ACS-2821-001
Information Security in Business

Cryptography

ACS-2821-001 – Slides Used In The Course

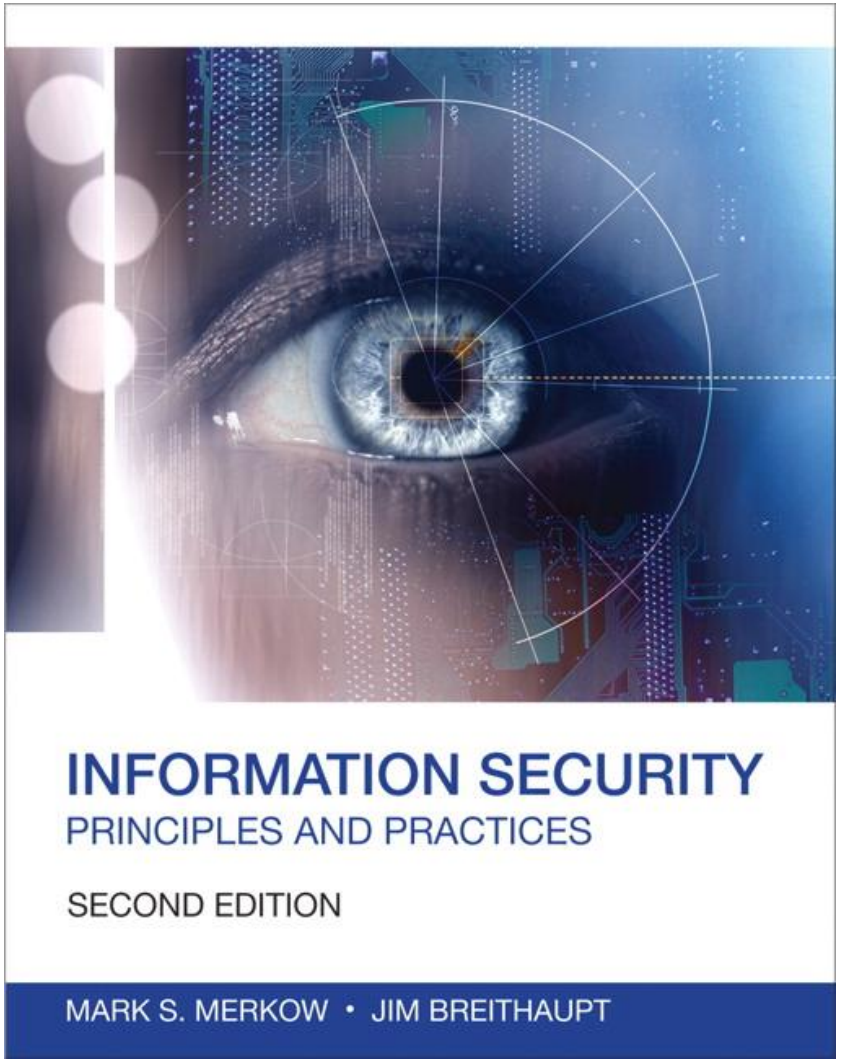
THE UNIVERSITY OF WINNIPEG

A note on the use of these slides:

These slides has been adopted and/or modified from the original for the use in this course. The author of the text have make these slides available to all (faculty, students, readers) and they obviously represent a *lot* of work on their part.

In return for use, please:

- If slides are being used (e.g., in a class) that the source be mentioned (after all, the author like people to use our book!)
- If any slides are being posted on a www site, note that they are adapted from (or perhaps identical to) the author original slides, and note their copyright of this material.



Objectives

- Explain common terms used in the field of cryptography
- Outline what mechanisms constitute a strong cryptosystem
- Demonstrate how to encrypt and decrypt messages using the transposition method
- Demonstrate how to encrypt messages using the substitution method
- Support the role of cryptography in e-commerce systems
- Explain the differences between symmetric and asymmetric cryptography
- Outline the mechanisms used for digital signatures
- Explain the purpose and uses of digital certificates
- Evaluate commercial implementations of public key infrastructure (PKI) products

Overview

- Because most computer application-level security relies on cryptography, it is essential to have a strong understanding of cryptography technologies

Brief History on Cryptology

- Cryptography is a systematic study of cryptology as a science (and perhaps an art)
- Has been used for thousands of years to hide secret messages
- First recorded evidence in the use of cryptography was found in around 1900 BC in Egypt in the main chamber of the tomb of the nobleman Khnumhotep II
- Around 100 BC, a substitution cipher, known as Caesar cipher created by Julius Caesar was use to convey secret messages to his army generals posted in the war front
- In the 16th century, Vigenere was the first to design a cipher that used an encryption key

Brief History on Cryptology

- At the start of the 19th century, Edward Hebern designed an electro-mechanical contraption which was called the Hebern rotor machine
  - It uses a single rotor
  - the secret key is embedded in a rotating disc
  - The key encoded a substitution table
  - With each key press from the keyboard resulted in the output of cipher text
  - By rotating the disc by one notch and a different table would then be used for the next plain text character

Brief History on Cryptology

- The Engima machine invented by German engineer Arthur Scherbius
  - Heavily used by the German forces during the Second World War
  - The Enigma machine used 3 or 4 or even more rotors.
  - The rotors rotate at different rates as you type on the keyboard and output appropriate letters of cipher text
  - The key was the initial setting of the rotors
  - The Enigma machine was eventually broken by British cryptographers at Bletchley Park (Watch the movie “Imitation Game”)

Brief History on Cryptology

- Early 1970's, IBM realized the importance of encryption and formed a "crypto group" headed by Horst-Feistel.
  - Designed a cipher called Lucifer
  - In 1973, NIST (at the time it was called Nation Bureau of Standards) request for proposals for a block cipher
  - Lucifer was eventually accepted and was called DES or the Data Encryption Standard
  - In 1997, and in the following years, DES was broken by an exhaustive search attack
  - DES problem was the small size of the encryption key and as computing power increased it became easy to brute force different combinations of the key to obtain a possible plain text message.

Brief History on Cryptology

- In 1997, NIST again request for proposal for a new block cipher
  - It received 50 submissions and accepted Rijndael's proposal, it was named as AES or the Advanced Encryption Standard
- Through out history is has taught us that
  - secrecy of your message should always depend on the secrecy of the key, and not on the secrecy of the encryption system
  - Always use ciphers that have been publicly reviewed and have been established as a standard

Applying Cryptography to Information Systems

- Applied cryptography—the science of secret writing—enables the storage and transfer of information in forms that reveal it only to those permitted to see it, while hiding it from everyone else
- In the 20th century, international governments began to use cryptography to protect their private and sensitive information and for communications purposes
- Since the 1970s, academic interest in cryptography has grown at a tremendous rate, and private citizens have increasingly gained access to various cryptography techniques, permitting personal information protection and enabling the conduct of secure electronic transactions

Basic Terms and Concepts

- Cryptology is the umbrella study of cryptography and cryptanalysis
- Cryptosystems disguise messages, allowing only selected people to see through the disguise
- Cryptography is the science (or art) of designing, building, and using cryptosystems
- Cryptanalysis is the science (or art) of breaking a cryptosystem

Basic Terms and Concepts

Cryptographers use two basic methods:

- Substitution: letters are replaced by other letters and/or symbols
- Transposition: Letters are rearranged into a different order

Plaintext

- The original message or data that is fed into the encryption algorithm as input

Encryption algorithm

- The encryption algorithm performs various substitutions and transformations on the plaintext

Secret key

- The secret key is also input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key

Basic Terms and Concepts

Ciphertext

- This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts

Decryption algorithm

- This is essentially the encryption algorithm run inreverse. It takes the ciphertext and the secret key and produces the original plaintext

Substitution and Transposition Ciphers

Substitution Cipher

- Atbash cipher
- Pigpen cipher
- Affine cipher
- Caesar shift cipher
- Homophonic substitution cipher
- …

Transposition Cipher

- Rail Fence cipher
- Route cipher
- Columnar transposition cipher
- Myszkowski transposition cipher
- Peermutation transposition cipher
- …

Substitution Cipher - Example

Caesar Shift Cipher

- Plaintext = Information Security in Business
- The key is shifting 1 letter over
- Ciphertext = JOGPSNBUJPO TFDVSJUZ JO CVTJOFTT

Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext Alphabet	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

- Plaintext = Information Security in Business
- The key is shifting 2 letter over
- Ciphertext = KPHQTOCVKQP UGEWTKVA KP DWUKPGUU

Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext Alphabet	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

Transposition Cipher - Example

Simple Transposition Cipher

- Plaintext = Information Security in Business
- The key is reverse the order of the letters in a plaintext
- Ciphertext = SSENISUB NI YTIRUCES NOITAMROFNI

- Plaintext = Information Security in Business
- The key is reverse the letters of each word, but not the order in which the words are written
- Ciphertext = NOITAMROFNI YTIRUCES NI SSENISUB

Strength of Cryptosystems

- A strong cryptosystem is considered strong only until it's been cracked
- Strong cryptosystems
  - Produce ciphertext that always appears random to standard statistical tests
  - Also resist all known attacks on cryptosystems
  - Have been brutally tested to ensure their integrity
- Popular cryptosystems have the following common characteristics
  - The algorithms used are public
  - The key is kept secret
    - The longer the key the stronger the cryptosystem

- Each employee must have an ID and password to access the email system, but beyond that, any guarantees of authenticity require trust in the users of the system
- To ensure that electronic commerce is secure, however, requires an implicit distrust in users of the Internet and public networks

The Role of Keys in Cryptosystems

Two basic types of cryptosystems or crypto methods

- **Symmetric key** cryptography
  - Also know as private key or shared secret cryptography
- **Asymmetric key** cryptography
  - Also know as public key cryptography

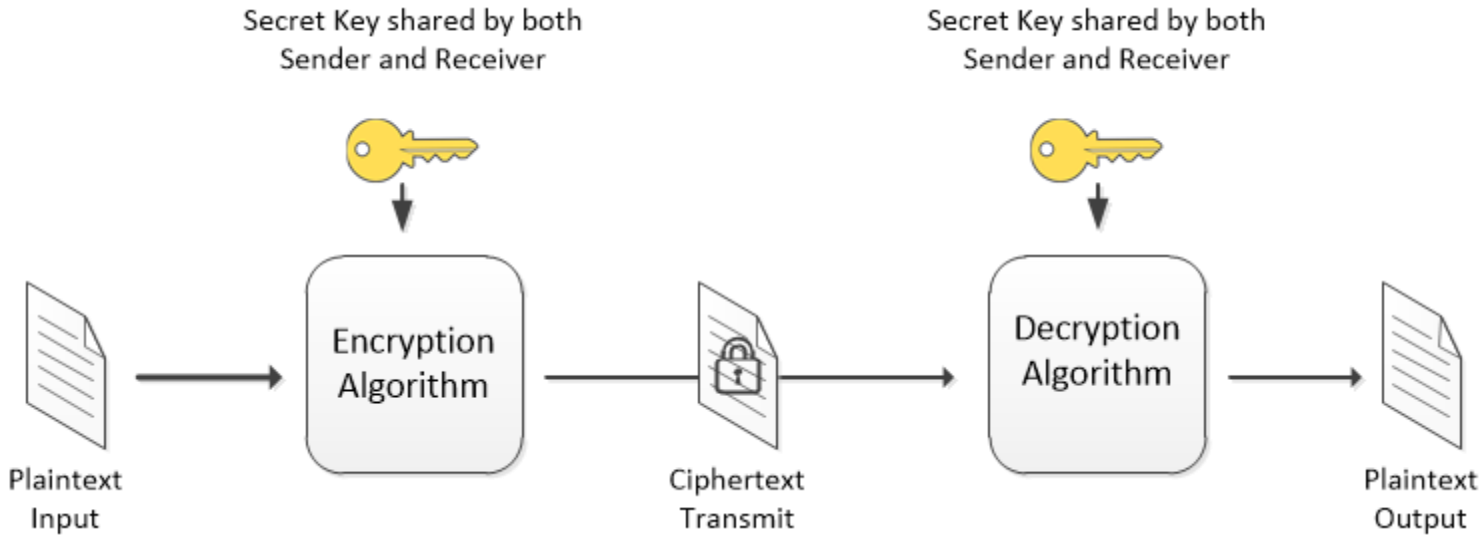
The Role of Keys in Cryptosystems

Symmetric key cryptography (private key or shared secret)

- It uses the same key to both encrypt and decrypt a message
- The most common form of symmetric key cryptography is the Data Encryption Standard (DES), which uses 64 bits of data (8 bytes) with a 56-bit (7 byte) use as the key plus parity bits
- 3DES or Triple DES
  - Uses 128 bit key (16 bytes)
  - Used commonly by banks to encrypt PIN numbers
- Advance Encryption Standard (AES): Replace DES
- One of the most significant challenges of symmetric key cryptography lies in sharing keys prior to needing them

The Role of Keys in Cryptosystems

Symmetric Key Encryption - Simplified



The Role of Keys in Cryptosystems

Asymmetric key cryptography (public key)

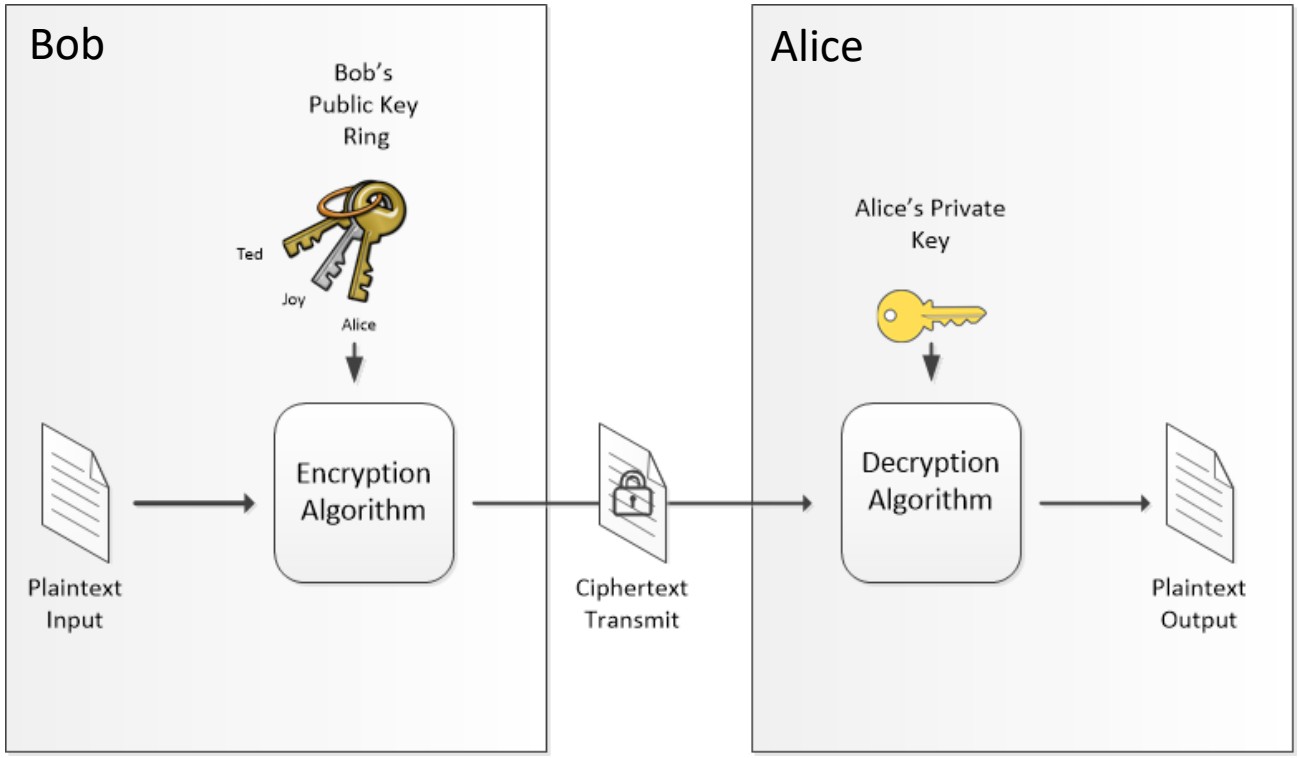
- It uses two (2) keys, a public key and a private key
- The two keys works in pair
  - Typically, the key lengths that are used with strong asymmetric key cryptography are 1024 bits long (128 bytes)
- A message encrypted using one key can only be decrypted using the other key and vice versa
- The public key is shared with everyone you want to communicate with privately, but the private key is kept secret and should not be shared with anyone
- The two keys that compose a pair are mathematically related, but neither can be derived from the other
- RSA (Rivest–Shamir–Adleman) is an example of an asymmetric key cryptography system

The Role of Keys in Cryptosystems

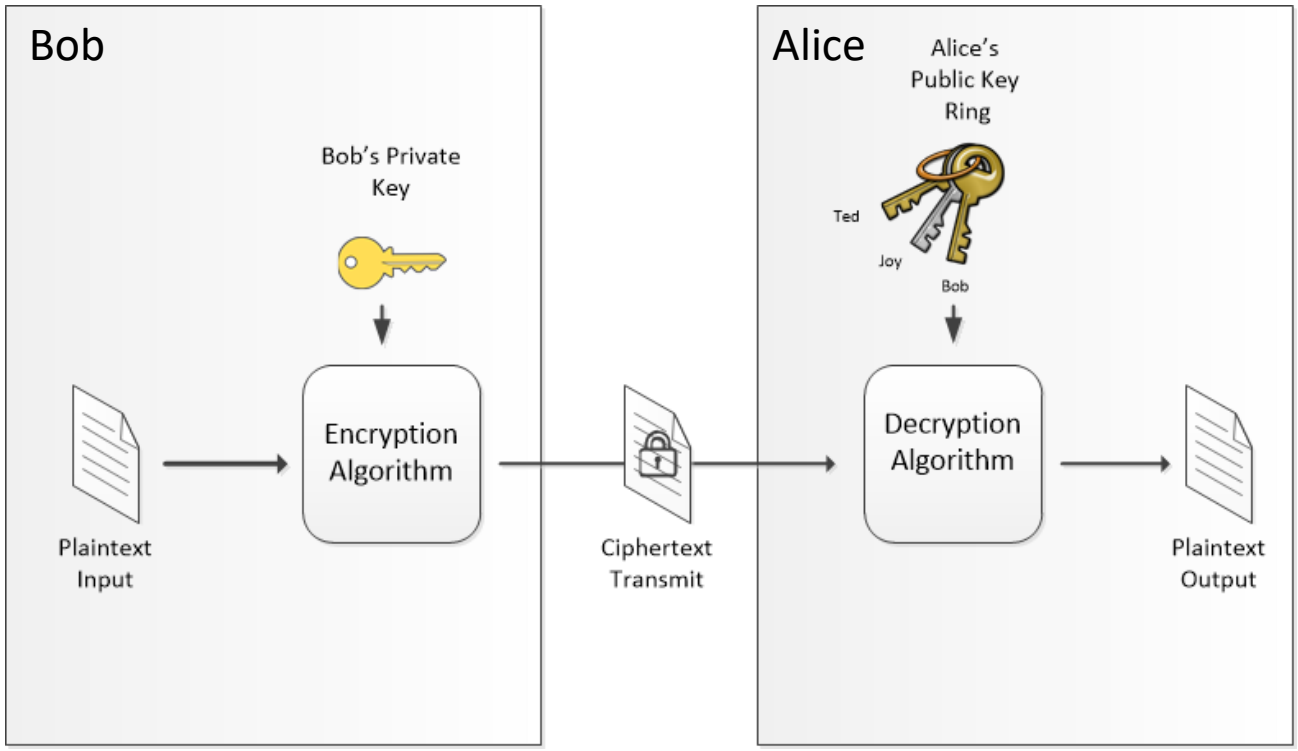
Asymmetric key cryptography (cont.)

- It enables you to communicate over any open channel with a high degree of confidence and permits you to trust in these ways:
  - Authentication: Messages you receive are from their advertised source
  - Privacy: Messages you send can be read only by their intended receiver(s)
  - Message integrity: All messages sent and received arrive intact

Asymmetric Key Encryption – Simplified Using Receiver (Alice) Public Key



Asymmetric Key Encryption – Simplified Using Sender (Bob) Private Key



Putting the Pieces to Work

Background Technologies

- A hash or a hash function is a transformation of data into distilled forms that are unique to the data
- With a computer program, a document is run through a one-way hashing formula to produce a small numeric value that's unique but easily repeatable for that exact stream of data
- This process is also called digesting data or creating a message digest

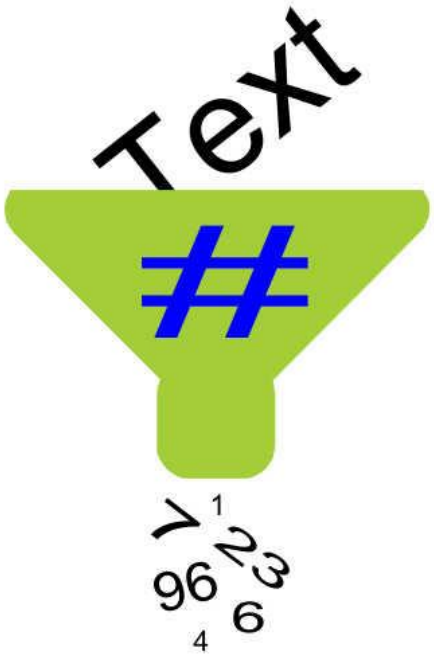
Using the text "ACS-2821-001 Information Security in Business"

- *MD5 Hash*: 4924f0754f5f3f1c61ea8ec07695607a
- *SHA-1 Hash*: 83831a21b993bfd81920acb5aa1fafb6bc2fff29
- *SHA-256 Hash*: 0000e5598a095d03e0fb8e7567f40e5ee5cb25aec9c97deb6cae5bacc8b1c0dd

Cryptographic Hash Function

A cryptographic hash function has for properties:

1. Computationally Efficient
2. Deterministic
3. Pre-Image Resistant
4. Collision Resistant



Digesting Data

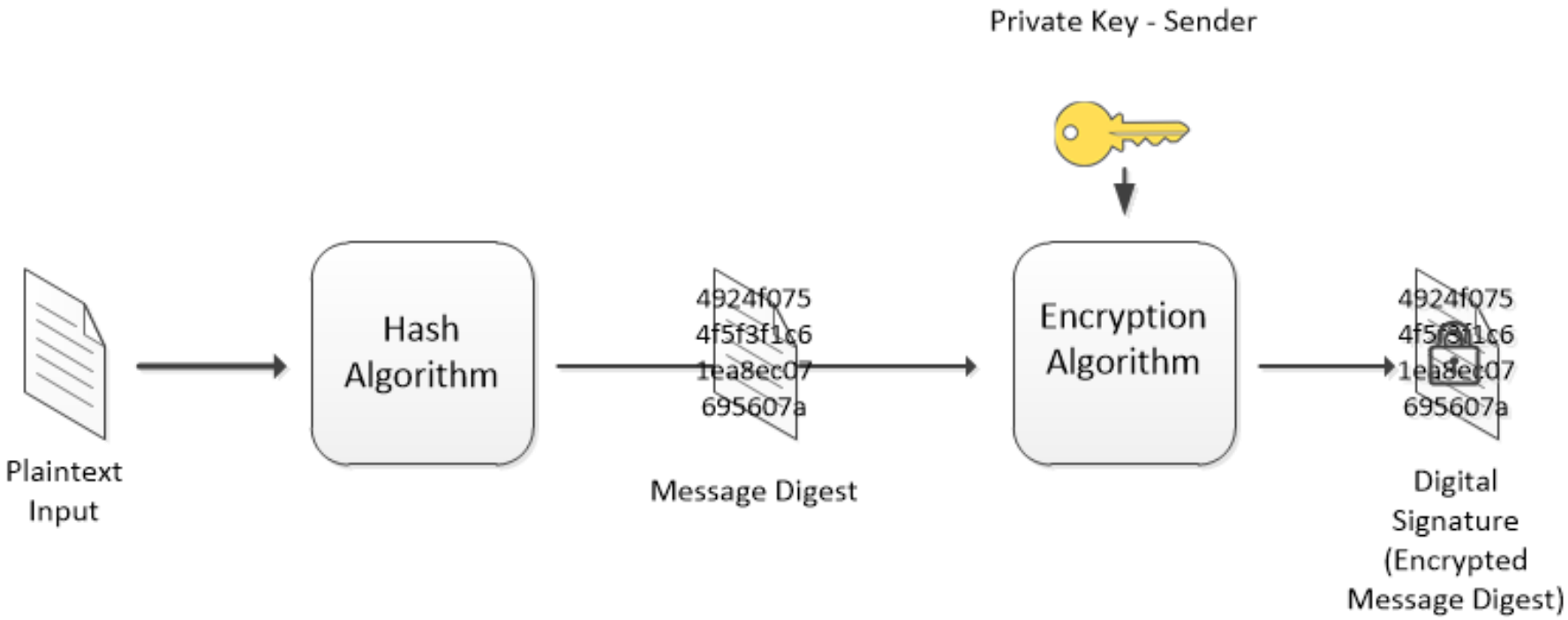
Common hashing algorithms

- MD5
- SHA1 or SHA256

Digital signatures

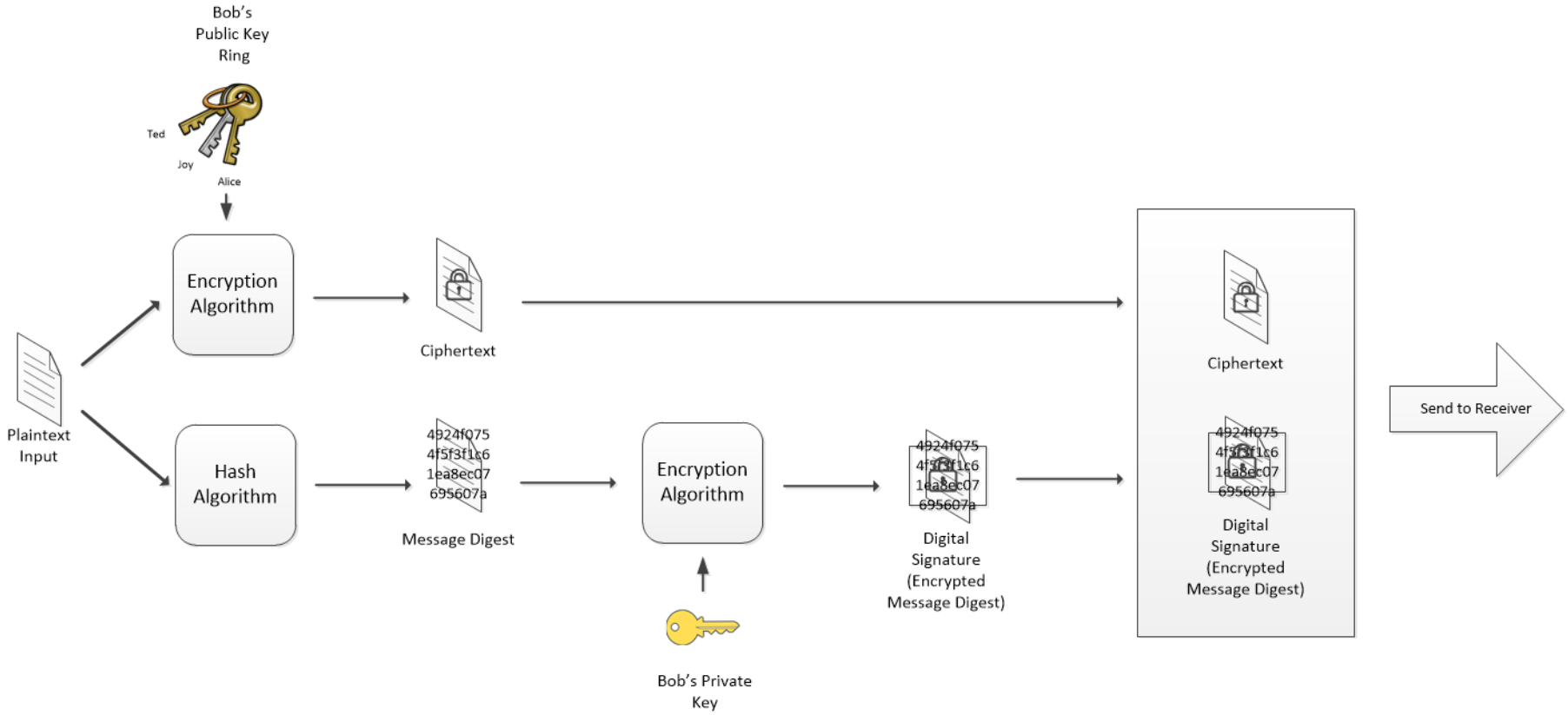
- Used to verify the identity of the sender (nonrepudiation)
- Uses a message digest

Digital Signature - Simplified



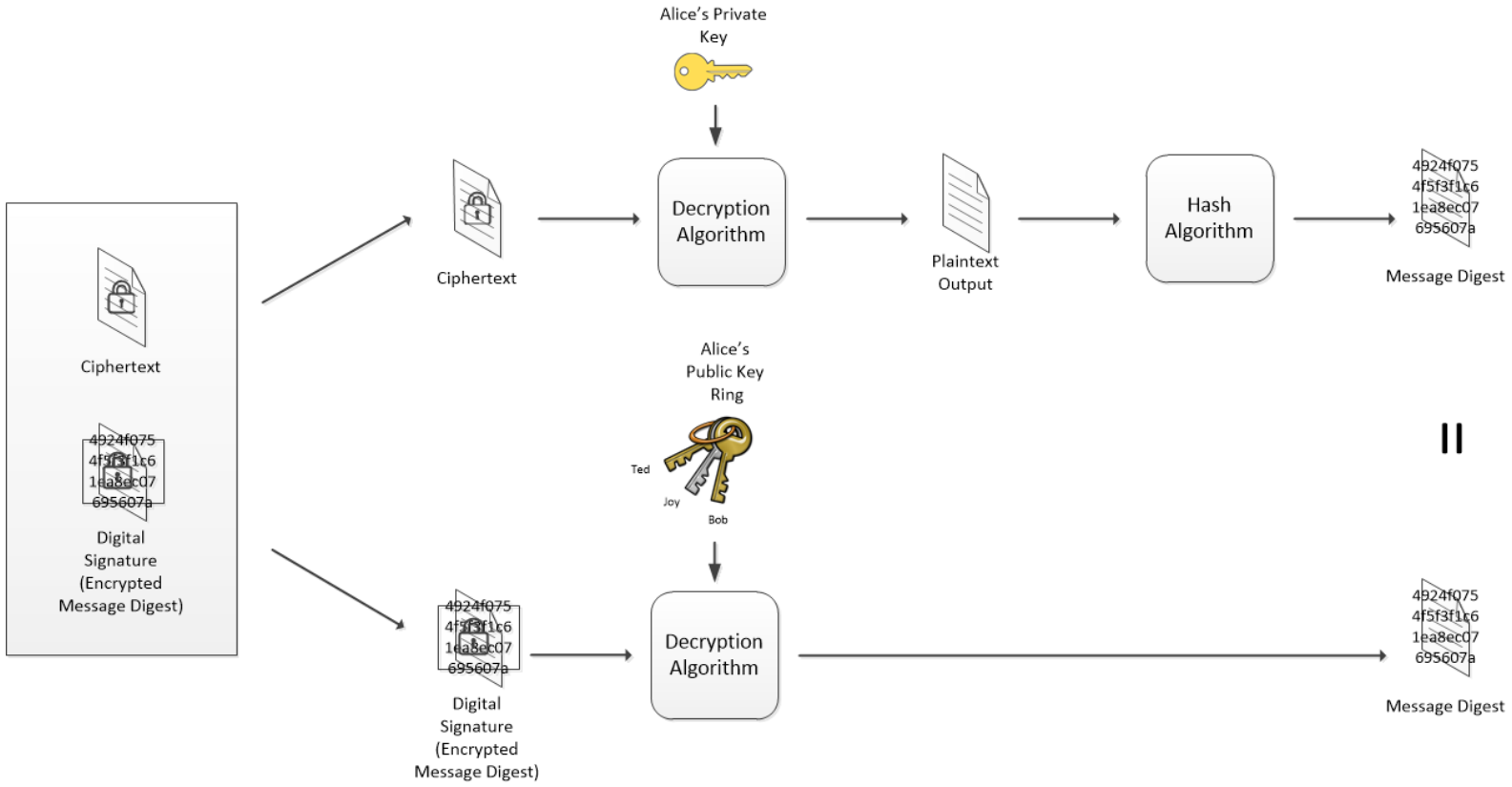
Email with Digital Signature - Send

Confidential, Integrity and Nonrepudiation

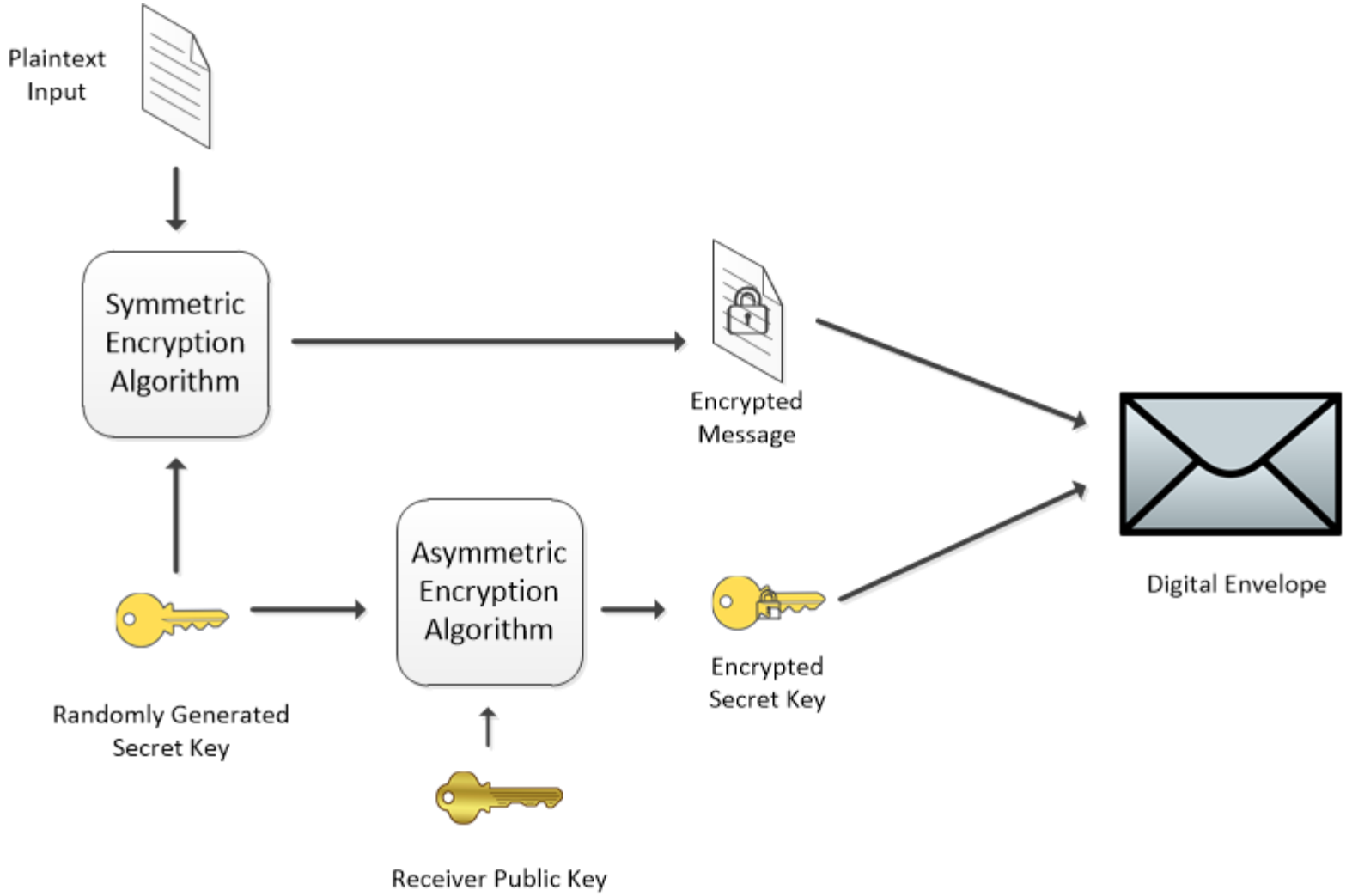


Email with Digital Signature - Receive

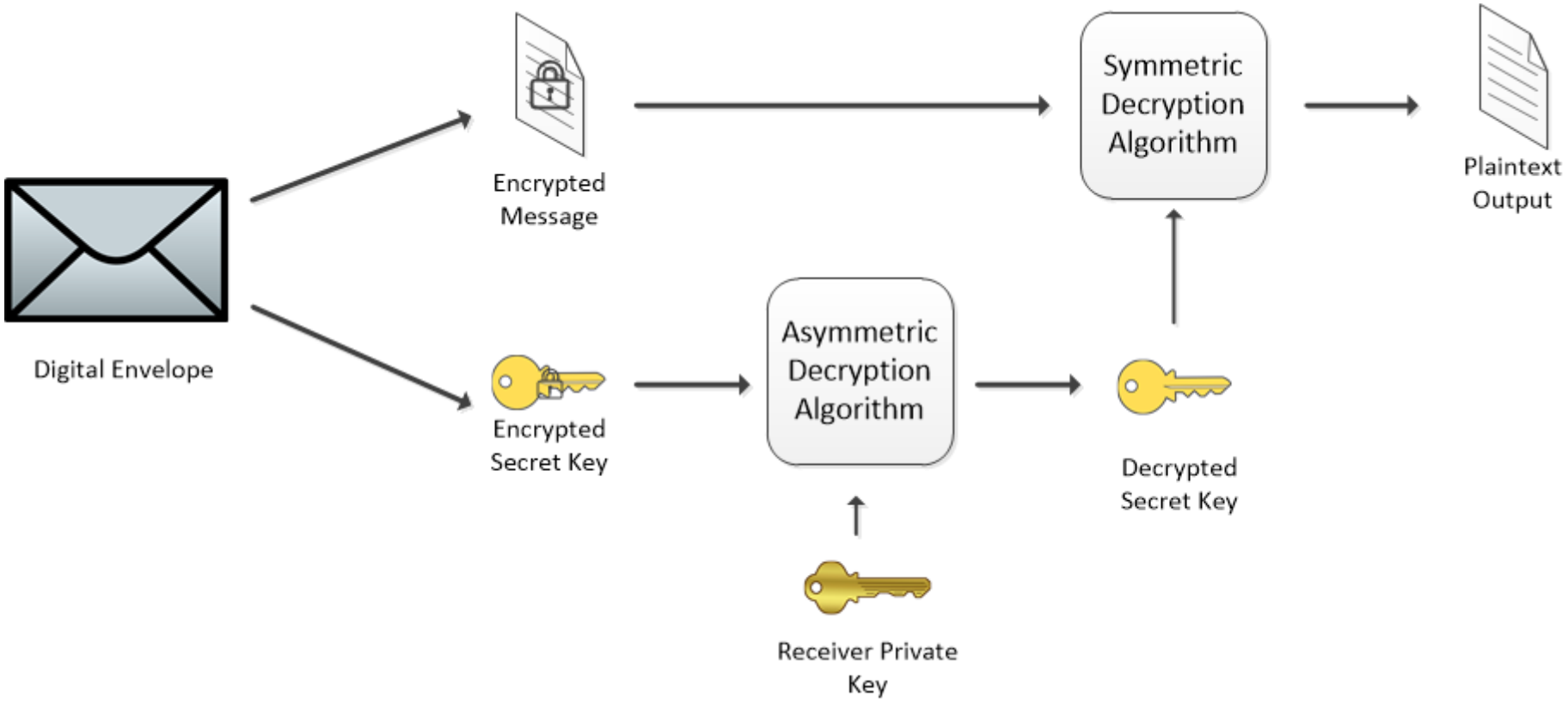
Confidential, Integrity and Nonrepudiation



Digital Envelope - Encrypt



Digital Envelope - Decrypt



Digesting Data

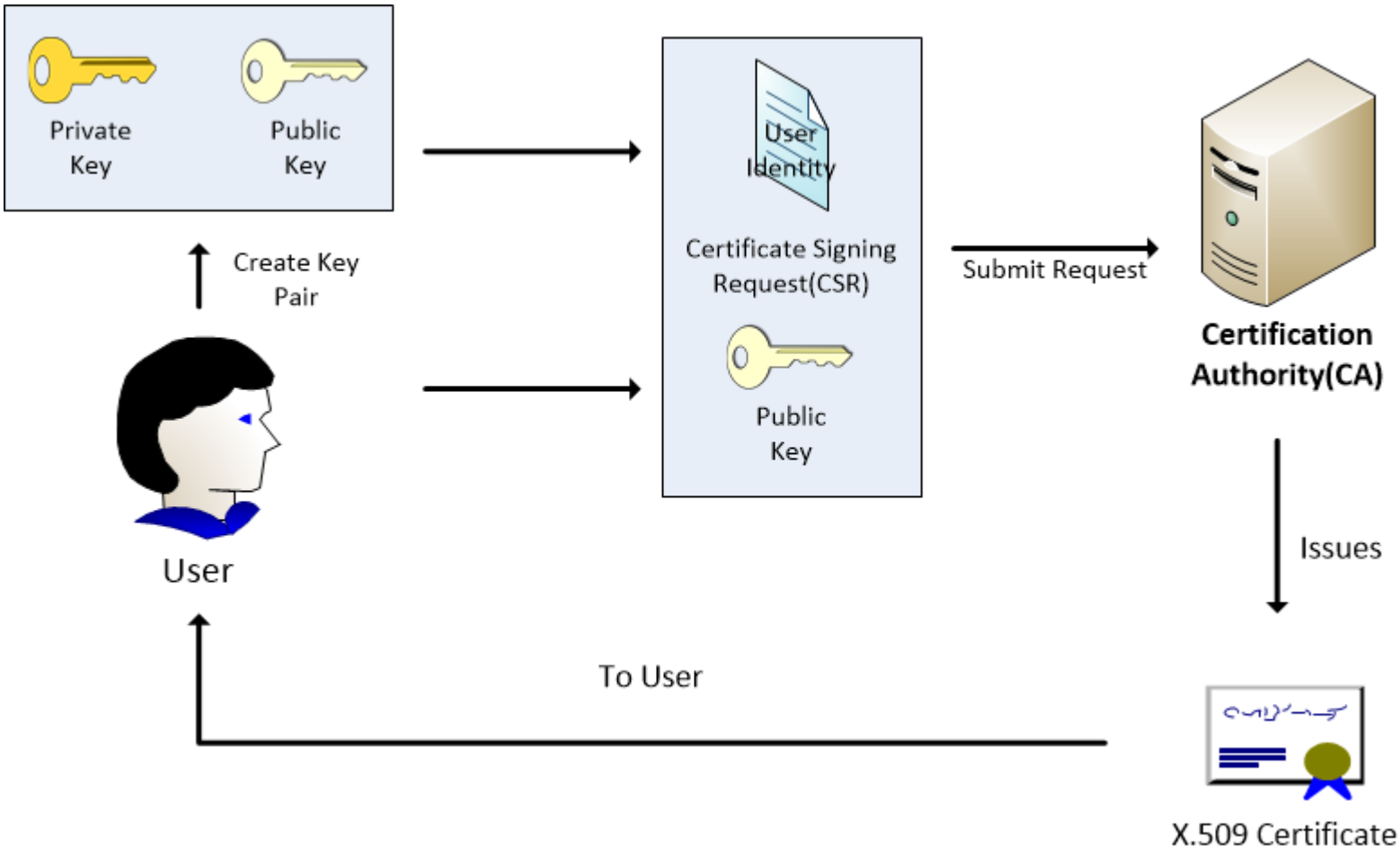
THE UNIVERSITY OF WINNIPEG

Private/Public Key Uses				
	Create Digital Signature	**Verify Digital Signature**	**Create Digital Envelope**	**Verify Digital Envelope**
Sender's Private Key	X			
Sender's Public Key		X		
Receiver's Private Key			X	
Receiver's Public Key				X

Digital Certificates

- Similar to a driver's license: Used to verify identity
- The digital certificate standard, X.509, governs how certificates are constructed and used between communicating parties
- X.509 is an International Telecommunications Union (ITU) recommended standard and has become a de facto industry standard for user authentication on open systems, such as the Internet
- X.509 digital certificates are similar to notary seals in that they bind a person's identity to cryptographic keys
- X.509 digital certificates are issued by a trusted party, called a certificate authority (CA)
- These CAs operate on behalf of those who want to operate a PKI using X.509 recommended standards

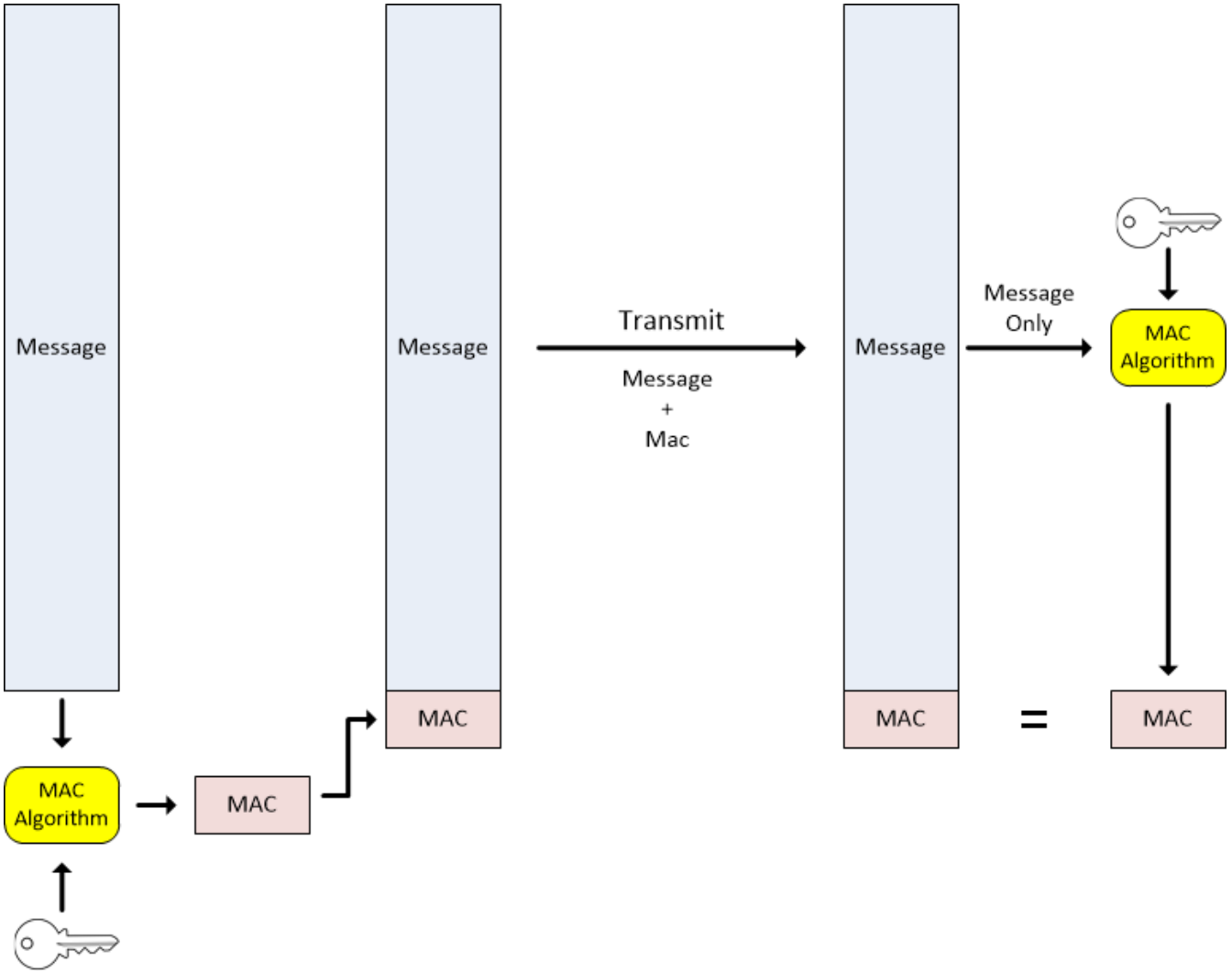
Digital Certificates



Examining Digital Cryptography

- Hashing Functions
  - The most common hashing functions create the message digest for digitally signed messages
    - Hashing is also used to protect user passwords
- Hashing-type functions can also be used with symmetric key cryptography, and the result of the operation is called a message authentication code (MAC)
- Secure Hashing Algorithm (SHA) variants are the most common variants of hashing functions found in commercial software

Examining Digital Cryptography



Message Authentication Code (MAC)

Examining Digital Cryptography

- Block Ciphers
  - DES and Triple-DES are the most common forms of symmetric key block cipher cryptosystems
  - DES uses a 56-bit (7 bytes + checksum byte) key and Triple DES uses a 112-bit (14 bytes + 2 checksum bytes) key
  - The Advanced Encryption Standard (AES) is based on the Rijndael algorithm
  - AES was adopted by the U.S. Department of Commerce as the Federal Information Processing Standard (FIPS) in 2001

Examining Digital Cryptography

- Implementations of PPK (Public/Private Key) Cryptography
  - Secure Sockets Layer (SSL)
    - The most popular form of PPK; the de facto standard for transporting private information across the Internet
    - The goals of SSL are to ensure the privacy of the connection, authenticate a peer's identity, and establish a reliable transport mechanism for the message using integrity checks and hashing functions
    - Two signs that SSL is active during an Internet session:
      - The URL begins with "https//. . ." rather than "http://. . ."
      - A padlock appears on the status bar of the browser

Examining Digital Cryptography

- Implementations of PPK Cryptography (cont.)
  - Transport Layer Security (TLS) Protocol
    - The goals of TLS protocols are to provide
      - Cryptographic security: TLS should be used to establish a secure connection between two parties
      - Interoperability: Programmers should develop applications using TLS that will successfully exchange cryptographic parameters without knowledge of one another's code
      - Extensibility: Provide a framework into which new public key and bulk encryption methods can be incorporated as necessary
      - Relative efficiency: Cryptographic operations tend to be highly CPU intensive, particularly public key operations

Examining Digital Cryptography

- Implementations of PPK Cryptography (cont.)
  - Pretty Good Privacy (PGP)
    - Distributed key management approach that does not rely on certificate authorities
    - Users can sign one another's public keys, adding some degree of confidence to a key's validity
    - Someone who signs another's public key acts as an introducer for that person to someone else so that if someone trusts the introducer, they should also trust the person who's being introduced
    - PGP is often used to encrypt documents that can be shared via e-mail over the open Internet
    - Similar to a digital envelope

Examining Digital Cryptography

- Implementations of PPK Cryptography (cont.)
  - Secure/Multipurpose Internet Mail Extensions (S/MIME)
    - Another standard for electronic-mail encryption and digital signatures
    - S/MIME along with a version of PGP called Open PGP are used in Netscape Communications Corporation Web browsers
    - S/MIME and Open PGP use proprietary encryption techniques and handle digital signatures differently

Examining Digital Cryptography

- Implementations of PPK Cryptography (cont.)
  - Secure Electronic Transactions (SET)
    - Addresses most consumer demands for privacy when using a credit card to shop online
    - Uses a robust set of strictly controlled digital certificates to identify cardholders and merchants, and acquire secure payment gateways for messages passing through open channels like the Internet
    - Uses multiple forms of symmetric key cryptography (such as DES) to provide confidentiality of payment card and transaction data

Summary

- Cryptography is needed by computer applications to implement the privacy and security that users demand
- The strength of a cryptosystem rests in the size and means used to protect cryptographic keys
- The same key can be used to both encrypt and decrypt information and is called a symmetric key, or different keys can be used for encryption and decryption and are called asymmetric keys
- Cryptography relies on two basic methods: transposition and substitution
- Digital signatures are used in asymmetric key cryptography to support authentication, integrity, and nonrepudiation services

ACS-2821-001 – Questions?