The University of Guyana
Faculty of Natural Sciences

LECTURE 2

Computer and Information Security Fundamentals

(CSE 2203)

SEMESTER II (2018-2019)

Sandra Khan BSc MSc CISSP PG Dip Education (Higher Ed)

sandra.khan@uog.edu.gy

Before we begin..

- Please switch cell phones to silent

- Admin Issues

- Will be using Moodle to manage course
- Office Hours: (E29) Wednesdays 13:00 – 15:00 hrs

- ***Email:sandra.khan@uog.edu.gy***

Course Outline

Week 1 – Security Basics
Week 2 – Introduction to Cryptography
Week 3 - Authentication, Encryption (DES/RSA), Hashing
Week 4 - Integrity – Digital Certificates, Message Digests
Week 5 – Network and Internet Security
Week 6 - Internet Commerce, SSL, IPSec, Firewalls
Week 7 – VPN / IDS
Week 8 & 9 – Wireless Security
Week 10 – System Security
Week 11 – Access Control
Week 12 – Application Security
Week 13 – Cyber Crime

Learning Objectives

By the end of this lesson students will be able to:

- Discuss the role of Cryptography in securing information
- Explain basic Cryptosystems
- Describe Classical Ciphers
- Distinguish between two types of Cryptography: Symmetric and Asymmetric

Recap

In the last lecture, we discussed:

- the nature of the Computer and Information Security challenge
- the major security goals (CIA Triad)
- Some terminology – Vulnerabilities, Threats, Control Paradigm
- The M-O-M Framework

The University of Guyana
Faculty of Natural Sciences

Recap Quiz

What is the term that best describes the following: a sender is not able to deny sending a message, e.g. an email or text message

a) message integrity
b) message confidentiality
c) message availability
d) message nonrepudiation

Komisarczuk, P., Martin, K. & Alis, J. (2019), Information Security: Context and Introduction [Coursera course]

Recap Quiz

A message has integrity if:

a) it is authenticated
b) it contains the truth
c) it is verifiably unaltered
d) it contains the senders handwritten signature

Komisarczuk, P., Martin, K. & Alis, J. (2019), Information Security: Context and Introduction [Coursera course]

Recap Quiz

A third party (e.g. a spy) is not able to read a message when:

a) The message is using a cryptographic protocol to implement confidentiality
b) The message has high availability
c) The message is sent with integrity
d) The message is sent using a nonrepudiation technique

Komisarczuk, P., Martin, K. & Alis, J. (2019), Information Security: Context and Introduction [Coursera course]

The University of Guyana
Faculty of Natural Sciences

Information Security Requirements

Let's imagine an old "computer free" office, where everything is done by telephone and paperwork.

What are the basic security processes in the physical world that help us to make security decisions about information that we receive?

(Martin, 2009)

The University of Guyana
Faculty of Natural Sciences

Information Security Requirements in the Digital Age

Now imagine a modern fully networked office environment. Let's suppose that nobody has implemented any information security controls.

- **How do you identify the sender of a file?**
- **Can anyone else read an email that you send to a colleague?**
- **How do you sign a contract?**
- **Is this a more secure environment than the old office?**

(Martin, 2009)

The University of Guyana
Faculty of Natural Sciences

Basic Security Requirement in the Digital Age

"The basic security requirement is the need for the translation of the basic security mechanisms used in the physical world into mechanisms suitable for application in an electronic environment. "

(Martin, 2009)

The University of Guyana
Faculty of Natural Sciences

Business Security Requirement in the Digital Age

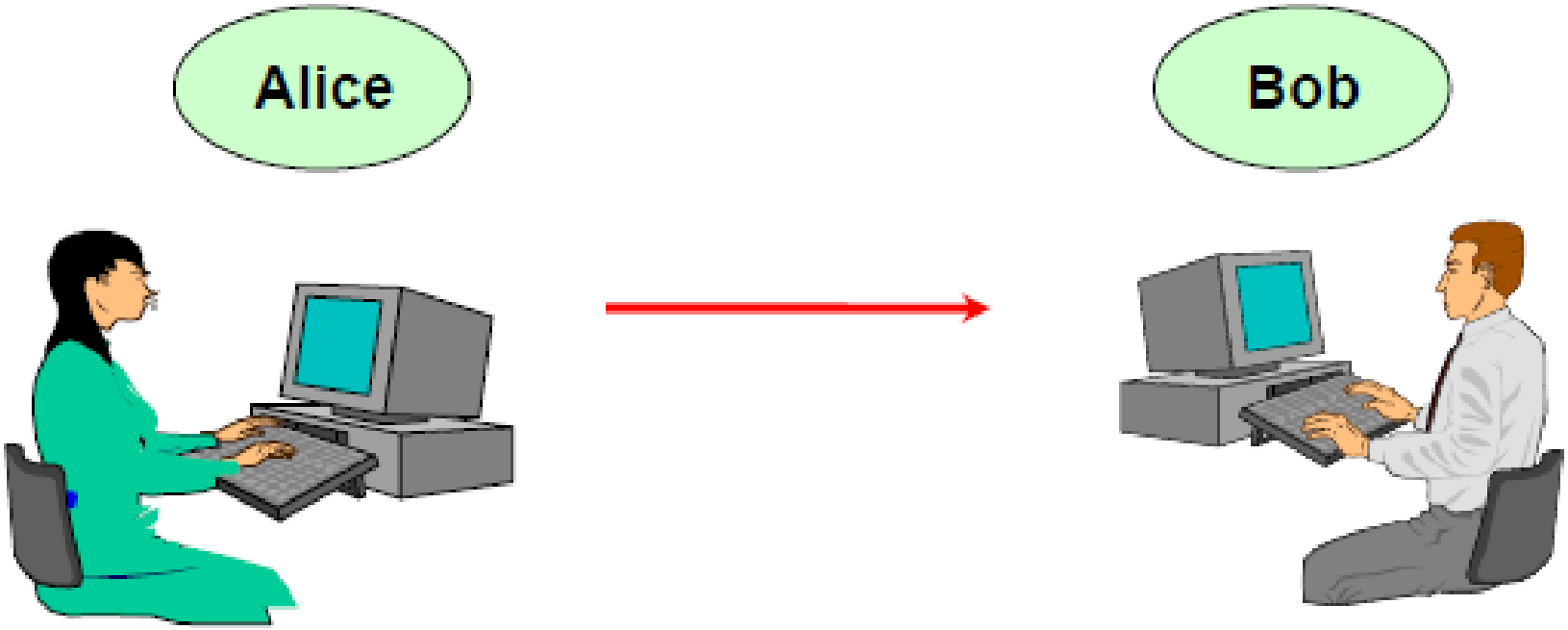
“For businesses (and organisations in general), the Internet represents both a great opportunity and a significant risk.

The main business security requirement is that increased automation and adoption of new technologies should not lead to a decrease in the overall security of conducting business.”

A central aim of today's lesson is to discuss what role cryptography plays in this translation process.

(Martin, 2009)

Meet Alice and Bob

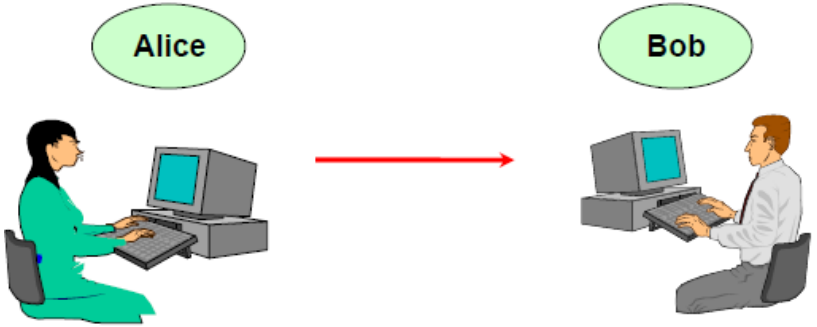


(Martin, 2009)

The University of Guyana
Faculty of Natural Sciences

Meet Alice and Bob

If Alice and Bob are to have any assurances about the security of the communication that they have just exchanged then they must ask themselves some serious questions.



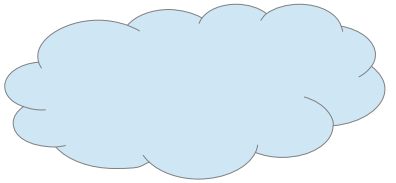
(Martin, 2009)

.What questions should Alice be thinking about before she sends her information to Bob?

.After he has received the information, what questions should Bob be contemplating with regard to his newly received information?

The University of Guyana
Faculty of Natural Sciences

Role of Cryptography



What is the role of Cryptography?

What is Cryptography?

The University of Guyana
Faculty of Natural Sciences

Cryptography

What is the role of Cryptography?

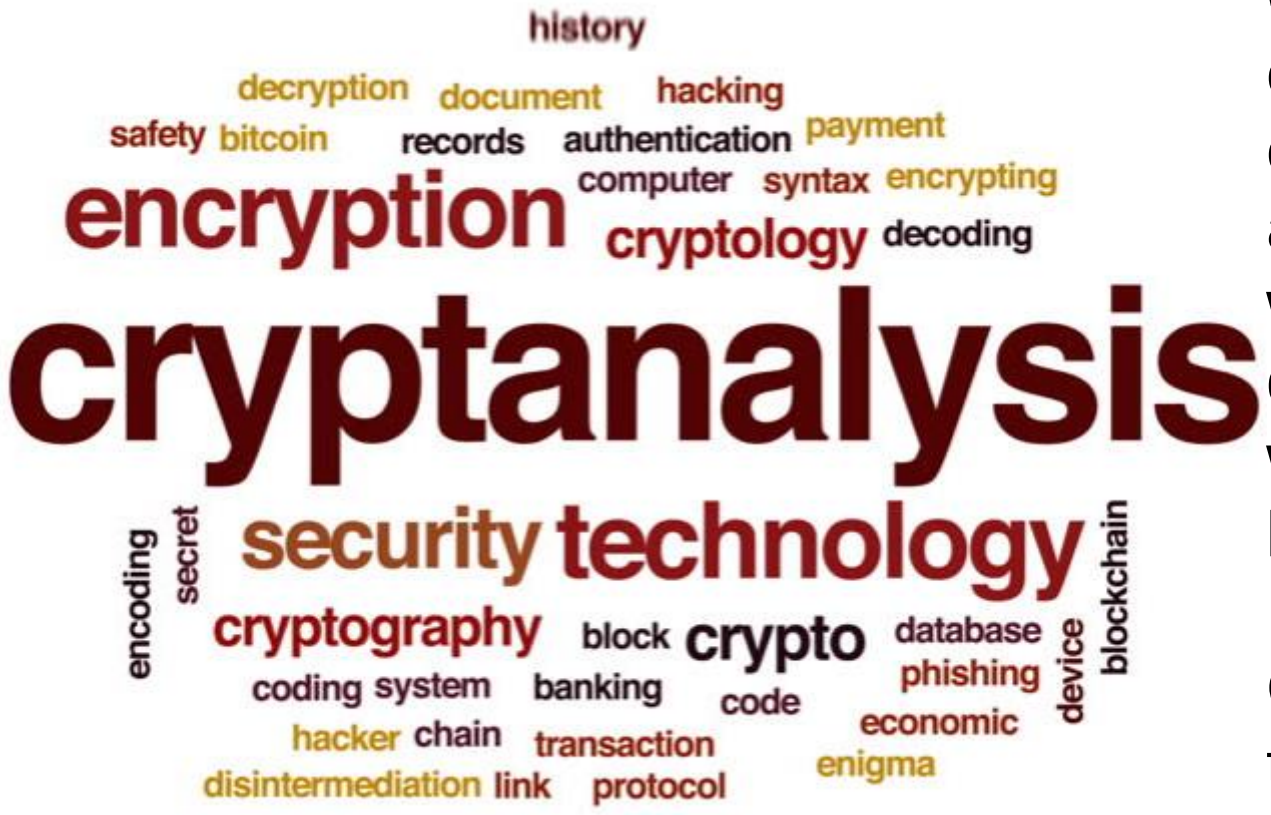
- **Cryptography is not a new concept – used for thousands of years preceding the Information Age.**

What is Cryptography?

- **Cryptography is the art and science of designing techniques for secure communication in the presence of malicious third parties called adversaries.**

The University of Guyana
Faculty of Natural Sciences

Cryptanalysis / Cryptology



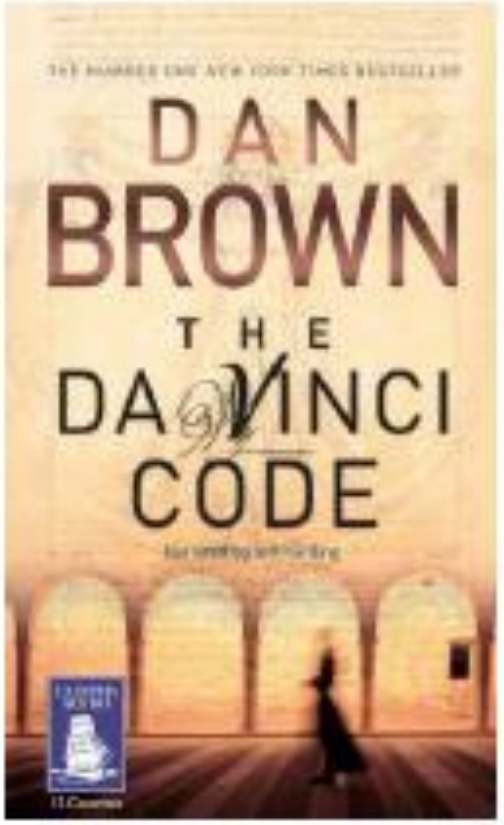
Cryptanalysis is a process of finding weaknesses in cryptographic algorithms and using these weaknesses to decipher the ciphertext without knowing the secret key.

Cryptology is the science that underpins cryptography and cryptanalysis.

(OWASP, 2009)

The University of Guyana
Faculty of Natural Sciences

Ciphers in Public Imagination



(Martin, 2009)

The University of Guyana
Faculty of Natural Sciences

Classical Ciphers

"There's an easier way," Sophie said, taking the pen from Teabing.

"It works for all reflectional substitution ciphers, including the Atbash. A little trick I learned at the Royal Holloway."

Sophie wrote the first half of the alphabet from left to right and then, beneath it, wrote the second half, right to left.

"Cryptanalysts call it the fold-over. Half as complicated. Twice as clean."

Teabing eyed her handiwork and chuckled.: "Right you are. Glad to see those boys at the Holloway are doing their job."

(Martin, 2009)

The University of Guyana
Faculty of Natural Sciences

Ciphers in Public Imagination

http://www.themakeupgallery.info/hair/shaved/rushhour3.htm

The University of Guyana
Faculty of Natural Sciences

Ciphers in Public Imagination

http://www.themakeupgallery.info/hair/shaved/rushhour3.htm

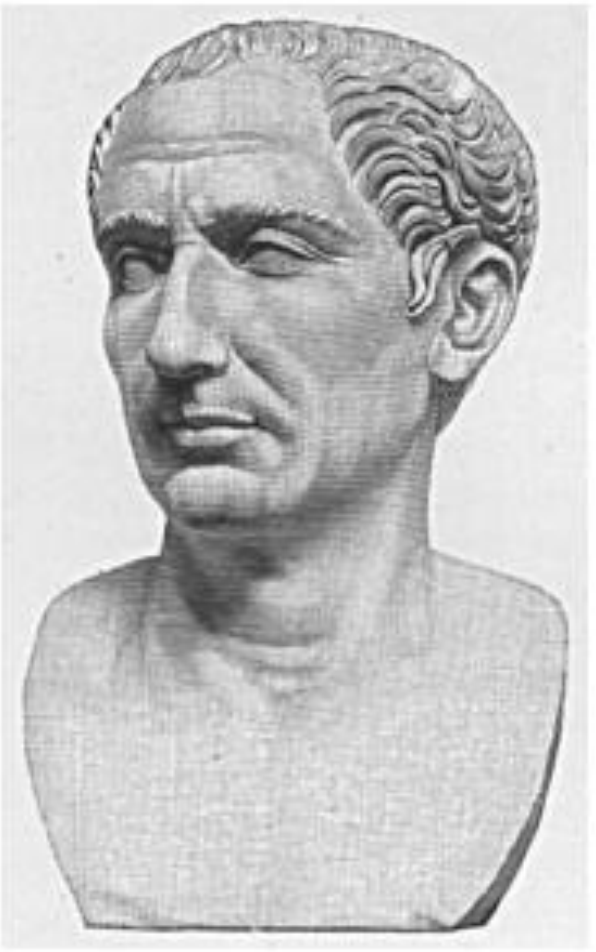
The University of Guyana
Faculty of Natural Sciences

Ciphers in Public Imagination

http://www.themakeupgallery.info/hair/shaved/rushhour3.htm

The University of Guyana
Faculty of Natural Sciences

Historical Cryptography - Caesar Cipher



(Martin, 2009)

Caesar Cipher

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ

ABCDEFGHIJKLMNOPQRSTUVWXYZ

sliding ruler

NOTE: There are 26 keys, i.e. 26 'settings'

(Martin, 2009)

The University of Guyana
Faculty of Natural Sciences

Decipher the following:

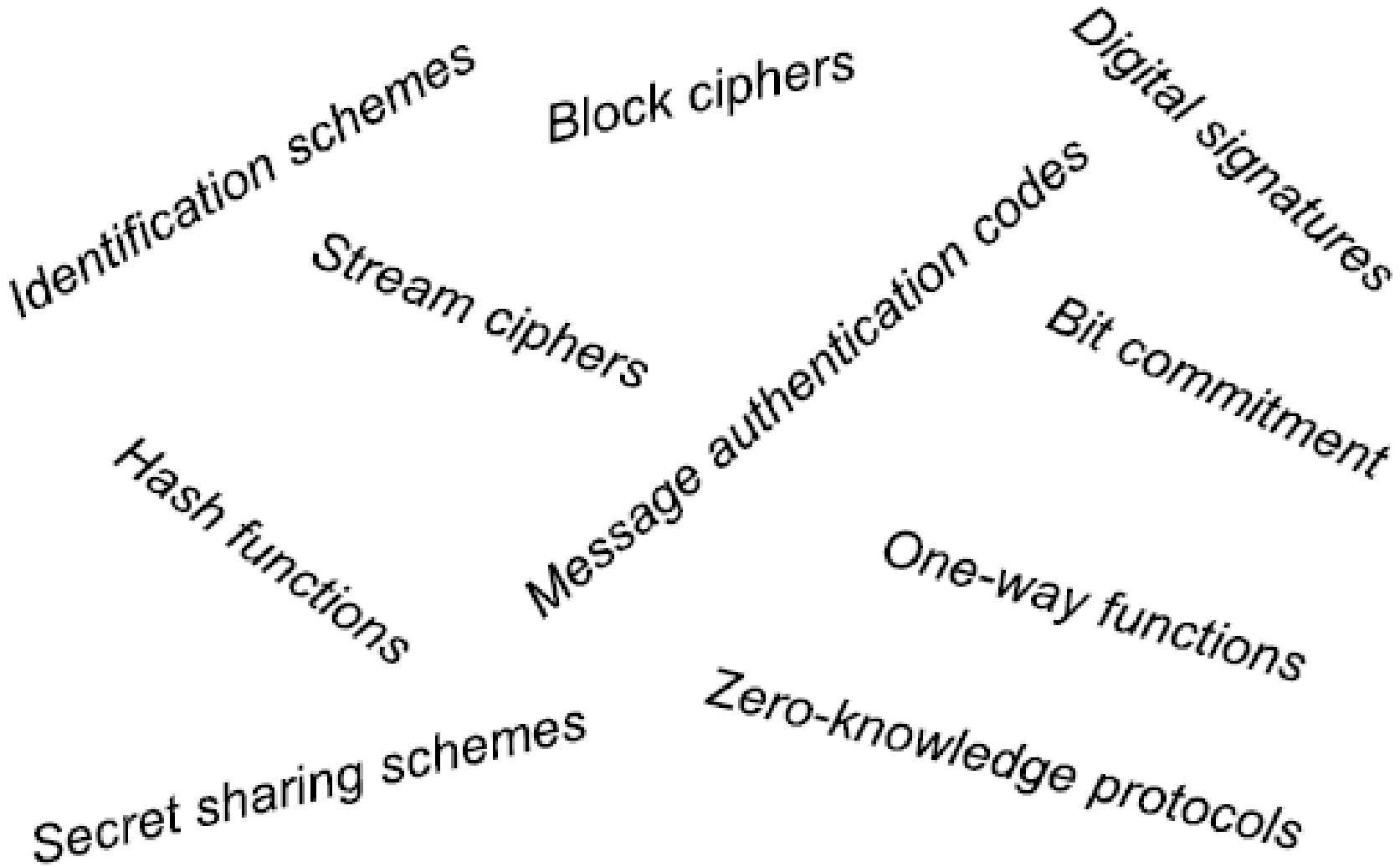
Ciphertext HSPPW

HSPPW	QBYYF	ZKHHO
ITQQX	RCZZG	ALIIP
JURRY	SDAAH	BMJJQ
KVSSZ	TEBBI	CNKKR
LWTTA	UFCCJ	DOLLS
MXUUB	VGDDK	EPMMT
NYVVC	WHEEL	FQNNU
OZWWD	XIFFM	GROOV
PAXXE	YJGGN	

(Martin, 2009)

The University of Guyana
Faculty of Natural Sciences

Digital Cryptographic Primitives



(Martin, 2009)

What is a Cryptosystem

A **cryptosystem** is a general term referring to a set of cryptographic primitives used to provide information security services.

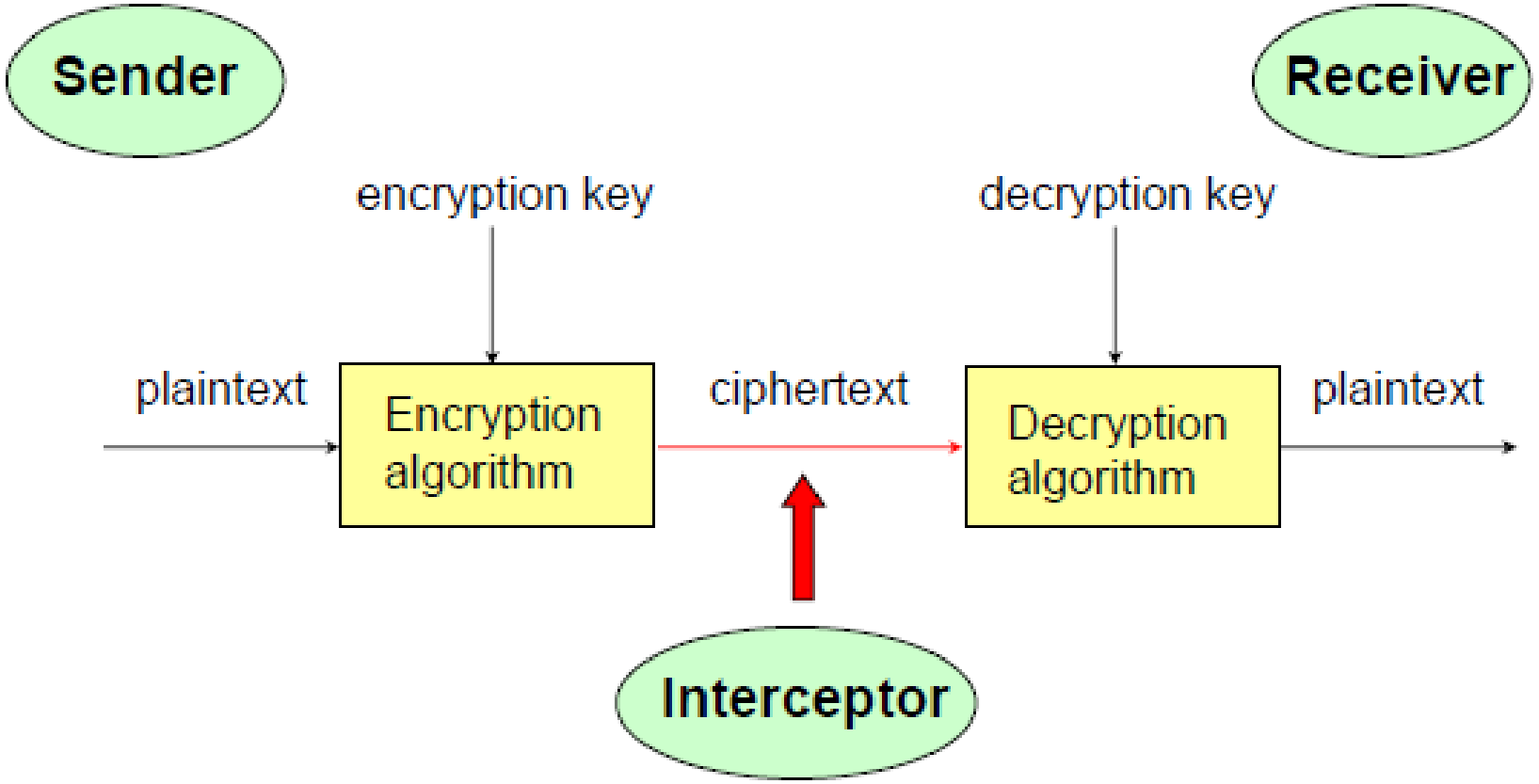
Most often the term is used in conjunction with primitives providing confidentiality (i.e. encryption).

Source: Handbook of Applied Cryptography

(Martin, 2009)

The University of Guyana
Faculty of Natural Sciences

A Cryptosystem



(Martin, 2009)

A Symmetric Cryptosystem

In **symmetric** cryptosystems the decryption key is easily obtained from the encryption key. Often, in a symmetric cryptosystem the encryption key and the decryption key are exactly the same.

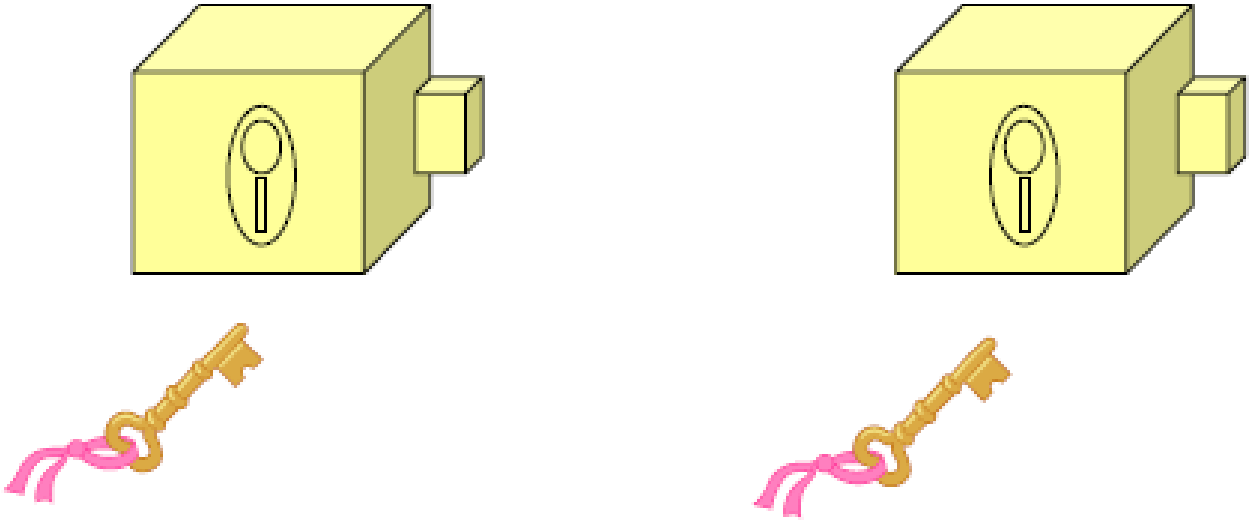
All practical cipher systems prior to the 1980's were symmetric cryptosystems. Indeed symmetric cryptosystems are still heavily used today and there is no sign that their popularity is fading.

The study of symmetric cryptosystems is often referred to as **symmetric cryptography**.

(Martin, 2009)

A Symmetric Cryptosystem

Locking = Unlocking



(Martin, 2009)

The University of Guyana
Faculty of Natural Sciences

Public Key Cryptosystems

In **public key** cryptosystems it is computationally infeasible (in other words, practically impossible) to determine the decryption key from the encryption key.

In this case the encryption key and the decryption key must be different. For this reason, public key cipher systems are sometimes referred to as **asymmetric** cryptosystems.

The study of public key cryptosystems is often referred to as **public key cryptography**.

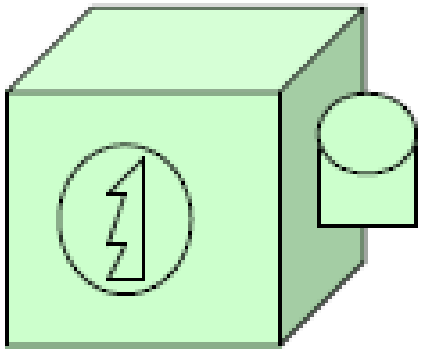
(Martin, 2009)

The University of Guyana
Faculty of Natural Sciences

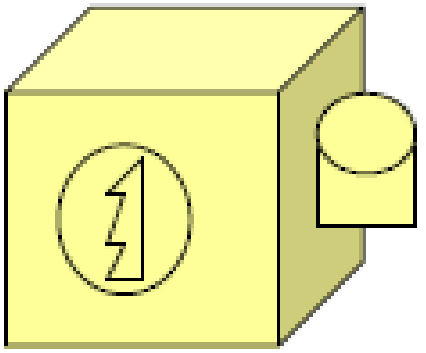
Public Key Cryptosystems

.

Anyone can lock



Only a key holder can unlock



(Martin, 2009)

Questions

1. Can cryptography prevent a communication from being intercepted?

2. Which of the following need to be kept secret?
   a) Encryption algorithm
   b) Decryption algorithm
   c) Encryption key
   d) Decryption key

3. Does using a good encryption algorithm guarantee the confidentiality of a message?

(Martin, 2009)

Perspectives on Cryptography

Individual Perspective:

Individuals have a right to use cryptography as they see fit. Cryptography enables perceived rights such as privacy and freedom of expression.

Government Perspective:

On the other hand, governments may wish to control crime and manage issues of national security. They may try to do this by imposing certain barriers and introducing other laws and regulations.

(Martin, 2009)

FURTHER INFORMATION

Course notes and references are available via Moodle.

Required Readings:

Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in computing:* Chapter 2

Readings

Required Reading(s)

Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in computing*. Prentice Hall Professional Technical Reference.

Stallings, W. (2006). *Cryptography and Network Security, 4/E*. Pearson Education India.

Recommended Reading(s)

Stallings, W. (2007). *Network security essentials: applications and standards*. Pearson Education India.

https://www.sans.org/security-resources/glossary-of-terms/

REFERENCES

Martin,K.(2009). Intro to Cryptography [PowerPoint Presentation]. Retrieved from Royal Holloway ISG

Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in computing.* Prentice Hall Professional Technical Reference.

End of Lecture 2