

# Introduction

## – Cryptography and Secured Communications –

Lionel Morel

Telecommunications - INSA Lyon

Fall-Winter 2021-22

# Lecturer - Lionel Morel<sup>2</sup> (lionel.morel@insa-lyon.fr)

- ▶ MSc in Computer Science - Grenoble 2001
- ▶ PhD in CS at INPGrenoble - Programming of Critical Reactive Systems
- ▶ Associate Professor at INSA Lyon since 2007.
- ▶ (past) Research topics:
  - ▶ at Grenoble, Turku (Finland), Rennes, and Lyon: Models of concurrency and computations, programming languages, performance analysis for parallel multi-core architectures.
  - ▶ at CEA-Grenoble (2017-2020): **Counter-measures against physical (side-channel, fault-injection, etc) attacks**
- ▶ Current Research: **operating systems** and programming languages **for** addressing so-called **frugality**, Phenix Citi<sup>1</sup>
- ▶ Teaching at the IF department: Computer Architecture, Operating Systems, Compiler Construction

---

<sup>1</sup><https://phenix.citi-lab.fr/>

<sup>2</sup>[lionel.morel.ouvaton.org/](https://lionel.morel.ouvaton.org/)

# Course Objectives

Give you some “necessary and sufficient” background on:

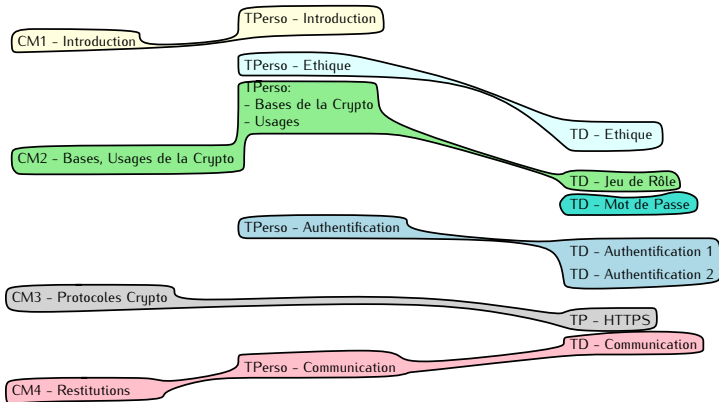
- ▶ Cryptography
- ▶ Cryptographic protocols
- ▶ Public-key infrastructures
- ▶ Associated ethical issues

# Course Plan

W1



W9



# Information Security

- ▶ **Information security**  $\triangleq$  practice of protecting information by mitigating information risks<sup>3</sup>
- ▶ Need to protect all elements dealing with information: computers, networks, people
- ▶ Security covers a lot of different aspects: physical security, social engineering, communication security, etc.
- ▶  $\triangleq$  practice that allows to maintain the CIA triad (see next)

---

<sup>3</sup>[https://en.wikipedia.org/wiki/Information\\_security](https://en.wikipedia.org/wiki/Information_security)

# The CIA Triad

- ▶ **Confidentiality**: Information is not made available or disclosed to unauthorized individuals, entities, or processes.<sup>4</sup>
- ▶ **Integrity**: Information is not modified in an unauthorized or undetected manner. Also called **anti-tampering**.
- ▶ **Availability**: Information is available when it is needed.

---

<sup>4</sup>Beckers, K. (2015). Pattern and Security Requirements: Engineering-Based Establishment of Security Standards.

# Threats

- ▶ A **threat** is a potential negative action or event that can result in unwanted impact to a computer system, application or user information.
- ▶ A **threat model** is a set of properties that characterize threats associated to a particular environment. Often implies **security requirements** on a system.

# Vulnerabilities

- ▶ A **vulnerability** is a weakness which can be exploited by an attacker to access unauthorized information or to compromise the attacked system's behavior.
- ▶ The **attack surface** of a system/application is the set of (known) vulnerabilities exposed by it to a potential attacker.



# Attacks

- ▶ **Attack** = Attempt to exploit a vulnerability
- ▶ Attack can be:
  - ▶ Passive (eavesdropping, side-channel, etc)
  - ▶ Active (worm, faults, etc)
  - ▶ Denial-of-service
- ▶ When the attack is successful, we say the system is **compromised**

# Trust

- ▶ **Trust** = Degree to which an entity (person, system, hardware, software) is going to behave as expected
- ▶ A **Trust model** describes which entity(ies) is/are trusted and at which level.

# Threats and attack techniques - Examples

- ▶ Eavesdropping, Trojans, Worms, Viruses
- ▶ Buffer Overflows, Spoofing, MITM attacks, Replay attacks,
- ▶ Shoulder surfing, Dumpster diving,
- ▶ Password attacks (brute-force, dictionary based), malicious-code attacks,
- ▶ Side-channel attacks: cache, timing, power-monitoring, etc.

## Quelques définitions:

- ▶ Trojan
- ▶ Worm
- ▶ Virus
- ▶ Buffer Overflow
- ▶ Spoofing
- ▶ Man-in-the-Middle Attack
- ▶ Replay

# Defenses - a quick panorama

- ▶ Cryptography
- ▶ Secured communication protocols
- ▶ Code and Data Encryption
- ▶ Physical shielding
- ▶ White-box cryptography

# Definition - Communication Security

**Communication Security**  $\triangleq$  discipline of preventing unauthorized interceptors from accessing telecommunications in an intelligible form, while still delivering un-altered content to the intended recipients.

Confidentiality

Availability

Integrity

5

---

<sup>5</sup>inspiration:

[https://en.wikipedia.org/wiki/Communications\\_security](https://en.wikipedia.org/wiki/Communications_security)

# Cryptology

Cryptology, is the science of practice and study of techniques for secure communication in the presence of adversarial behavior.

- ▶ **Cryptography:** Practice and study of techniques for secure communication in the presence of adversarial behavior.
- ▶ **Cryptanalysis:** Process of analyzing information systems in order to understand hidden aspects of the systems.
- ▶ **Cryptology = Cryptography + Cryptanalysis**

In this course, we mainly focus on **Cryptography**.

# A brief history of cryptography

- ▶ Keeping message secret has always been a (powerful) men's concern ...
- ▶ ... but (at least today) it's also of every person's interest.
- ▶ ... because there is no "I got nothing to hide"



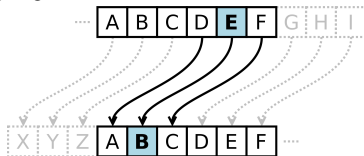
# History (1) Caesar cipher

- ▶ Substitution cipher
- ▶ Each letter is encoded with its order in the alphabet: A→0, B→1, ..., Z→26
- ▶ We choose a **fixed shift value**  $sh$
- ▶ To **encrypt**, each letter  $P_i$  in Plaintext is replaced by the corresponding shifted letter:

$$E(P_i) = (P_i + sh) \bmod 26$$

- ▶ To **decrypt**, each letter  $C_i$  in the Ciphertext is converted back with :

$$D(C_i) = (C_i - sh) \bmod 26$$



# History (1) Caesar cipher

- ➕ Encryption and decryption are cheap
- ➖ Easy to crack with frequency analysis
- ➖ Sufficient when no-one around can read :) (in particular, what's the difference between a foreign language and an encrypted language, if you can't read the first).



# One-time pad

- ▶ Substitution cipher
- ▶ Choose a **random key**  $K$  as least as long as the plaintext
- ▶ To **encrypt**, each letter  $P_i$  in Plaintext is replaced by the corresponding shifted letter:

$$E(P_i) = (P_i + K_i) \bmod 26$$

- ▶ To **decrypt**, each letter  $C_i$  in the Ciphertext is converted back with :

$$D(C_i) = (C_i - K_i) \bmod 26$$

A	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
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	
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	
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	C	
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	

# One-time pad - Pros and Cons

- ⊕ Proven secure
- ⊕ Even to frequency analysis
- ⊕ Encryption and decryption are cheap
- ⊖ Key must be as long as the plaintext ...
- ⊖ Key must be kept secret
- ⊖ Key must not be lost (not by one character)
- ⊖ Key must be truly random

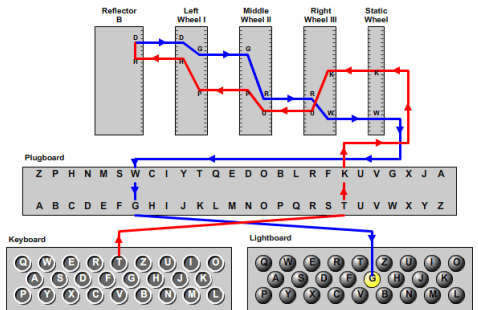
# Enigma

- ▶ Invented at the end of WWI
- ▶ Used extensively by Nazi Germany during WWII
- ▶ First cracked by Polish services during the early 30s ...
- ▶ ... then by British-led effort at Bletchley Park, including Alan Turing.



# Enigma - How does it work?

## ► Substitution cipher



© 2006, by Louise Dade

# Enigma - Combinatorial

- ▶ **Every day**, the machine is reset to a pre-established configuration:
  - ▶ 20 Rotors choice (3 or 4 or 5 among 6 possible).
  - ▶  $26^3$  Rotors permutation
  - ▶  $26^3$  Rotors initial positions
  - ▶ Plug-board settings:  $150 \cdot 10^{12}$
- ▶ **Every message** contains a rotors position the machine should be reset to before decrypting the rest of the message.

# Enigma - Breaking the machine

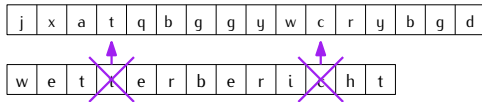
- ▶ To brute-force Enigma is unpractical: 150 millions millions combinations
- ▶ A letter is encrypted into a different letter every time ....
- ▶ ... but never to itself !! **Main flaw**
- ▶ Try to guess a word or phrase in a message (and Germans military did use recurring messages, like weather reports)
- ▶ ...



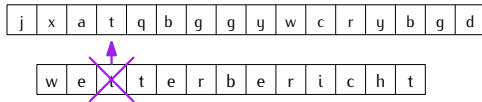
# Enigma - breaking the machine

j	x	a	t	q	b	g	g	y	w	c	r	y	b	g	d
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

# Enigma - breaking the machine



# Enigma - breaking the machine



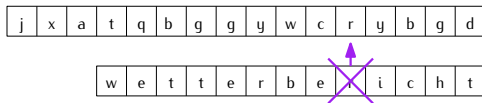
# Enigma - breaking the machine

j	x	a	t	q	b	g	g	y	w	c	r	y	b	g	d
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

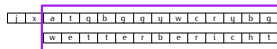
w	e	t	t	e	r	b	e	r	i	c	h	t
---	---	---	---	---	---	---	---	---	---	---	---	---

OK !

# Enigma - breaking the machine



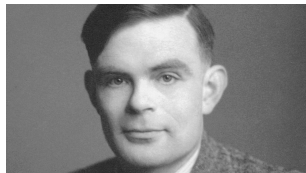
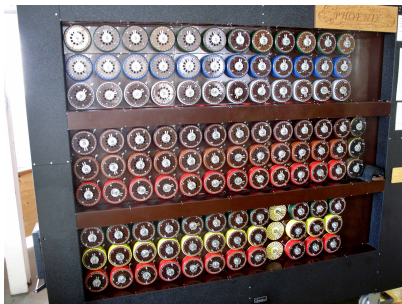
Possible Solutions



# Enigma - Breaking the machine

- ▶ Adding a couple more properties, evict impossible configurations.
- ▶ Scan through the remaining combinations using **the Bombe** : electro-mechanical machine able to “play” 36 Enigma equivalent “in parallel”.
- ▶ In the end .... guess the key (wheel starting positions + plug-board) in less than 20minutes per day.

# Enigma



<sup>6</sup>watch

[https://en.wikipedia.org/wiki/The\\_Imitation\\_Game](https://en.wikipedia.org/wiki/The_Imitation_Game)

# Next time - Cryptography

- ▶ Symmetric cryptography
- ▶ Asymmetric cryptography
- ▶ Key sharing