SMARCO

SMARt COmmunities Skills Development in Europe

Cybersecurity

Short Term Course – Unit 2

Cefriel

POLITECNICO DI MILANO

Co-funded by the European Union

smarco

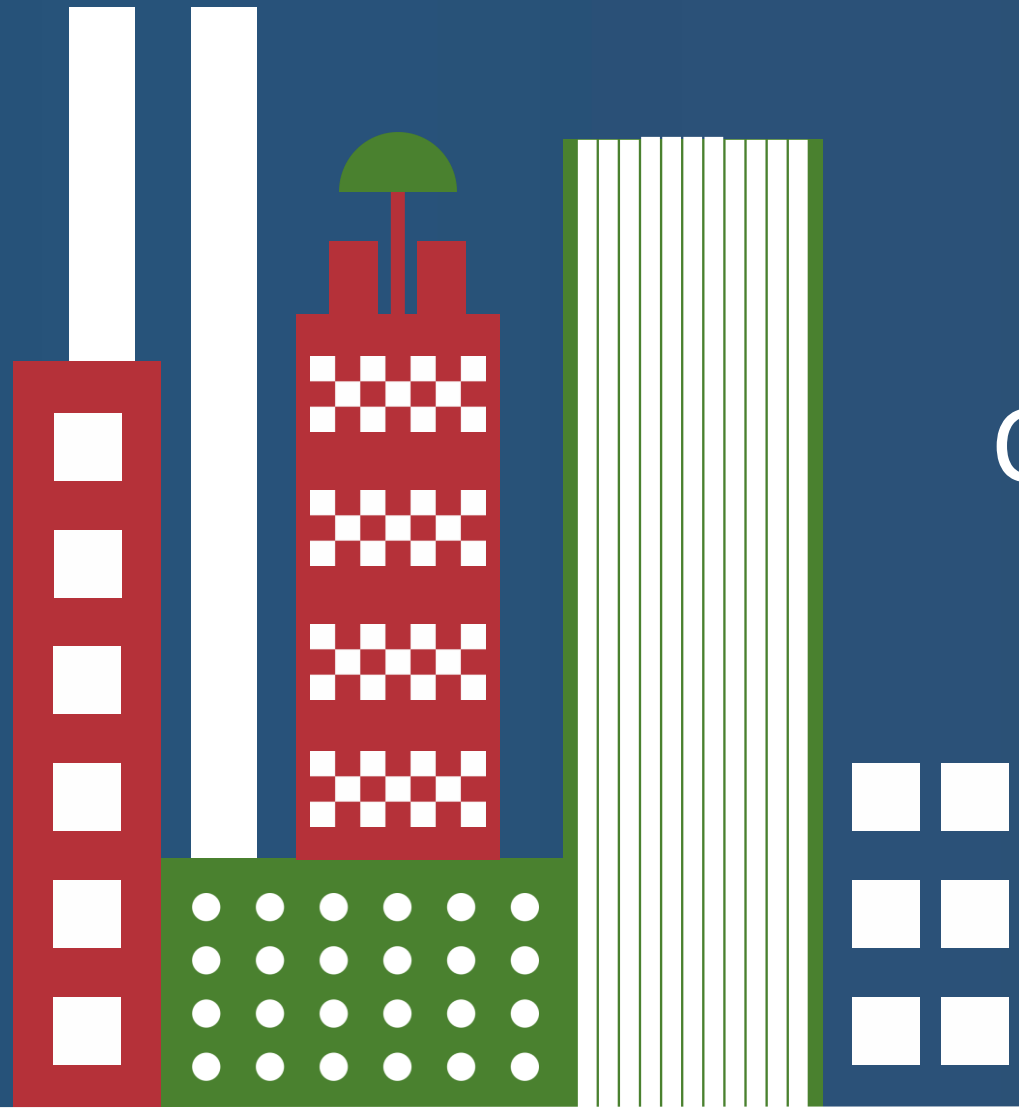
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Aim of the course

This course helps you enhance **smart communities' resilience** by teaching risk assessment, threat analysis, mitigation, encryption, and cybersecurity compliance to protect shared digital environments.

Co-funded by the European Union

smarco



Unit 2

Cryptography Fundamentals for Smart Community Engineers

Co-funded by the European Union

smarco

AGENDA

- Introduction to Cryptography
- Core cryptographic elements
- Security attacks and challenges
- Authentication and post-quantum cryptography

Co-funded by the European Union

smarco

How secure?

No Total Security

Absolute security is unattainable; different security levels provide varying protection degrees.

Evaluating Security Needs

Security measures must consider information value, costs, and usability impacts for balanced protection.

Contextual Security Levels

Security levels should be tailored to the sensitivity of information, from email to secret services.

Co-funded by the European Union

smarco

CIA paradigm

Cybersecurity is the set of technologies, processes, and practices designed to protect computers, networks, programs, and data from unauthorised access, attacks, or damage. Its core principles are encapsulated in the **CIA triad**:

- **Confidentiality**: Ensuring that sensitive information is accessible only to authorised individuals or systems.
- **Integrity**: Safeguarding the accuracy and trustworthiness of data by preventing unauthorized alterations.
- **Availability**: Guaranteeing that systems and data are accessible to authorised users when needed.

Co-funded by the European Union

smarco

Authorisation, non-repudiation, anonimity

Authorization and Access Control

Authorization limits resource access to verified users, typically based on authentication systems.

Non-Repudiation Service

Non-repudiation ensures message senders and recipients cannot deny sending or receiving communications.

Anonymity Protection

Anonymity protects sender or recipient identities, preventing their identification in communications.

Co-funded by the European Union

smarco

Data states

Data at Rest

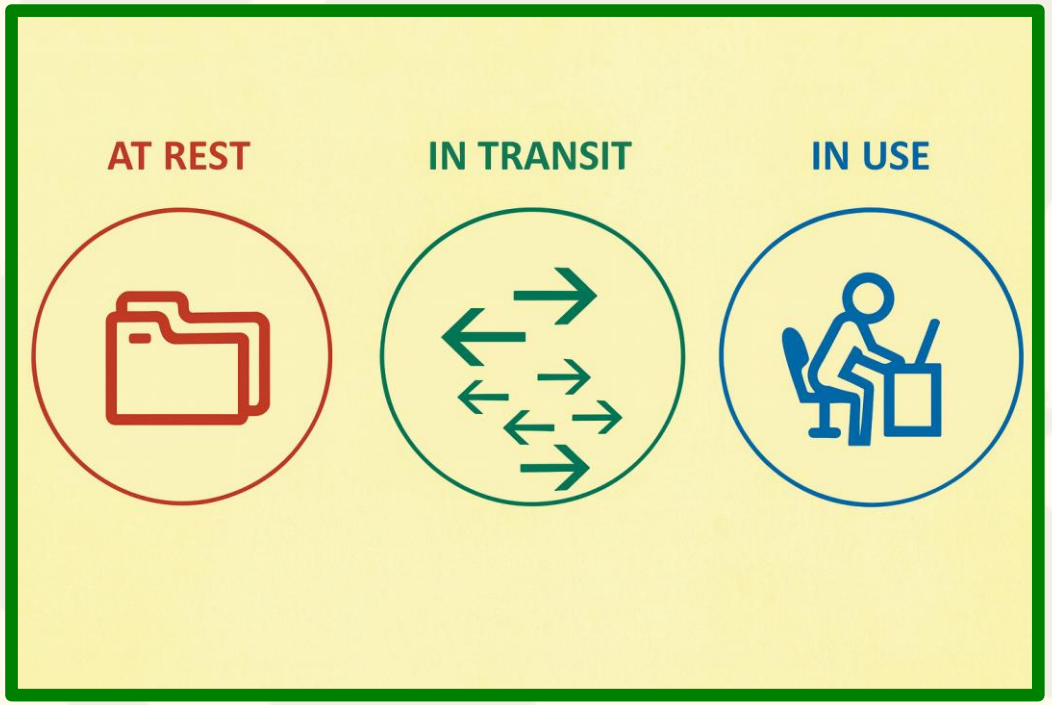
Data at rest refers to information stored on physical or logical media without active access.

Data in Transit

Data in transit is information traveling through communication channels like email and messaging apps.

Data in Use

Data in use is actively accessed or processed by applications or users for various purposes.



Co-funded by the European Union

smarco

Types of secrecy systems

Claude Shannon, 1949

Concealment Systems

These systems hide the very existence of a message using methods like invisible ink or steganography.

Privacy Systems

Privacy systems alter messages, such as speech inversion, requiring special equipment to recover intelligible content.

True Secrecy Systems

True secrecy hides the meaning of messages using ciphers or codes, assuming interception is possible.

Co-funded by the European Union

smarco

Probability and redundancy in cryptography

Claude Shannon, 1949

Discrete Information in Cryptography

Cryptographic messages consist of discrete symbols chosen from a finite set for secure communication.

A Priori Probability

A priori probability is the chance of an event before any evidence is gathered in secrecy systems.

A Posteriori Probability

A posteriori probability refers to chances of messages or keys after intercepting cryptograms in cryptanalysis.

Co-funded by the European Union

smarco

Probability and redundancy in cryptography

Claude Shannon, 1949

Redundancy: Associated with a language, there is a certain parameter D, which we call the redundancy of the language. D measures, in a sense, how much a text in the language can be reduced in length without losing any information. As a simple example, since u always follows q in English words, the u may be omitted without loss.

A **secrecy system** is defined abstractly as a set of transformations of one space (the set of possible messages) into a second space (the set of possible cryptograms). Each particular transformation of the set corresponds to enciphering with a particular key. The transformations are supposed reversible (non-singular) so that unique deciphering is possible when the key is known.

Each key and, therefore, each transformation is assumed to have an a priori probability associated with it—the probability of choosing that key. Similarly, each possible message is assumed to have an associated a priori probability, determined by the underlying stochastic process.

Co-funded by the European Union

smarco

The calculation of the a posteriori probabilities is the generalized problem of cryptanalysis

Example

Alphabetic message
In a simple substitution cipher with random key there are 26! transformations.
A priori probability in this case is 1/26!
Assumption: the text is in English
If the enemy intercepts N letters of cryptograms in this system his probabilities change. If N is large enough (say 50 letters) there is usually a single message of a posteriori probability nearly unity, while all others have a total probability nearly zero.
In this case there is an essentially unique “solution” to the cryptogram.
For N smaller (say N = 15) there will usually be many messages and keys of comparable probability, with no single one nearly unity.
In this case there are multiple “solutions” to the cryptogram.

Co-funded by the European Union

smarco

More concepts and terms on cryptography

A **cryptogram** is a type of puzzle or coded message in which the letters of the alphabet are substituted for one another, often with the aim of concealing the original content from unauthorized readers. Each letter in the plaintext is replaced by a corresponding letter in the ciphertext, forming a new message that can be deciphered by using a specific key or code
ROT13, Each letter is replaced by the one 13 positions after it in the alphabet. Applying ROT13 twice restores the original text.
Playfair Cipher, Encodes pairs of letters using a 5×5 grid derived from a keyword.

H(N) equivocation: measures in a statistical way how near the average cryptogram of N letters is to a unique solution; that is, how uncertain the enemy is of the original message after intercepting a cryptogram of N letters.
H(N) approaches to zero for longer N
ROT13 if the attacker has a long enough ciphertext sample, it can find the key (13)

Perfect secrecy: systems for which H(N) doesn't approach to zero as $N \to \infty$.
In other words, the ciphertext tells you nothing about the plaintext
Zero eavesdrops

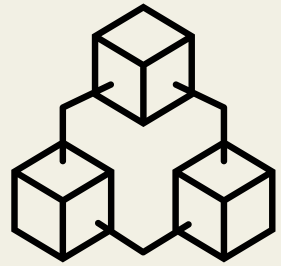
Co-funded by the European Union

smarco

Assumptions on cryptography

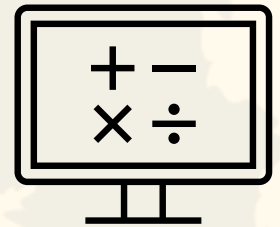
Cryptography as a Process

Cryptography involves networks, software, hardware, and people; it is a continuous security process, not a product.



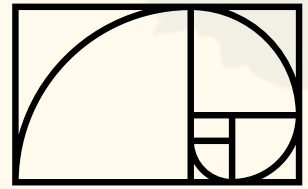
Common Security Mistakes

Common mistakes include using outdated protocols, short keys, self-signed certificates, and poor key management.



Avoiding Custom In-House Encryption

Relying on outdated or custom in-house encryption solutions often causes security problems and should be avoided.



Importance of Automation

Automation is critical to maintain security processes and ensure regular updates of keys and certificates.

Co-funded by the European Union

smarco

Basic cryptography

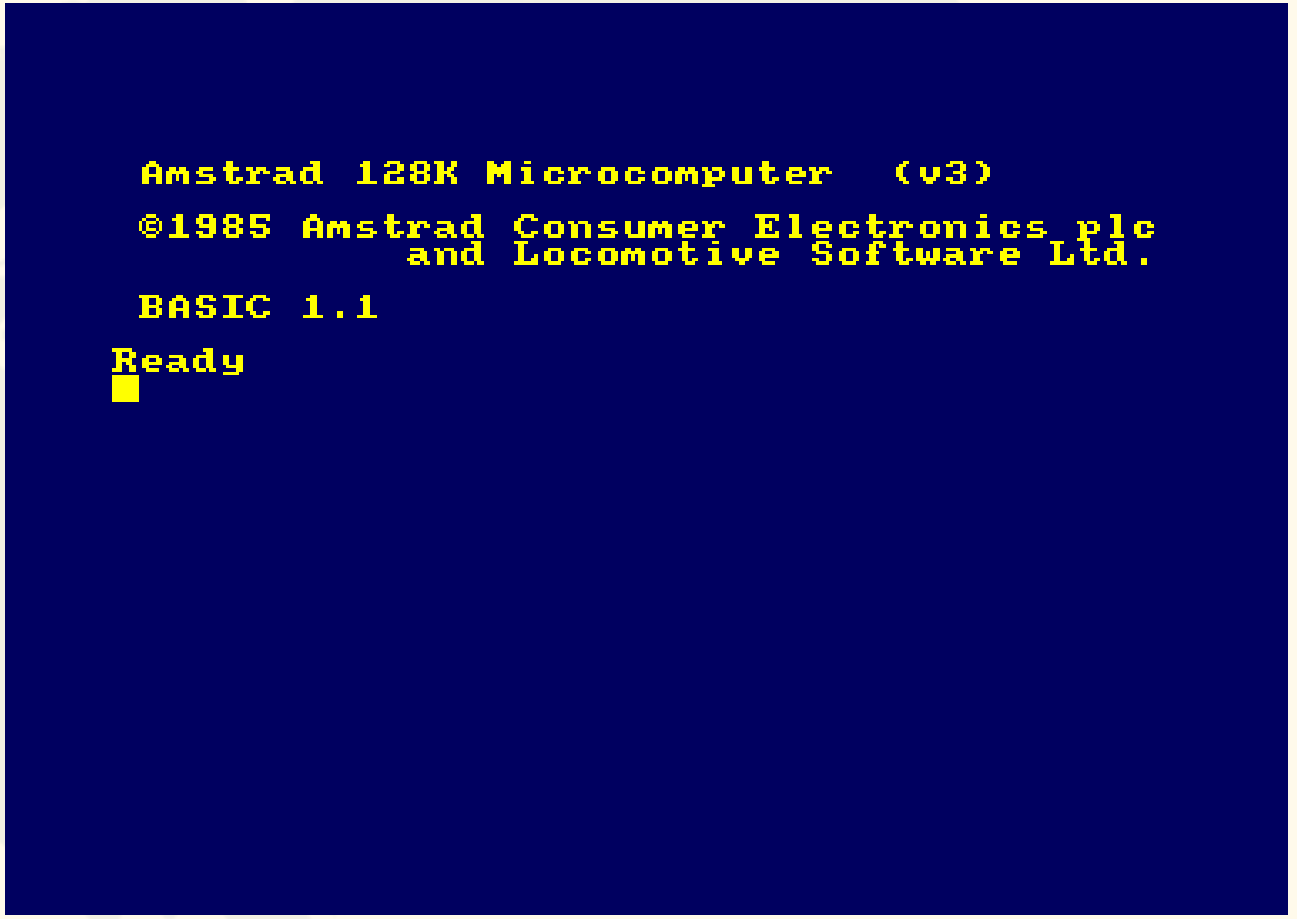
Basic cryptography is sufficient to cover some key aspects:

1. Integrity (one-way hash algorithm)

2. Confidentiality (encryption)

3. Authentication (digital signature/certificates)

4. Non-repudiation (a combination of the former)



Co-funded by the European Union

smarco

One-way hash functions and properties

Purpose and Characteristics

One-way hashes verify data integrity by producing fixed-length control bits. Altering one bit drastically changes the hash.

Common Algorithms

Popular hash algorithms include MD5, SHA-1, SHA-2, and SHA-3 with varying digest lengths and security features.

Hashing in Communication

Hashing ensures message integrity during transmission.

Salting for Security

Salting adds random data to passwords before hashing to enhance security and mitigate attacks.

Co-funded by the European Union

smarco

Hashing process and message verification

Hashing Overview

Hashing converts a message into a fixed-size digest for integrity verification.

Message Digest

The digest is a unique representation of the original message used for verification.

Message Verification

The digest is sent along with the message to verify authenticity and integrity.

Co-funded by the European Union

smarco

Common hash algorithms and their security

MD Family Hash Algorithms

MD2, MD4, and MD5 produce 128-bit hashes but MD5 is now insecure due to collision vulnerabilities.

SHA-1 Algorithm

SHA-1 produces 160-bit hashes and was widely used until attacks compromised its security in 2005.

SHA-2 Family

SHA-2 includes SHA-256, SHA-384, and SHA-512 with variable hash lengths, offering stronger security.

RIPEMD Algorithm

RIPEMD offers variable bit lengths and is a European alternative to MD5 and SHA-1.

Co-funded by the European Union

smarco

Salting passwords for protection

Concept of Salting

Salting adds random data to passwords before hashing to enhance security against attacks.

Salting in Password Hashing

The salt is concatenated with the password and hashed; both salt and hash are stored together.

Challenge of Salt Sharing

Sharing the salt securely during transmission presents challenges requiring careful protocol design.

Co-funded by the European Union

smarco

Encryption and decryption basics

Encryption and Decryption

Encryption transforms plain text into cipher text, while decryption reverses the process to retrieve the original text.

Requirement for Encryption

Both encryption and decryption require an algorithm and a key to securely encode and decode information.

Types of Keys

There are two main key types used in cryptography: symmetric keys and public (asymmetric) keys.

Co-funded by the European Union

smarco

Symmetric key cipher structure

Basic Structure

Symmetric key ciphers use the same key for both encryption and decryption processes.

Encryption Process

Plaintext is converted into ciphertext using the symmetric key and an encryption algorithm.

Decryption Process

Ciphertext is reverted to plaintext with the same key through a decryption algorithm.

Co-funded by the European Union

smarco

Asymmetric key cipher structure

Public and Private Keys

Asymmetric encryption uses a pair of keys: a public key for encryption and a private key for decryption to enhance security.

Encryption and Decryption Process

Data encrypted with the public key can only be decrypted by the corresponding private key, ensuring confidentiality.

Secure Communication

Asymmetric ciphers enable secure communication over unsecured channels without sharing private keys.

Co-funded by the European Union

smarco

Hill Cipher

Hill Cipher Matrix Operation

Hill cipher uses a matrix and its inverse as keys to encode and decode pairs of letters numerically.

Numeric Conversion of Text

Letters are converted to numbers using a defined table with padding for uneven text length.

Security and Vulnerabilities

Hill cipher is vulnerable to known-plaintext attacks due to linear dependency but resists brute-force attacks effectively.

Diffusion Property Advantage

The cipher diffuses data so nearby plaintext values become distant in ciphertext after key multiplication.

Co-funded by the European Union

smarco

Hill Cipher - vulnerabilities

Key Space and Matrix Constraints

The number of valid keys depends on invertible matrices without null rows, limiting keys for n=2 to about 26.

Resistance to Brute-Force Attacks

Hill cipher is highly effective against brute-force attacks due to the limited number of valid keys and matrix conditions.

Known-Plaintext Attack Vulnerability

Linear dependency in the algorithm makes it vulnerable to known-plaintext attacks using linear algebra to find keys.

Diffusion Property Advantage

Hill cipher provides diffusion by spreading nearby plaintext data far apart in ciphertext after key multiplication.

Co-funded by the European Union

smarco

Key-based authentication process

Evolution from Passwords

Key-based authentication is an evolution of password authentication with secret information kept securely by the user.

Secret Information Usage

Users prove possession of secret information by encrypting a predefined message instead of entering the secret directly.

Verification by System

System verifies encryption correctness to authenticate the user, ensuring secure and reliable access.

Co-funded by the European Union

smarco

Security by obscurity

Kerkhoffs's Principle

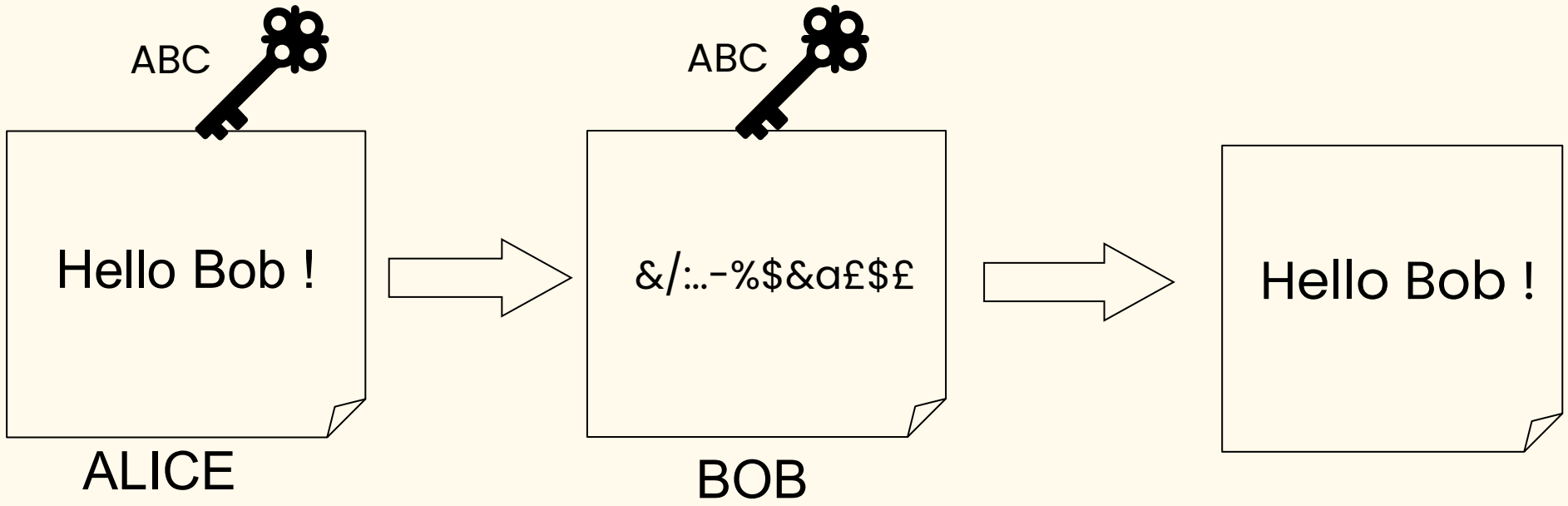
"The security of an encryption scheme must not depend on keeping the algorithm secret. Security relies solely on keeping the key secret." (La cryptographie militaire, 1883)

Co-funded by the European Union

smarco

Symmetric key

It requires a “shared secret” between Alice and Bob



Co-funded by the European Union

smarco

Public key

No “shared secret”

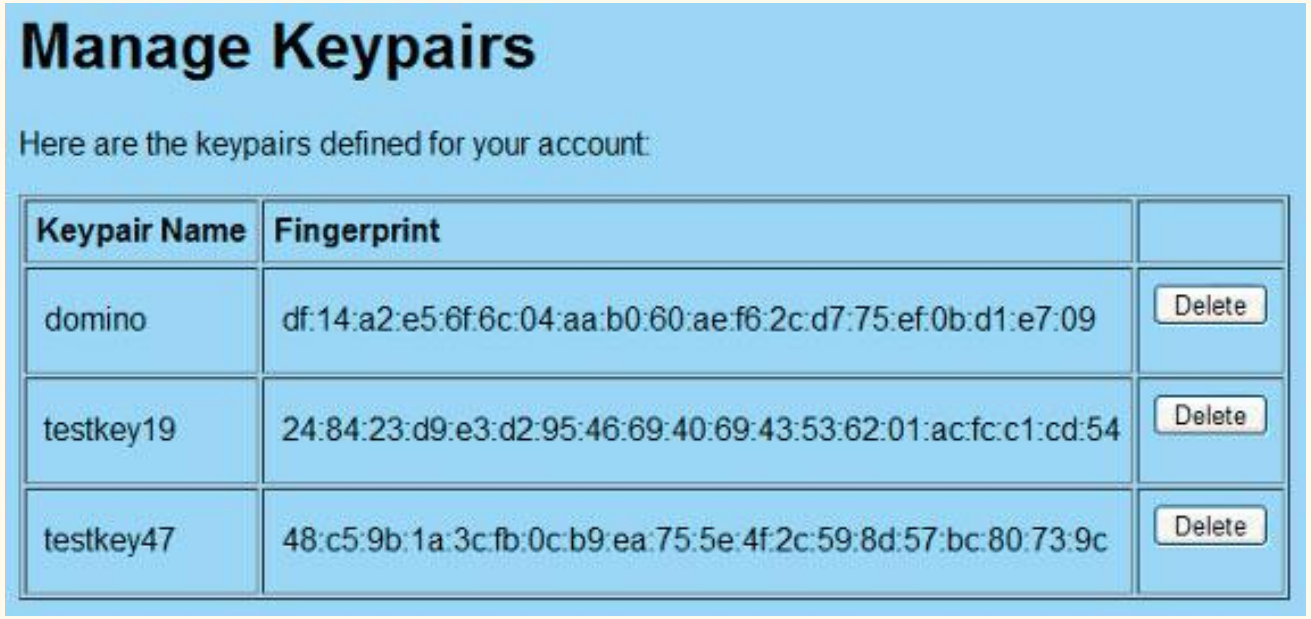
Two keys are created at the same time:

- A private key
- A public key

One encrypt and the other decrypt.

Infinite number of combinations

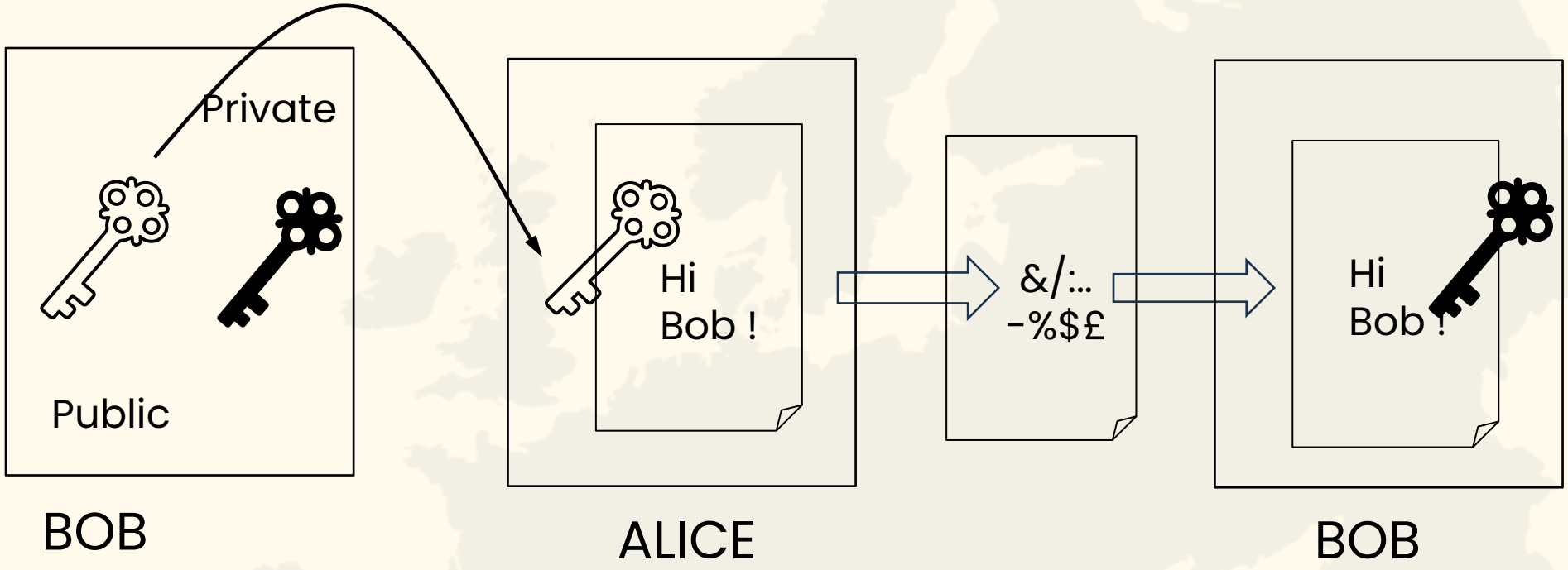
It is not possible to determine one knowing the other



Co-funded by the European Union

smarco

Public key

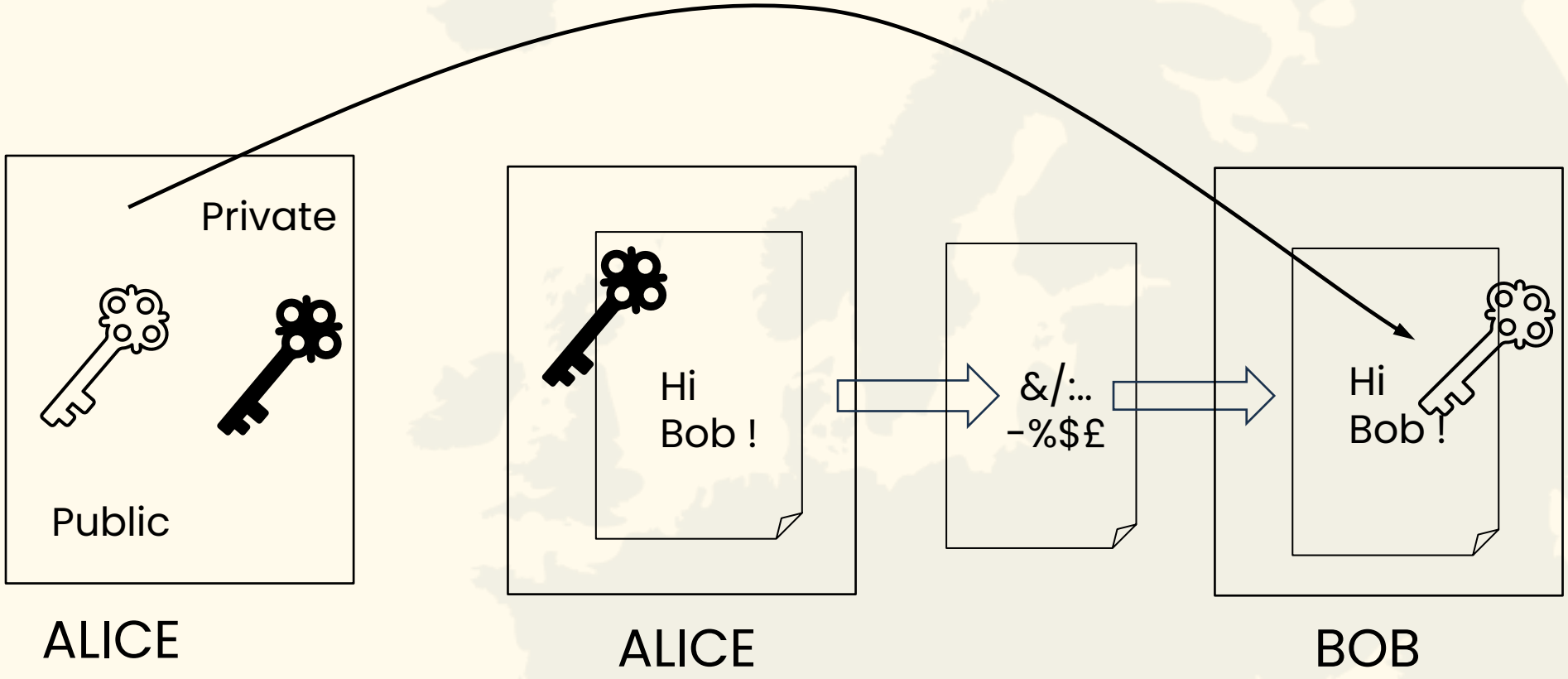


- Integrity
- Confidentiality

Co-funded by the European Union

smarco

Public key



- Non-repudiation
- Authentication

Co-funded by
the European Union
smarco

Asymmetric key/public key

Pros & Cons:

+ More secure

- Slower

Co-funded by the European Union

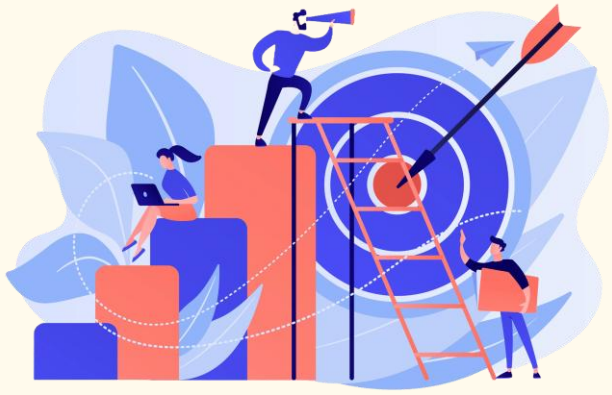
smarco

Unit Completed – What's Next?

To consolidate your learning and reflect on the key concepts covered, please take a moment to complete this quiz.

Your feedback and results will help you track your progress and support continuous improvement of the training experience.

Click the link to begin the quiz!



Co-funded by the European Union

smarco

SMARCO

SMARt COmmunities Skills Development in Europe

www.smarco.eu

info@smarco.eu

We are social! Follow us on:

@smarcoproject

@smarcoproject

@smarcoproject

Co-funded by the European Union

smarco

Cefriel
POLITECNICO DI MILANO

Project 101186291 — SMARCO