Week 1: Module overview

Hasan Chizari and Madhu Khuruna

University of Gloucestershire

hchizari@glos.ac.uk

UNIVERSITY OF GLOUCESTERSHIRE

Overview

UNIVERSITY OF GLOUCESTERSHIRE

What is cryptography?

- Refers to the development and application of systems to secure information
- Consists of two components, namely:
  - Cryptology: the study of *encrypt* information
  - Cryptanalysis: the study of different cryptographic systems with goal of *breaking* them

Confidentiality, Integrity, Availability

- One of the fundamental tenets of cybersecurity
- Confidentiality: Ensuring only authorised personal has access to resource
- Integrity: Assurance that data has not been tampered with
- Availability: Proper functioning of systems after attack

CIA Triangle

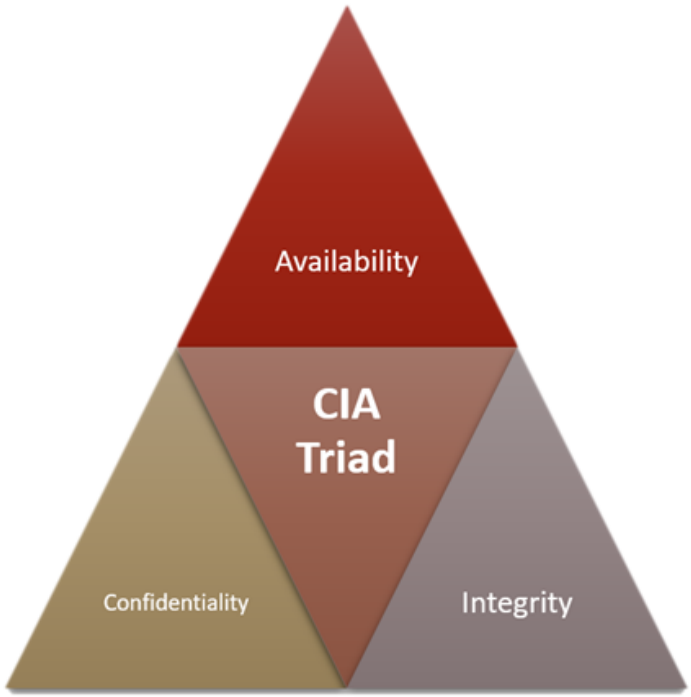

Figure: CIA Triangle, from [1]

UNIVERSITY OF GLOUCESTERSHIRE

Confidentiality

- Preventing authorised access to data
- Operate on a "Need-to-know" basis
- Difficult to provide assurance, but easy to measure
- Addresses the following:
  - Identification
  - Authentication
  - Access control

Integrity

- Assurance against authorised modification of data
- Not as clearly-specified as confidentiality
- Context-dependent
- Features the use of:
  - Non-repudiation: Means of verifying proof of integrity and origin of data

Availability

- Assurance that systems should still be available even after protective mechanisms are in place
- Context-dependent
- Addresses the following:
  - Timely request response
  - Fair allocation of resources (no starvation!)
  - Fault tolerant (no total breakdown)
  - Easy to use in the intended way

Applications of crptography

- Securing email communications.
- Securing email messages.
- Providing non-repudiation (digital signatures).
- Securing network protocols.
- Securing Internet communications (SSL/TLS)
- Etc

Components

- Plaintext
  - Original *unencrypted* message
- Ciphertext
  - Encoded message obtained from *encrypting* it
- Cipher
  - Algorithm used to transform the plaintext into ciphertext

Components (cont.)

- Key
  - Information used together with an algorithm to create the ciphertext from the plaintext or *vice versa*
- Key space
  - Range of values that can be used to construct an individual key
- Work factor
  - The amount of effort required to perform to decode an encrypted message without knowledge of key and/or algorithm
  - Measured in hours

How they work together

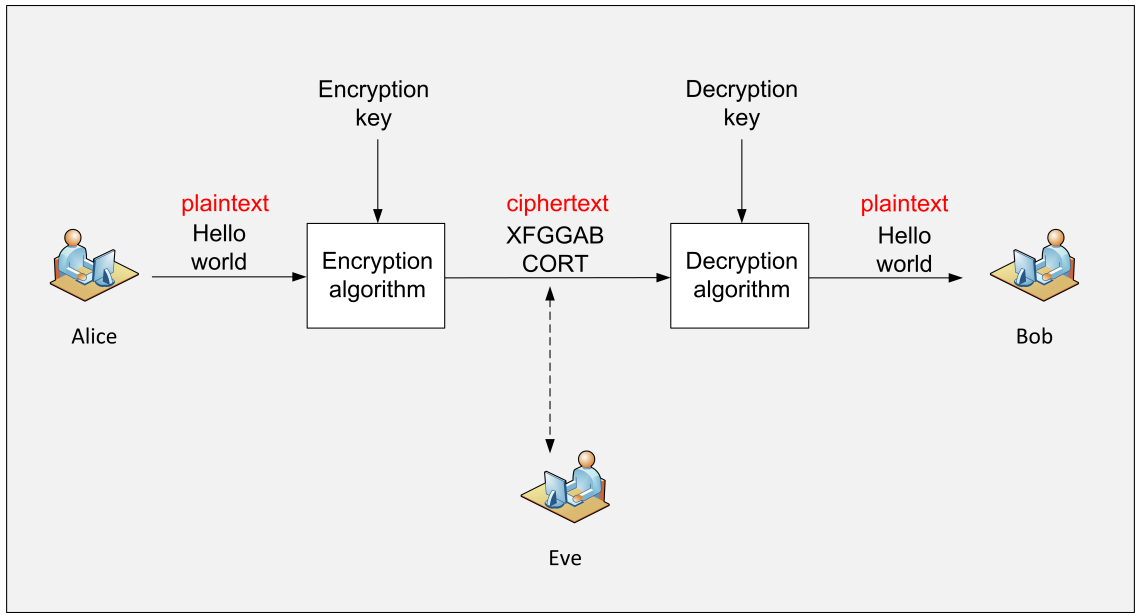

Figure: Cryptosystem overview, adapted from [3]

Algorithm Classifications

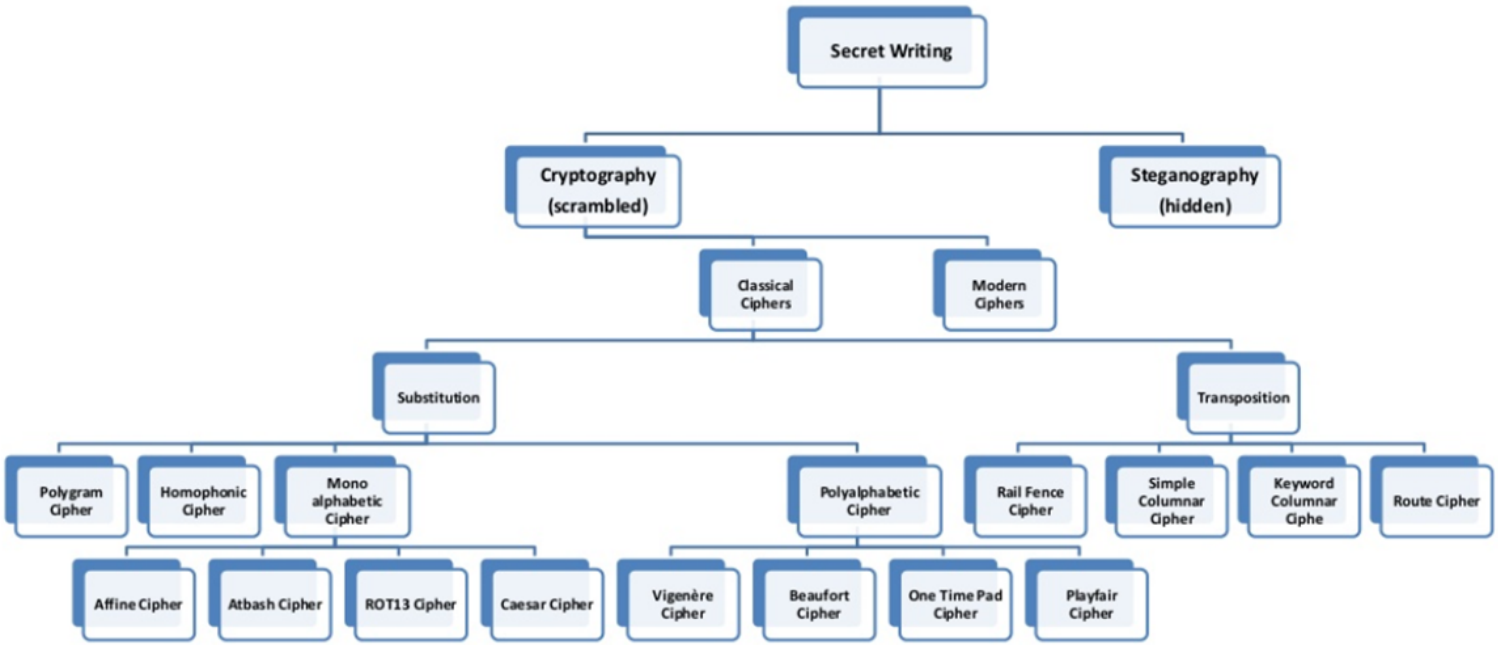

Figure: Classification of different algorithms

UNIVERSITY OF GLOUCESTERSHIRE

Classical

- Substitution cypher
  - Replace bits, characters, or blocks of characters with different bits, characters or blocks.
  - E.g., Caesar, Vigenère are substitution ciphers.
- Transposition cypher
  - The letters or units of the plaintext are shifted, rearranged or transposed (anagram) according to the algorithm.
  - E.g., Rail fence and route ciphers

Modern

- Based on the type of keys used
  - Public and private keys.
  - Symmetric keys.
- Based on the type of input data.
  - Stream ciphers
  - Block ciphers

Video: How hackers and governments can hack your smartphone camera

[Video] How hackers and governments can hack your smartphone camera, from *TechInsider*

Attacks on cryptosystems

- Regardless of how strong a cryptosystem is, they will always be subjected to attacks
- Attacks against a given cryptosystem can be grouped together as
  - Active attacks
  - Passive attacks

Active attacks

- Masquerade
  - Attack through false pretences
- Replay
  - Retransmission of previously captured data
- Message modification
  - Illegal alteration of some or all of a legitimate message
- Denial of Service
  - Rendering some or all of the communication infrastructure needed for data transmission

Passive attacks [3]

- Ciphertext only
  - Analysing the ciphertext produced
- Known plaintext
  - Uses *both* plaintext and ciphertext
- Chosen plaintext
  - Uses plaintext on a given cyphersystem to analyse ciphertext obtained
- Chosen ciphertext
  - Uses ciphertext on a given cyphersystem to analyse plaintext obtained

Goals of this module

- Understand the fundamental principles of cryptography
- Understand the application of cryptographic techniques and protocols to protect the transmission and storage of information
- Identify and explain the Public-Key Infrastructure (PKI) and its components
- Identify and understand the requirements to implement cryptographic applications

How this module is structured

- The delivery of this module is divided into two components, namely
  - **Lectures**: which discuss the *theory* aspects of cryptography
  - **Practicals**: which look at the *implementation* aspects of theories discussed

Content outline

- Different cryptography approaches which we'll look at include:
  - Information and number theory
  - Symmetric/Asymmetric encryption
  - Hashing
  - Public Key Infrastructure (*PKI*)

Software tools and packages for this module

- For this module, we will be using *CryptTool 2*
  - Open source
  - Platform-independent
  - Contains implementation of different cyptography algorithms
  - Available from here
- Occasionally we will also be using `Python` as well

Key points to keep in mind

- Submit the weekly post-sessional work **before** the next lecture session
- Lecture and practical slides on *Moodle*
- Feel free to send any questions/issues regarding the module contents into Moodle Forum

Reference books for this module

- Mao, W. (2003). Modern cryptography: theory and practice. Prentice Hall Professional Technical Reference.
- Stallings, W. (2014). Cryptography and Network Security. Principles and Practice. 6^{th} ed. Pearson.
- Stanoyevitch, A. (2013). Introduction to Cryptography with Mathematical Foundations and Computer Implementations. Taylor & Francis Group.

Bringing it all together

- Today we looked at the module overview and its details
- We also looked at the rationale behind cryptography
- We also looked at the overview of the cryptographic algorithm classifications
- Next week: *Introduction to Cryptography I*

Post-sessional work

- Using Section 2.3 of [2] as a starting point, discuss how a cryptography system can be attacked
- Using Example 1.5 of [3], discuss the following:
  - Monoalphabetic ciphers
  - Polyalphabetic ciphers
  - Statistical frequency counts
- Upload your completed work to *Moodle* before next *Monday*

References

[1] Infosec Institute. *CIA Triad*. http://resources.infosecinstitute.com/cia-triad/. Accessed: 20-10-2017. 2017.

[2] Wenbo Mao. *Modern cryptography: theory and practice*. Prentice Hall Professional Technical Reference, 2003.

[3] Alexander Stanoyevitch. *Introduction to Cryptography with mathematical foundations and computer implementations*. CRC Press, 2013.

Q & A