Introduction to Cryptography and Information Security

Part 1
Introduction

Jorge Camargo, PhD

Table of Content

Introduction

- Definition
- Goals of Cryptography
- Terminology
- Common Players
- One–Time Pad (OTP)
- Perfect Secrecy
- Unconditionally Secure Vs Computationally Secure
- Kerckhoffs' Principle

Cryptography

Cryptography is about:

- "communication in the presence of adversaries" (RONALD RIVEST)
- "an intellectual battle between a code-maker and a code-breaker" (SIMON SINGH)
- "the study of math techniques to meet the fundamental objectives of information security" (HANDBOOK OF APPLIED CRYPTOGRAPHY)

The origin of the word cryptology lies in ancient Greek

Κρυπτο – γραφια = to write secret(ly)

(hidden) (to write)

Goals of Cryptography

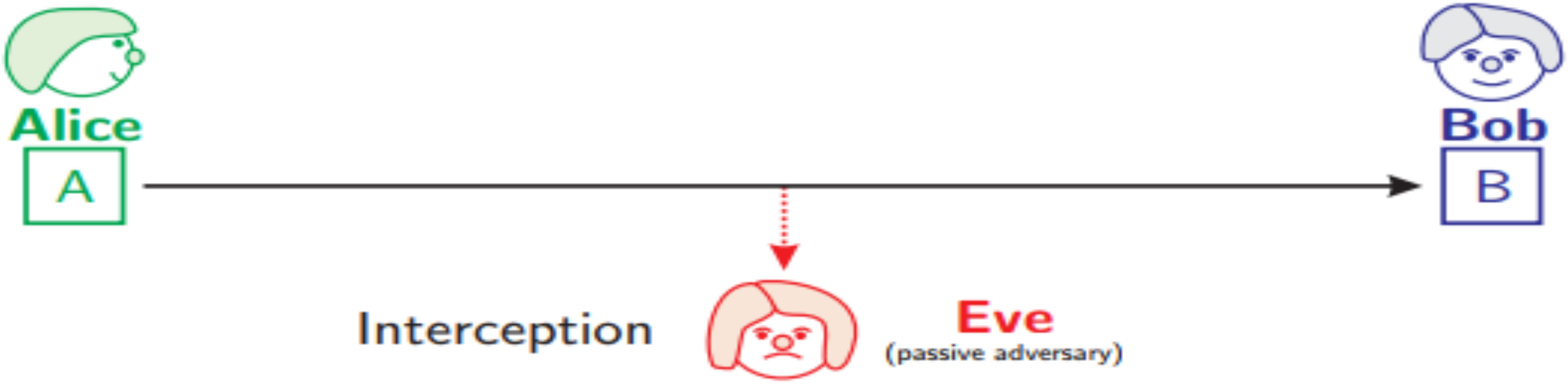
In spite of adversaries, we want to achieve (among other things):

1) Confidentiality - prevent unauthorized access
2) Integrity - no modification of existing info
3) Authentication - or identifying either entities or data origins
4) Availability - information must be available when is needed
5) Non-repudiation - preventing denials of messages sent

A fundamental goal of cryptography is to adequately address these five areas in both theory and practice

The CIA triad (confidentiality, integrity and availability) is one of the core principles of **information security**

Goal 1: Confidentiality
(Is Private?)

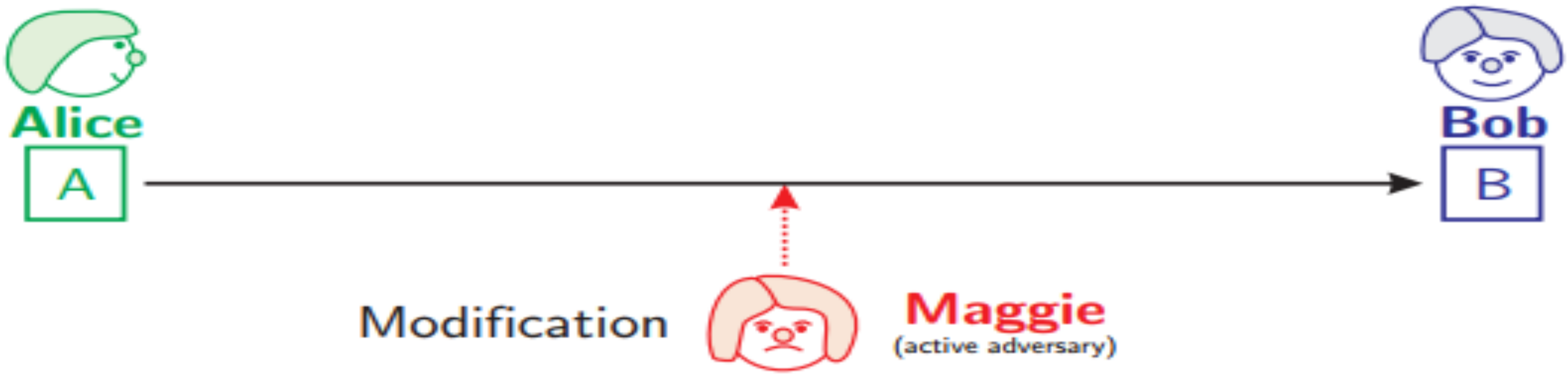


This comprises two separate requirements:

- no observer can access the contents of the message; and
- no observer can identify the sender and receiver.

The term 'privacy' or 'secrecy' is also used to mean confidentiality

Goal 2: Integrity
(Has been altered?)



This requires that the recipient can be sure that:

- the message has not been changed or lost during transmission;
- the message has not been prevented from reaching the recipient; and
- the message has not reached the recipient twice.

Goal 3: Authentication
(Who am I dealing with?)

This requires that:

• the sender can be sure that the message reaches the intended recipient, and only the intended recipient; and

• the recipient can be sure that the message came from the sender and not an imposter. The act by an imposter of sending such a message is referred to as ’spoofing’.

Goal 4: Availability
(Is it available?)

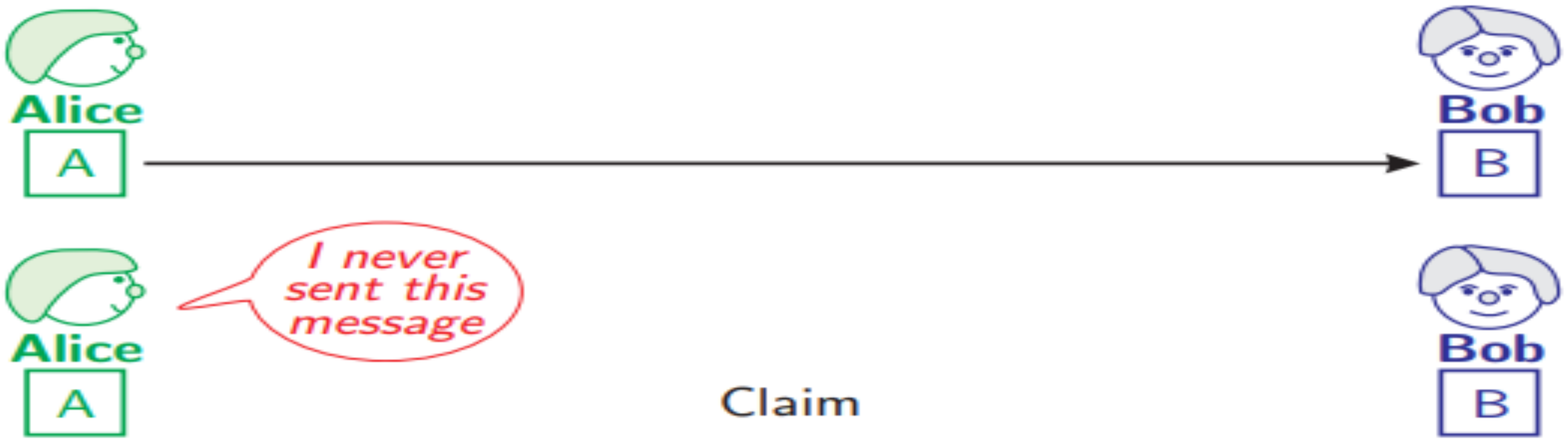
This requires that the following items must be functioning correctly:

- the computing systems used to store and process the information.
- the security controls used to protect the information.
- the communication channels used to access the information.

Availability appears as a target in information security.

Attacks such as Denial of Service (DoS) are a common threat to availability

Goal 5: Non-Repudiation
(Who sent/received it?)



This requires that:

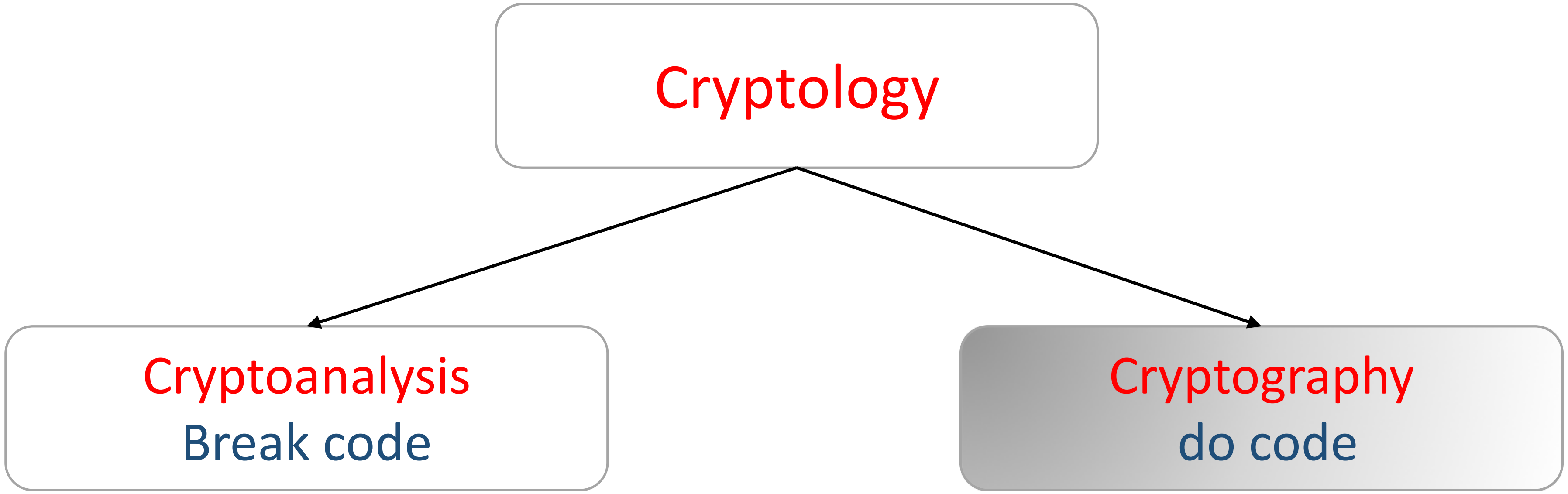
- the sender cannot credibly deny that the message was sent by them; and
- the recipient cannot credibly deny that the message was received by them.

Terminology

- The message is called plaintext or cleartext.
- Encoding the contents of the message in such a way that hides its contents from outsiders is called encryption.
- The encrypted message is called ciphertext.
- The process of retrieving the plaintext from the ciphertext is called decryption.
- Encryption and decryption usually make use of a key.

Terminology (cont.)

- Cryptoanalysis is the art of deciphering the ciphertext message.
- Cryptology is the science of encoding messages (cryptography) and decoding them (cryptoanalysis).



Common Players

- Alice and Bob: Good guys. Generally Alice wants to send a message to Bob.
- Eve: an *eavesdropper*, she is a passive attacker.
- Maggie: *malicious attacker* (sometimes Mallory), she is an active attacker; unlike Eve, Maggie can modify messages, substitute his own messages, replay old messages, and so on.
- Peggy: a *prover*
- Victor: a *verifier*

The problem of securing a system against Maggie is much greater than against Eve

These names were used by Ron Rivest in the 1978 paper presenting the RSA cryptosystem and believed to come from the childrens novel "Alice in Wonderland" by Lewis Carroll

One–Time Pad (OTP)
(Gilbert Sandford Vernam, AT&T, 1917)

One–Time Pad is a very simple Polyalphabetic encryption algorithm in which the key that encrypts and decrypts is a block of random data called pads that cannot be reused. This pad must be at least as long as the plaintext message.

- plaintext: a binary string of length n.
- key: a sequence of random bits of length n.
- encryption: exclisive-or of the plaintext and the key.
- decryption: exclusive-or of the ciphertext and the key.

In the 1940's Claude Shannon proved that OTP has perfect secrecy iff there are as many possible keys as possible plaintexts, i.e., the key size ≥ plaintext size.

Exclusive-Or operator (XOR)

a	b	C = a ⊕ b
0	0	0
0	1	1
1	0	1
1	1	0

exclusive-or is equivalent to addition modulo 2.

OTP Example

Encryption

Plaintext	0 1 0 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1 0 0 1 1 1 0
Key	0 1 0 1 0 0 0 1 1 0 0 1 0 0 1 1 1 0 0 0 0 0 0 1
ciphertext	0 0 0 1 0 1 1 1 1 1 0 0 0 1 1 0 1 1 0 0 1 1 1 1

Decryption

Ciphertext	0 0 0 1 0 1 1 1 1 1 0 0 0 1 1 0 1 1 0 0 1 1 1 1
Key	0 1 0 1 0 0 0 1 1 0 0 1 0 0 1 1 1 0 0 0 0 0 0 1
plaintext	0 1 0 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1 0 0 1 1 1 0

The messages corresponds to the binary representation of the text ”FUN”

OTP Example on Mod 26

Assign each letter a numerical value: e.g. ”A” is 0, ”B” is 1, and so on. To encrypt, combine plaintext and key using modular addition. To decrypt, the key is subtracted from the ciphertext using modular arithmetic.

Encryption

Plaintext	7 (H)	4 (E)	11 (L)	11 (L)	14 (O)
Key	4 (E)	14 (O)	23 (X)	9 (J)	5 (F)
ciphertext	11 (L)	18 (S)	8 (I)	20 (U)	19 (T)

Decryption

Ciphertext	11 (L)	18 (S)	8 (I)	20 (U)	19 (T)
Key	4 (E)	14 (O)	23 (X)	9 (J)	5 (F)
plaintext	7 (H)	4 (E)	11 (L)	11 (L)	14 (O)

Notice that there are 26^5 (11881376) possible keys of length 5, each with the same probability (26^{-5}) of being picked

One–Time Pad

Pros and Cons

Advantages

- Easy to encrypt and decrypt
- Hard to break (theoretically unbreakable)

Disadvantages

- key must be as long as the plaintext
- key distribution and management is difficult to accomplish
- key can only be used once

These drawbacks make OTP unpractical!

Perfect Secrecy

In the 1940's Claude Shannon introduced the term perfect secrecy stating that

"the ciphertext should leak NO information whatsoever about the plaintext, regardless of its distribution"

More formally:

$$Pr[\mathrm{M} = m \mid \mathrm{C} = \mathrm{c}] = Pr[\mathrm{M} = m]$$

where M and C represent the random variables taking the value of the actual message and ciphertext, respectively.

the OTP is effectively the only example of a perfect secrecy (unbreakable) cipher

It is impossible to guarantee the security of a cipher system even it is theoretically secure, it may be insecure in practice

Perfect Secrecy

- Let Pr(m_i = 0) = x, Pr(m_i = 1) = 1 − x and Pr(k_i = 0) = Pr(k_i = 1) = 1/2, then

m_i	**Prob.**	k_i	**Prob.**	c_i	**Prob.**
0	X	0	1/2	0	x/2
0	x	1	1/2	1	x/2
1	1-x	0	½	1	(1-x)/2
1	1-x	1	1/2	0	(1-x)/2

Pr(c_i = 1) = Pr(c_i = 0) = x/2 + (1 − x)/2=1/2, therefore ciphertext looks like a random sequence.

Attacker can do no better than just guessing

Unconditionally Secure Vs Computationally Secure

- In practice, unconditionally secure ciphers, thus, requiring that no adversary can learn anything about the plaintext, is quite complex.

- A cipher requiring that no adversary running in a reasonable among of time (e.g. 10^6 years) can learn anything about the plaintext except with a very small probability (e.g. 2^{-64}) is more feasible and it is call *computationally secure*

Some modern computationally secure ciphers are based on hardness of integer factorization problem and the discrete logarithm problem

Kerckhoffs’ Principle

In the 1883, Auguste Kerckhoffs stated that

“A cryptosystem should be secure even if everything about the system, except the key, is public knowledge. ”

As opposed to ”security by obscurity”

Kerckhoffs’ principle was reformulated by Claude Shannon as ”The enemy knows the system.”

Some advantages of open cryptographic design are:

- Public scrutiny leads to higher confidence
- No need to protect against reverse engineering
- Standards can be established

References

- Pinzon, Yoan. “Introducción a la criptografía y a la seguridad de la información”, 2013.
- Menezes A., Handbook of applied Cryptografy, 5th Edition. CRC Press, 2001.
- A Graduate Course in Applied Cryptography by D. Boneh and V. Shoup
- H. Delfs and H. Knebl, Introduction to Cryptography, 3rd ed. 2015.
- J. A. Buchmann, Introduction to Cryptography. 2004.
- T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, Ch. 31 in Introduction to Algorithms, 3rd ed. 2009.
- B. Lomas de Zamora: Gradi. Hacking desde cero, Fox Andina, 2011.
- Secure Coding Working Group, Japan Smartphone Security Association (JSSEC), Android Application Secure Design/Secure Coding Guidebook, 2017.