Introduction to Cryptography

Alessandro Barenghi

Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB)
Politecnico di Milano

alessandro -dot- barenghi - at - polimi -dot- it

Word of Warning

- This is a short, simplified introduction to cryptography
- We will only introduce what is needed for systems security discussions

What is cryptography (alt. cryptology)?

Definition

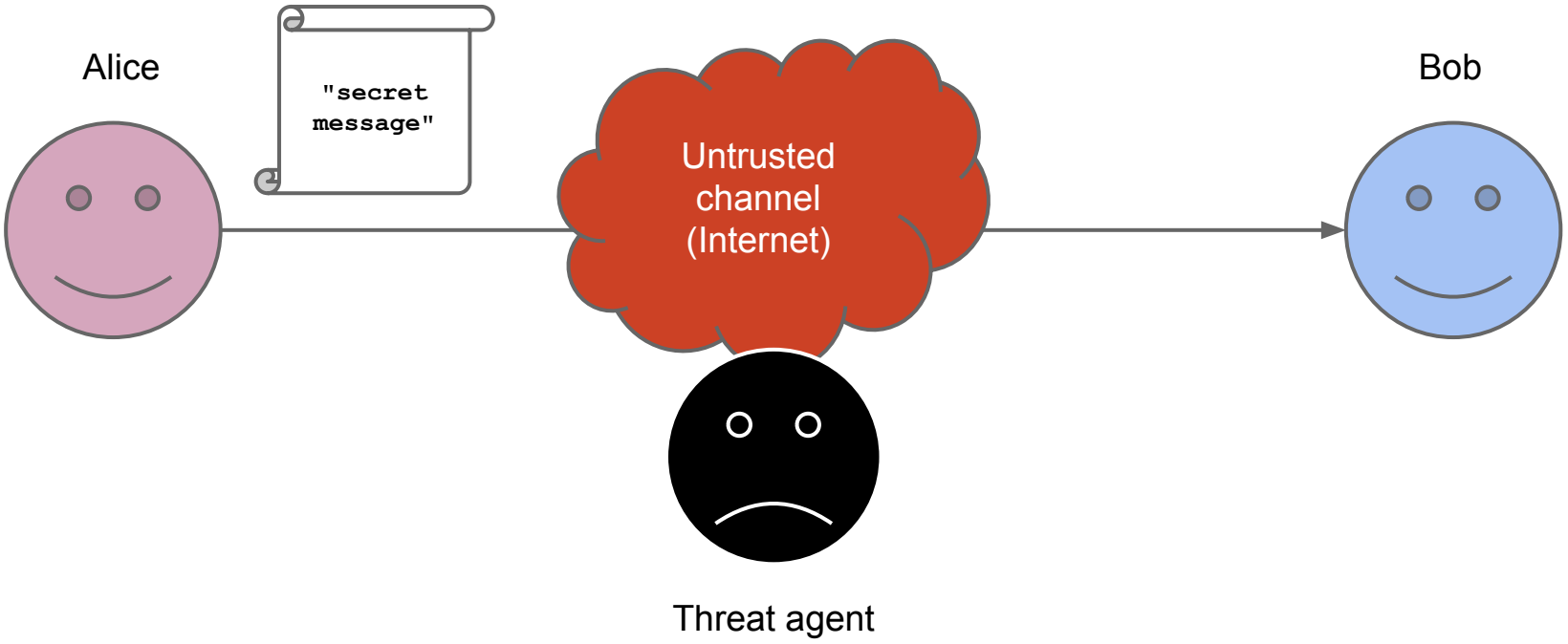
- The study of techniques to allow secure communication and data storage in presence of attackers

Features provided

- **Confidentiality**: data can be accessed only by chosen entities
- **Integrity/freshness**: detect/prevent tampering or replays
- **Authenticity**: data and their origin are certified
- **Non-repudiation**: data creator cannot repudiate created data
- **Advanced features**: proofs of knowledge/computation → DEMONSTRATE TO KNOW SOMETHING WITHOUT EXPLICITLY TELLING IT

SHARED COMPUTATION OF THE KNOWLEDGE, NOT SHARED THE KNOWLEDGE ITSELF ←

The Problem to Solve: Confidentiality and Integrity



A Brief History of Cryptography

- From Greek: *kryptos*, hidden, and *graphein*, to write (i.e., *“art of secret writing”*)
- Ancient history: writing itself was already a “secret technique”.
- Cryptography born in Greek society, when writing became more common, and hidden writing became a need.

Cryptographic prehistory

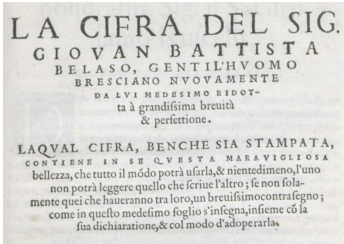
As old as written communication

- Born for commercial (recipe for lacquer on clay tablets) or military (Spartans) uses
- Designed by humans, for human computers
- Algorithms computed by hand, with pen and paper

Ancient view

Original approach

- A battle of wits between
  - cryptographers: ideate a secret method to obfuscate a text
  - cryptanalysts: figure out the method, break the "cipher"
- Bellaso (1553) [1] separates the encryption method from the key


LA CIFRA DEL SIG.
GIOVAN BATTISTA
BELASO, GENTIL'HVOMO
BRESCIANO NVOVAMENTE
DA LVI MEDESIMO RIDOT-
ta à grandiſsima breuità
& perfettione.

LAQVAL CIFRA, BENCHE SIA STAMPATA,
CONTIENE IN SE QVESTA MARAVIGLIOSA
bellezza, che tutto il mõdo potrà uſarla, & nientedimeno, l'uno
non potrà leggere quello che ſcriue l'altro; ſe non ſola-
mente quei che haueranno tra loro, un breuiſsimo contraſegno;
come in queſto medeſimo foglio s'inſegna, inſieme cõ la
ſua dichiaratione, & col modo d'adoperarla.

A Brief History of Cryptography

- Medieval and renaissance studies
  - **Gabriele de Lavinde**, who wrote a manual in 1379, copy available at the Vatican archives.
  - The mirror writing of **Leonardo da Vinci**.
- Mostly a *military interest*
  - Italian Army General **Luigi Sacco** wrote a famous *“Nozioni di crittografia”* book in 1925, one of the last “non-formalized” exercises in cryptography.

Cryptographic history

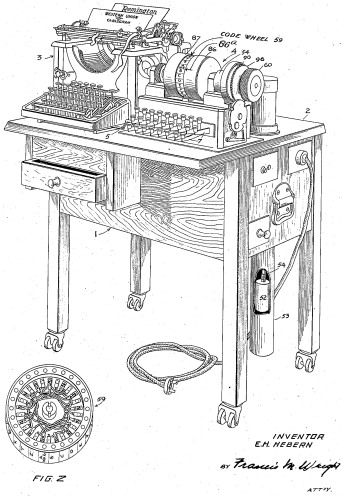
1883 - Kerchoff's six principles for a good cipher (apparatus)

1. It must be practically, if not mathematically, unbreakable
2. It should be possible to make it public, even to the enemy
3. The key must be communicable without written notes and changeable whenever the correspondants want
4. It must be applicable to telegraphic communication
5. It must be portable, and should be operable by a single person
6. Finally, given the operating environment, it should be easy to use, it shouldn't impose excessive mental load, nor require a large set of rules to be known

Cryptographic modern history

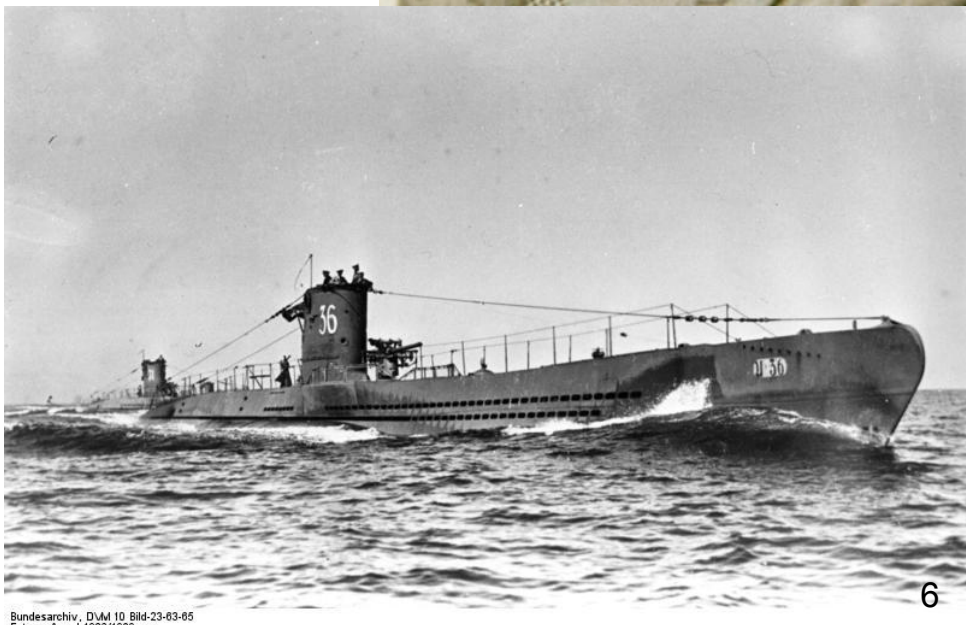
The advent of the machines

- Mechanical computation changes cryptography
  - First rotor machine in 1917 by Ed Hebern
  - Design "popularized" in WWII by German Enigma
- Cryptanalysist at Bletchley park (Turing among them) credited for a decisive effort in winning the war by Eisenhower



When Math Won a War

- During WWII, **Alan Turing** worked at Bletchley Park to **break** Axis ciphers, in particular the **Enigma cipher**.



Bundesarchiv, DVM 10 Bild-23-63-65
Foto: o.Ang. | 1936/1939 ca.

When Math Won a War

- During WWII, **Alan Turing** worked at Bletchley Park to **break** Axis ciphers, in particular the **Enigma cipher**.
- Birth of the first universal computers was stimulated by this effort.

THE BOMBE (replica)

Moving into the modern age

AN UNBREAKABLE CIPHER IS ONLY IDEOLOGICAL, BUT

An end to the battle of wits

- Shannon (1949) [4] - Proves that a mathematically unbreakable cipher exists
- Nash (1955) [2] - Argues that **computationally secure** ciphers are ok
  - Considers a cipher with a finite,λbit long, key
  - Conjecture: if "*parts of the key interact complexly [...] in the determination of their effects on the ciphertext*", the attacker effort to break the cipher would be $\mathcal{O}(2^{\lambda})$
  - The owner of the key takes $\mathcal{O}(\lambda^2)$ to compute the cipher
  - The computational gap is unsurmountable for large λ

SOMETHING NOT PERFECT BUT STRONG ENOUGH IS ACCEPTABLE

WE ARE TALKING ABOUT A BREAKABLE CIPHER BUT IN AN INCONVENIENT AMOUNT OF TIME

Key Concepts in Cryptography

- First formalized by Claude Shannon in his 1949 paper *"Communication theory of secrecy systems"*.
- **Cryptosystem**: a system that takes in input a message (known as **plaintext**) and transforms it into a **ciphertext** with a reversible function that usually takes a **key** as a further input.
- The use of *"text"* is historical, and today we mean *"string of bits"*.

Kerckhoffs' Principle

- *The security of a cryptosystem relies only on the secrecy of the key, and never on the secrecy of the algorithm.*
  - Auguste Kerckhoffs, *"La criptographie militaire"*, 1883
- This means that:
  - In a secure cryptosystem we cannot retrieve the plaintext from the ciphertext without the key.
  - Also, we cannot retrieve the key from analyzing ciphertext-plaintext pairs.
  - Algorithms must always be assumed known to the attacker, no secret sauce!

Outline of the topics

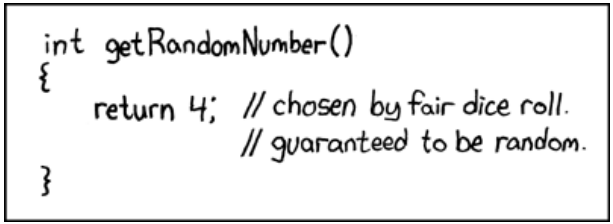
In this course

- Definitions of ciphers as components with functionalities
- How to obtain confidentiality, integrity, data/origin authentication
- An overview of protocols (combinations of ciphers)
- Goal: be able to use cryptographic components properly

In Cryptography and Architectures for Computer Security

- Design and cryptanalysis techniques for ciphers
- Cryptographic protocols and their inner workings
- Efficient, side channel attack resistant implementations
- Goal: be able to engineer cryptographic components

Before we start...



https://xkcd.com/221/

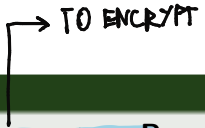
RANDOMNESS IS RELATED TO A PROCESS THAT GENERATE RANDOMIC NUMBERS

A "PURE RANDOM" NUMBER DOESN'T EXIST

A word on randomness

- Randomness (in this course) characterizes a generative process
- Stating: "00101 is a random string" actually makes little sense

Definitions



Data

- Plaintext space **P**: set of possible messages $\texttt{ptx} \in \mathbf{P}$
  - Old times: words in some human-readable alphabet, modern times $\{0,1\}^l$
- Ciphertext space **C**: set of possible ciphertext $\texttt{ctx} \in \mathbf{C}$
  - Usually $\{0,1\}^{l'}$, not necessarily $l = l'$ (ciphertexts may be larger)
- Key space **K**: set of possible keys
  - $\{0,1\}^\lambda$, keys with special formats are derived from bitstrings

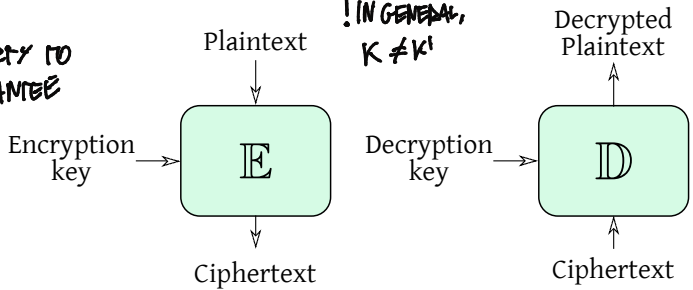
Definitions

Functions

- Encryption function $\mathbb{E} : \mathbf{P} \times \mathbf{K} \rightarrow \mathbf{C}$
- Decryption function $\mathbb{D} : \mathbf{C} \times \mathbf{K} \rightarrow \mathbf{P}$
  - Correctness: for all $\mathtt{ptx} \in \mathbf{P}$, we need $k, k' \in \mathbf{K}$ s.t. $\mathbb{D}(\mathbb{E}(\mathtt{ptx}, k), k') = \mathtt{ptx}$

PROPERTY TO GUARANTEE

! IN GENERAL, $K \neq K'$



Providing confidentiality

THE ATTACKER SHOULD NOT HAVE THE KEY

Goal

- Prevent anyone not authorized from being able to understand data

Possible attacker models

- The attacker simply eavesdrops (ciphertext only attack)
- The attacker knows a set of possible plaintexts
  - Limit case: the attacker chooses the set of plaintexts
- The attacker may tamper with the data and observe the reactions of a decryption-capable entity
  - Limit case: the attacker sees the actual decrypted value

SOMEONE THAT SIMPLY SPIES AND OBSERVES A CONVERSATION BETWEEN 2 USERS

CHOSEN-PLAINTEXT ATTACK