



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ACCA5034

Data Security and Compliance Week 9 : Cryptography

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Learning Objective(s) and Key Concepts

Learning Objective(s)

- Explain how businesses apply cryptography in maintaining information security.

Key Concepts

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

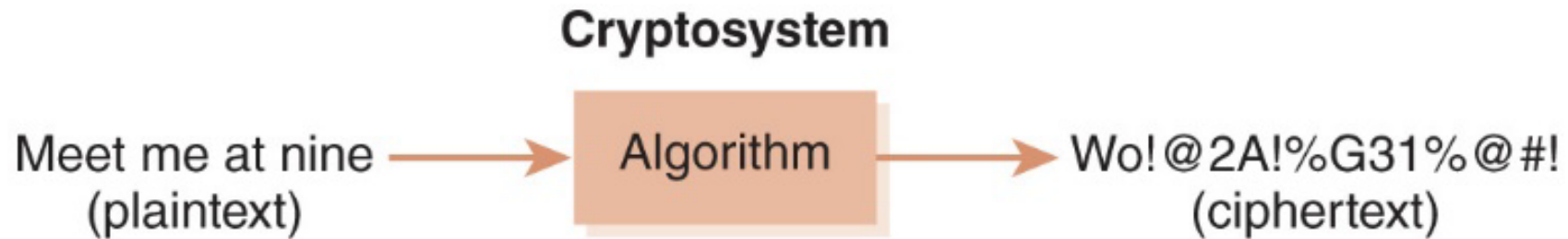
What Is Cryptography?

- 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

What Is Cryptography?

- Algorithm
 - A repeatable process that produces the same result when it receives the same input
- Cipher
 - An algorithm to encrypt or decrypt information
- Hash
 - Useful for protecting data from unauthorised changes

What Is Cryptography?



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

- Goal of cryptography
 - Make the cost or the time required to decrypt ciphertext without the key exceed the value of the protected information
- Keyspace
 - The number of possible keys to a cipher
- Open-source 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 World Wars I and II
- Symmetric and asymmetric key cryptography introduced in 1976
- Quantum cryptography uses photons, particles, or waves of light, and their unique properties transmitted across an optical fiber channel to create an unbreakable cryptosystem

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
 - Authorisation
 - Access control
- Security in business relationships
 - Message authentication
 - Signature
 - Receipt and confirmation
 - Nonrepudiation
- Security measures that benefit everyone
 - Anonymity
 - Timestamping
 - Revocation
 - Ownership
 - High resiliency
 - Supporting obfuscation

Cryptographic Principles, Concepts, and Terminology

- Security objectives are many and varied.
- It is important to understand how they work together and how they oppose one another.
- One of the best summaries (next slide) of these objectives is found in the Handbook of Applied Cryptography.
- These objectives represent most of the goals of security initiatives, including cryptography.

Information Security Objectives

Objective	Steps to Take
Privacy or confidentiality	Keep information secret from all unauthorized users.
Integrity	Ensure that unauthorised users or unknown processes have not altered information.
Entity authentication or identification	Corroborate the identity of an entity (e.g., a person, a computer terminal, or a credit card).
Message authentication	Corroborate the source of information; authenticate the data's origin.
Signature	Bind information to an entity.
Authorization	Convey an official sanction to do or be something to another entity.

Information Security Objectives

Objective	Steps to Take
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.
Receipt	Acknowledge that the recipient received information.

Information Security Objectives

Objective	Steps to Take
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 a 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.

Security Implementations for Businesses

- General classifications of security products and services
 - Authentication (non-PKI [public key infrastructure])
 - Access control/authorization
 - Assessment and audit
 - Security management products
 - Perimeter/network security/availability
 - Content filtering
 - Encryption
 - Administration/education
 - Outsource services/consultants

Cryptographic 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 is shifted 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

Product and Exponentiation Ciphers

- Product Cipher
 - Combination of multiple ciphers, each of which could be a transposition or substitution cipher
 - Example: Data Encryption Standard (DES)
- Exponentiation Cipher
 - Involves computing exponentials over a finite mathematical field and relies on the difficulty of factoring large numbers
 - Example: Rivest–Shamir–Adelman (RSA)

Symmetric and Asymmetric Key Cryptography

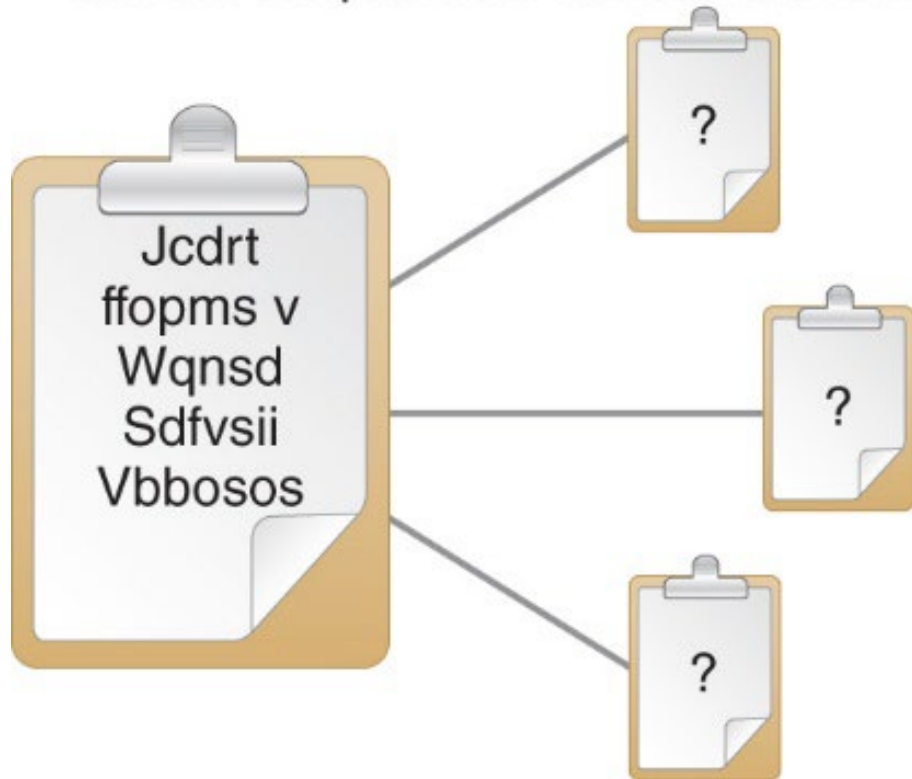
- Symmetric key ciphers use the same key to encrypt plaintext into ciphertext and then to decrypt ciphertext back into plaintext.
- Asymmetric key ciphers have four key properties:
 - Two associated algorithms that are inverses of each other exist.
 - Each algorithm is easy to compute.
 - It is computationally 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:
 - Analysing the ciphertext to find the plaintext or key
 - Analysing 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

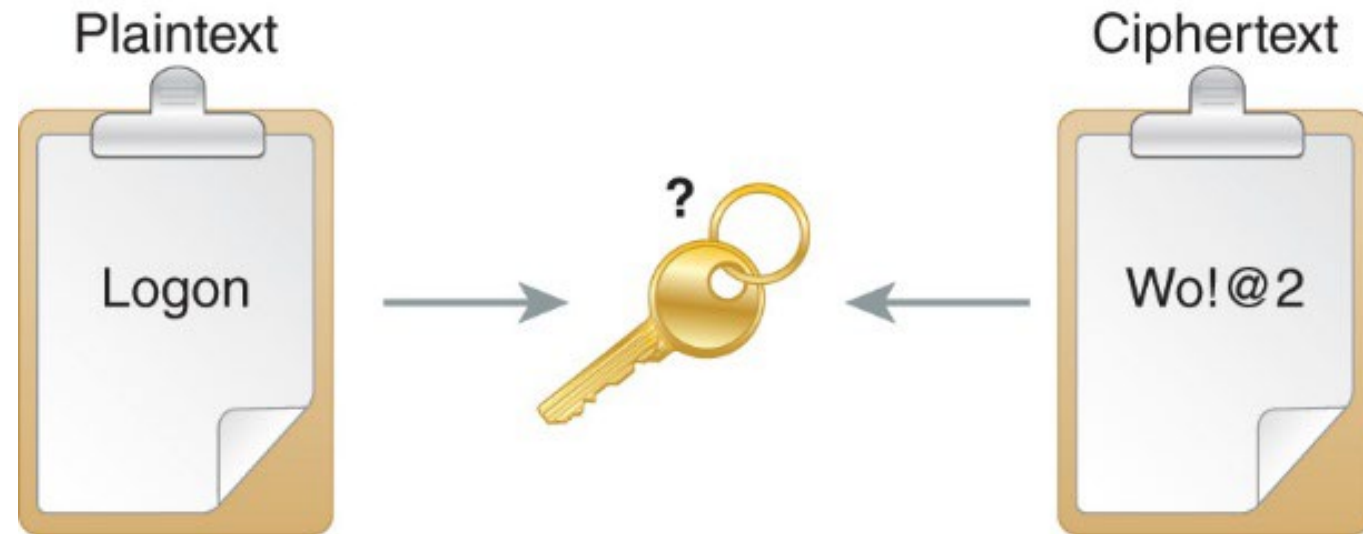
COA

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



KPA

The ciphertext and the corresponding plaintext are both available.



Symmetric and Asymmetric Key Cipher Resistance to Attack

- Cryptanalysis objectives:
 - Derive the plaintext of a target message.
 - Determine the key used to encrypt a target message.
 - Derive the algorithm used by a particular cipher.
 - Solve the general mathematical problem underlying the cryptography.

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

- Paper
- Digital media
- Hardware

Key Distribution Centres

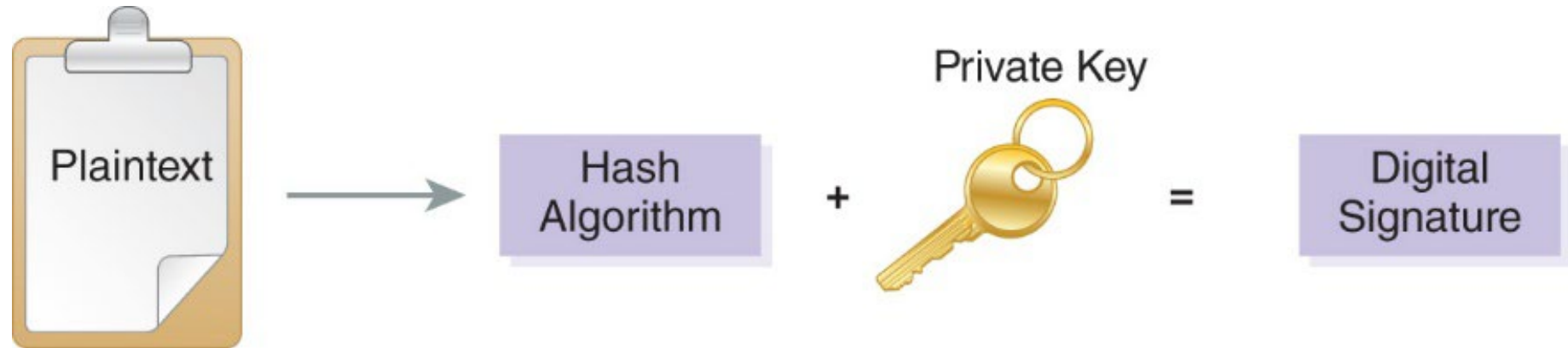
- Rather than each organization creating the infrastructure to manage its own keys, hosts could agree to trust a common key-distribution centre (KDC)
- All parties must trust the KDC
- With a KDC, each entity requires only one secret key pair—between itself and the KDC
- Kerberos and ANSI X9.17 use the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

Digital Signatures and Hash Functions

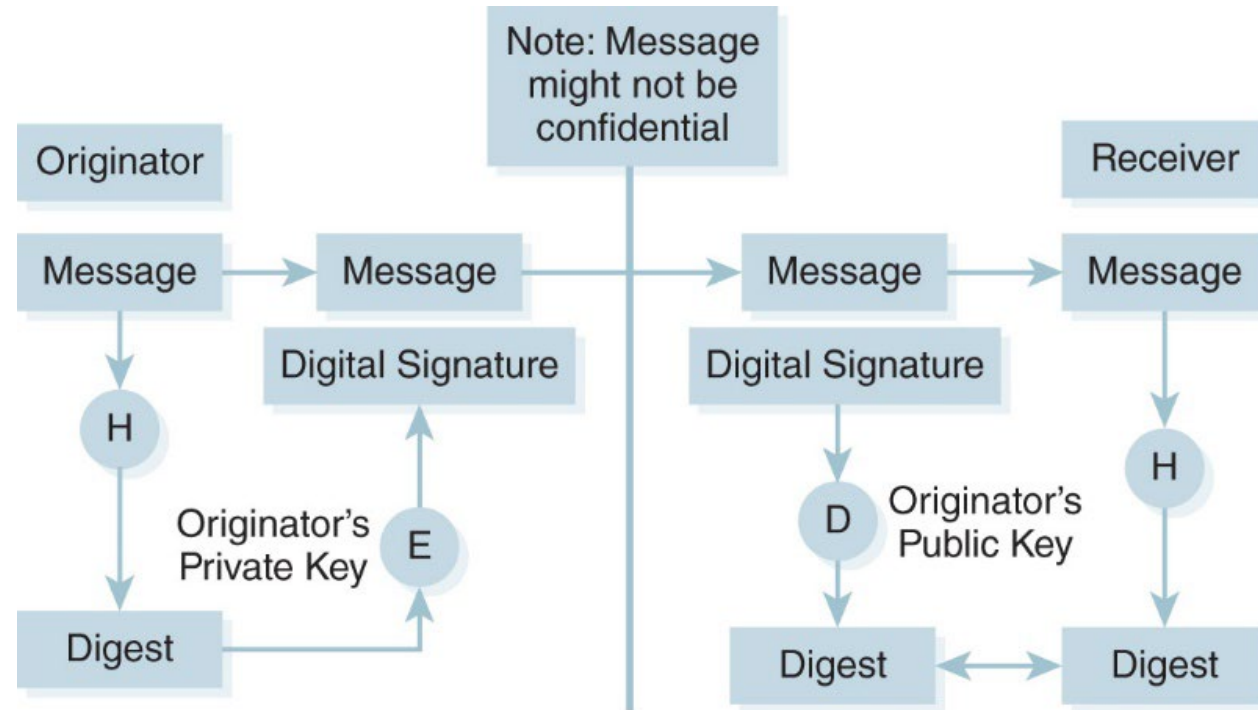
- Hash functions
 - Checksum
 - Summary information appended to a message to ensure that the values of the message have not changed
 - Hash
 - Like a checksum but operates so that a forged message will not result in the same hash as a legitimate message
 - Is usually a fixed size
 - Acts as a fingerprint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



Operation of a Digital Signature



Cryptographic Applications and Uses in Information System Security

- Security product and service categories
 - Anti-malware
 - Compliance/auditing
 - Forensics
 - ID management
 - Intellectual property
 - Managed security service providers (MSSPs)
 - Messaging safeguards
 - Patch management
 - Perimeter defenses
 - Security information and event management (SIEM) and incident response
 - Transaction security (e.g., digital certificates and secure file transfer)
 - Wireless security
 - Blockchain technology

Cryptographic Applications and Uses in Information System Security (2 of 4)

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

Cryptographic Applications and Uses in Information System Security (3 of 4)

- 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
- Email security tools often involve encrypting data in transit and sometimes at rest

Cryptographic Applications and Uses in Information System Security (4 of 4)

- Content filtering includes antivirus products, mobile code scanners, web filters, and spam blockers, all of which typically do not use encryption, although databases of threat signatures may be encrypted
- Encryption tools include line encryption, database security products, VPNs, PKI, and crypto accelerators

Symmetric Key Standards

- 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, default configuration generally doesn't enable it; vendors expect customers to enable it
- 802.11 wireless (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

Wireless Security

- 802.11 wireless protocols allow encryption through Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA), WPA2, and WPA3
- WEP has limitations and should not be used

Asymmetric Key Solutions

- An asymmetric key solution does not 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.

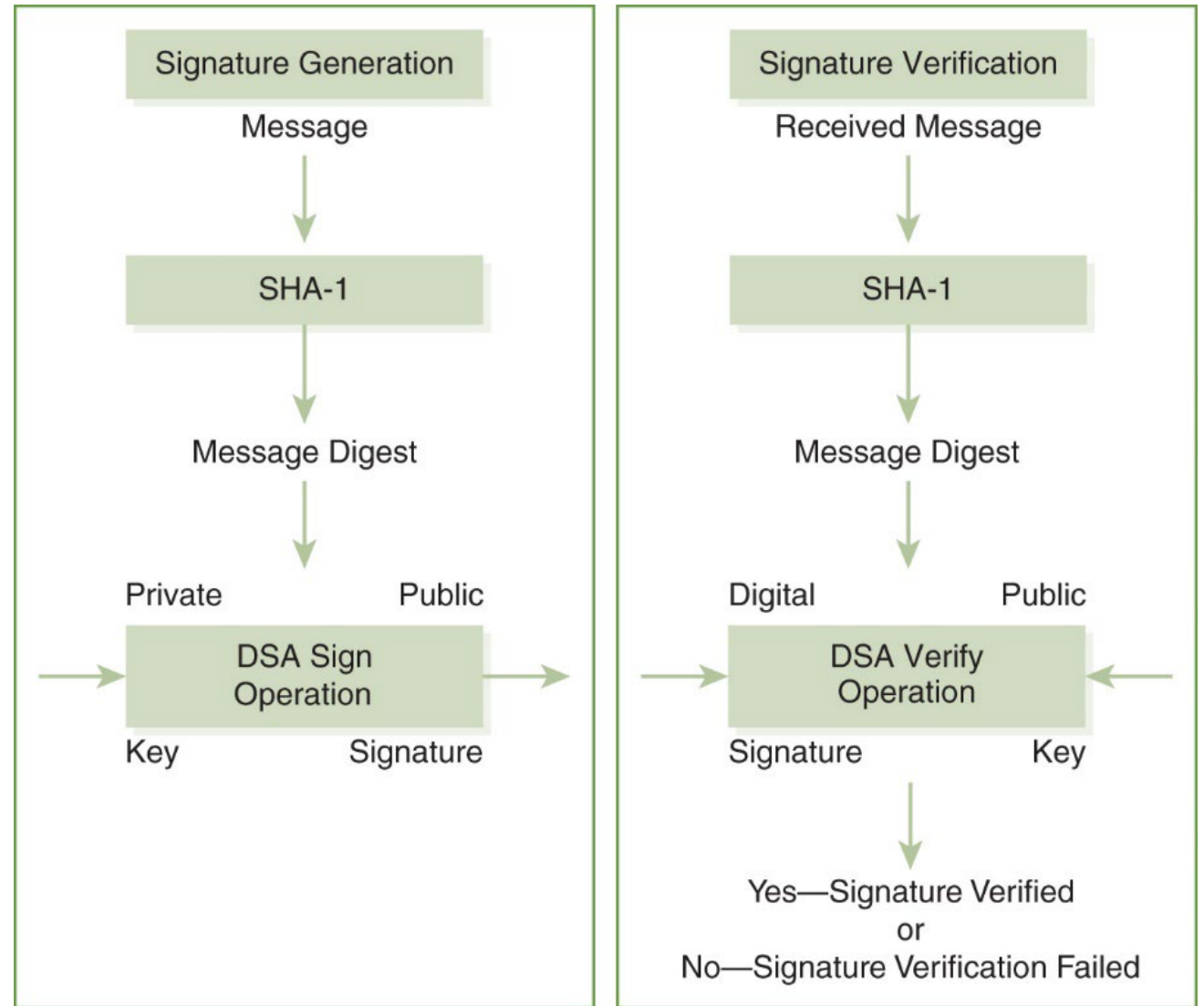
Hash Function and Integrity

- 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:
 - 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

Hash Function and Integrity

- 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



Modern Key Management Techniques

- Advanced Encryption Standard (AES)
- Internet Protocol Security (IPSec)
- Managed public key infrastructure (PKI)

Summary

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

References

- Slides are devised from the recommended books:
 - Whitman & Mattord, Principles of Information Security, 6th Edition
 - Chapter 10: Cryptography



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk