards

- Data Encryption Standard (DES)
- Triple DES (3DES)
- International Data Encryption Algorithm (IDEA)
- CAST
- Blowfish
- Advanced Encryption Standard (AES)
- RC2
- RC4

Wireless Security

- Wireless products have built-in security, the default configuration generally doesn't enable it; they expect customers to enable it
- 802.11 wireless security (Wi-Fi) provides wireless communications at transmission speeds from 11 Mbps for 802.11b, to over 780 Mbps for 802.11ac, and 100 Gbps for 802.11ay
- 802.11 wireless protocols allow encryption through Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA)
  - WEP has limitations and shouldn't be used

Asymmetric Key Solutions

An asymmetric key solution doesn't require each party to first share a secret key

The **key directory** is a trusted repository of all public keys

A **key escrow** is a key storage method that allows some authorized third party access to a key under certain circumstances

Asymmetric Key Solutions

- The **SSL Handshake Protocol** consists of two phases: server authentication and an optional client authentication
- Digital signatures verify a person's identity or that person's association with a message
- A **certificate authority (CA)** vouches for the validity of a credential, and maintains a list of invalid, or revoked, certificates in either a certificate revocations list (CRL) or by maintaining the data to support the newer online certificate status protocol (OCSP)

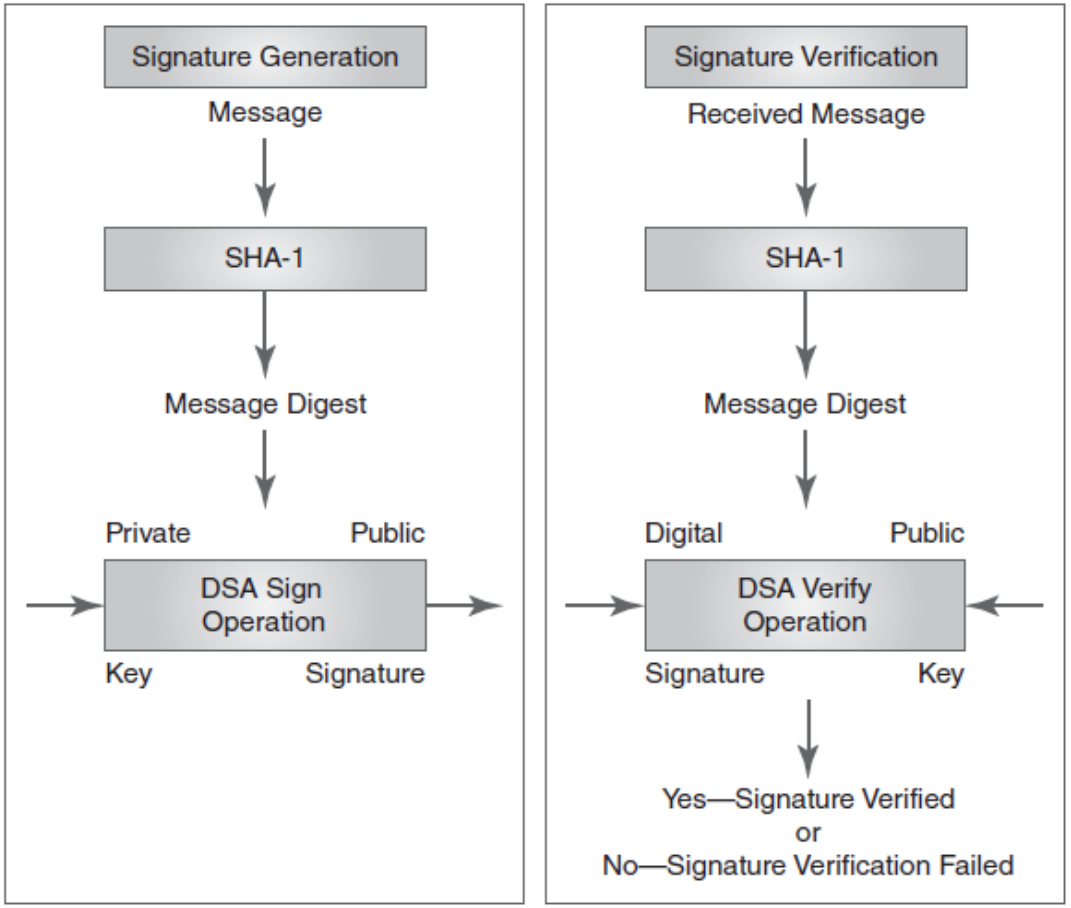
Hash Function and Integrity

- Hash functions:
  - Help detect forgeries
  - Compute a checksum of a message
  - Combine the checksum with a cryptographic function so that the result is tamperproof
- A hash is:
  - A checksum designed so that no one can forge a message in a way that will result in the same hash as a legitimate message
  - Usually a fixed size, resulting in a hash value, which is larger than checksum values

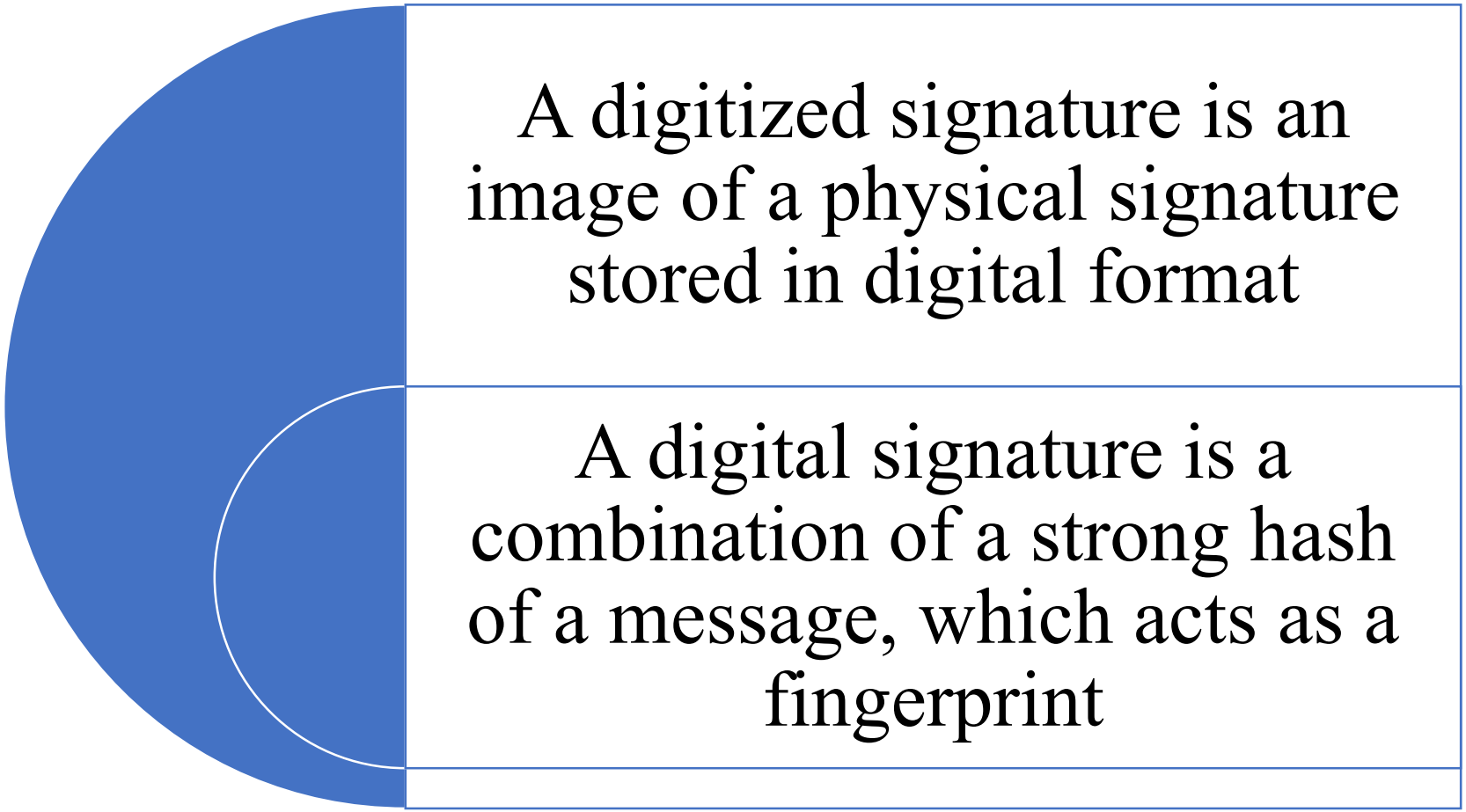
Hashing Algorithms

- **MD5 message digest algorithm**—Takes an input of any arbitrary length and generates a 128-bit message digest that is computationally infeasible to match by finding another input
- **Secure Hash Algorithm (SHA-1)**—Produces a 160-bit hash from a message of any arbitrary length
- **Hash message authentication code (HMAC)**—A hash function that uses a key to create the hash, or message digest
- **RACE Integrity Primitives Evaluation Message Digest (RIPEMD)**—A collection of functions that provide hash values for a wide range of applications

Relationship Between Hash and Digital Signature Algorithms



Digital Signatures and Nonrepudiation



Conditions for Proving Nonrepudiation

- An effective asymmetric key algorithm
- A strong hash function
- A means to apply the private encryption key to the hash value to produce a digital signature
- A tamperproof or trusted third-party timing device
- An agreed-upon protocol for validating digital signatures
- A secure key management and distribution system
- A public key repository with an assured level of integrity
- Key escrow to be able to produce public keys from reluctant parties
- Procedures to handle disputes

Principles of Certificates and Key Management

The best key management system in the world does not protect against a brilliant cryptanalyst if the encryption algorithm itself has any weaknesses

Modern Key Management Techniques

- Advanced Encryption Standard (AES)
- Internet Protocol Security (IPSec)
- The Internet Security Association and Key Management Protocol (ISAKMP)
- Extensible Markup Language (XML) key management specification (XKMS)
- Managed public key infrastructure (PKI)
- American National Standards Institute (ANSI) X9.17

Summary

- Basics of cryptography
- Business applications of cryptography
- Symmetric and asymmetric key cryptography
- Encryption mechanisms and techniques
- Certificate and key management

- https://planetcalc.com/1434/
- https://planetcalc.com/2468/
- https://www.cs.du.edu/~snarayan/crypt/vigenere.html
- https://8gwifi.org/CipherFunctions.jsp
- https://www.devglan.com/online-tools/rsa-encryption-decryption
- http://www.fileformat.info/tool/hash.htm
- http://www.pro-technix.com/information/crypto/pages/vernam_base.html
- https://www.modsecurity.org/
- https://twofactorauth.org/
- https://github.com/stephenhaunts/SafePad
- https://www.iptrackeronline.com
- https://nmap.org/
- https://nmap.org/zenmap
- https://www.ipswitch.com/resources/free-tools/

- http://www.hping.org/
- https://packetfence.org/
- https://www.wireshark.org/
- https://siemonster.com/
- https://www.logfusion.ca/
- https://www.netwrix.com
- https://logrhythm.com/
- https://correlog.com/
- https://www.sumologic.com/
- https://www.sumologic.com/
- https://cybersecurity.att.com/
- https://www.aircrack-ng.org/
- https://breachalarm.com/
- https://haveibeenpwned.com/
- https://www.browserling.com/
- https://github.com/gorhill/uBlock

http://www.getlinkinfo.com/
https://www.url2png.com/
http://browsershots.org
https://wheregoes.com/
https://www.comodo.com
https://www.ghostery.com/
https://www.e?.org/https-everywhere
https://disconnect.me/
https://sitecheck.sucuri.net/
https://scanurl.net/
http://quttera.com/
http://scr.im/
https://www.spam?ghter.com
https://www.spamihilator.com/en/
https://www.mailwasher.net/
https://spambully.com/

Messaging Tools – End to End Encryption

https://signal.org/
https://otr.cypherpunks.ca/index.php
https://www.tinc-vpn.org/
https://www.tinc-vpn.org/
https://www.softether.org/
https://www.strongswan.org/
https://www.qubes-os.org/
http://www.samurai-wtf.org/
http://www.pythonsecurity.org/

- **Free Cybersecurity Tools for Reconaissance**
- https://tools.kali.org/information-gathering/theharvester
- https://www.zaproxy.org/
- https://www.paterva.com/
- https://www.tenable.com/nessus
- https://www.cvedetails.com/
- http://www.oxid.it
- https://www.lastpass.com/
- https://ophcrack.sourceforge.io/
- https://duo.com/

OBJECTIVE	AUTHENTICATION	ACCESS CONTROL	ASSESSMENT AND AUDIT	SECURITY MANAGEMENT	NETWORK SECURITY	CONTENT FILTERING	ENCRYPTION	ADMINISTRATION	CONSULTANTS
Privacy or confidentiality		X			X		X	X	X
Integrity				X	X		X	X	X
Entity authentication or identification	X	X			X		X	X	X
Message authentication	X				X		X		
Signature	X				X		X	X	
Authorization	X	X			X				
Validation		X	X	X				X	
Access control	X	X		X	X	X	X	X	
Certification			X	X			X		X
Timestamping		X			X		X		
Witnessing			X				X		X
Receipt					X			X	
Confirmation					X			X	
Ownership			X				X	X	X
Anonymity							X	X	
Nonrepudiation					X		X	X	X
Revocation	X				X		X		

THANK YOU