Università degli Studi di Trieste

Corso di Laurea Magistrale in
INGEGNERIA CLINICA

DATA PROTECTION BASIC PRINCIPLES

Corso di Informatica Medica

Docente Sara Renata Francesca MARCEGLIA

Dipartimento di Ingegneria e Architettura

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Why medical data are critical

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

BANKING

Data OWNER	=	Data USER
Bank account holder		Bank account holder

MEDICINE

Data OWNER	≠	Data USER
Patient		Healthcare professional

In medicine the owner of data does not have the knowledge to use it → data have to be shared with others

SHARED CARE

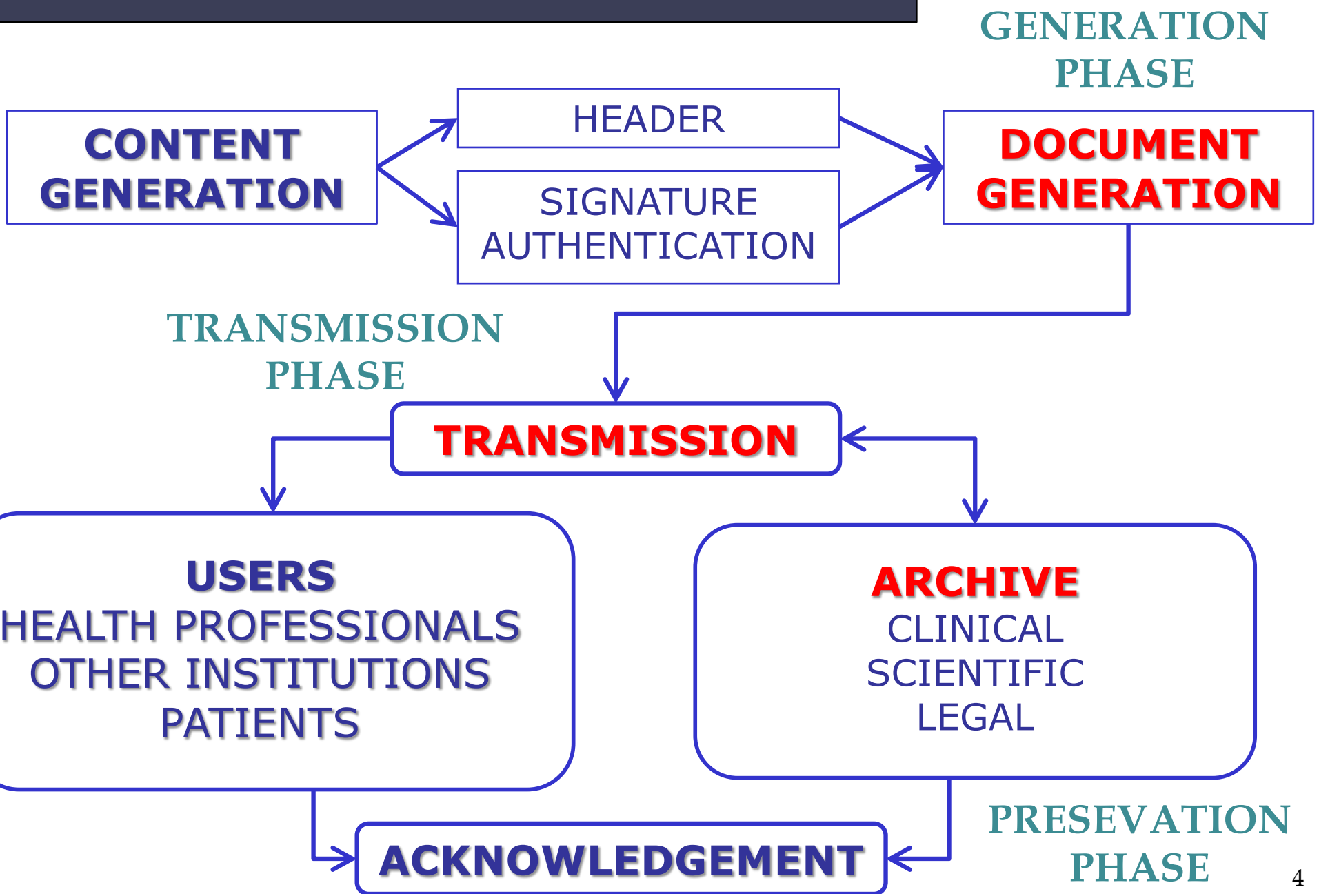
UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Shared care =

«A continuous and coordinated activity of **different persons in different institutions** under employment of different methods at different times in order to be able to help patients optimally with respect to their **medical, physiological, an social being**»

Data sharing and system integration is required to allow all the healthcare team to ensure **continuity of care.**

The medical document life cycle in shared care



Data protection

Security

- Safety: Preservation of data (data cannot be deleted, lost in a disaster)
- Quality: data integrity should be guaranteed

Privacy

- Unwanted access have to be avoided
- Management of access policies

PHYSICAL SAFETY: DATA BACKUP

POSSIBLE CAUSES

- Service interrupted (heartquakes, fire, energy, malware)
- Distruction (natural events)
- Theft (or delete)

BACKUP LEVELS

- Local backup (immediate, RAID, mirror disks)
- Remote backup with short recovery time (depends on the system and the network)
- Remote backup with long recovery time (>30 km, non continuous)

POSSIBLE DAMAGES

1. Integrity disruption → the document is totally or partially damaged
2. Data falsification → the document is changed/forged
3. Privacy violation → the document is read by someone who is not authorized
4. Knowledge theft → the document is copied by someone who is not authorized
5. Document loss → the document is lost/deleted

DATA FALSIFICATION

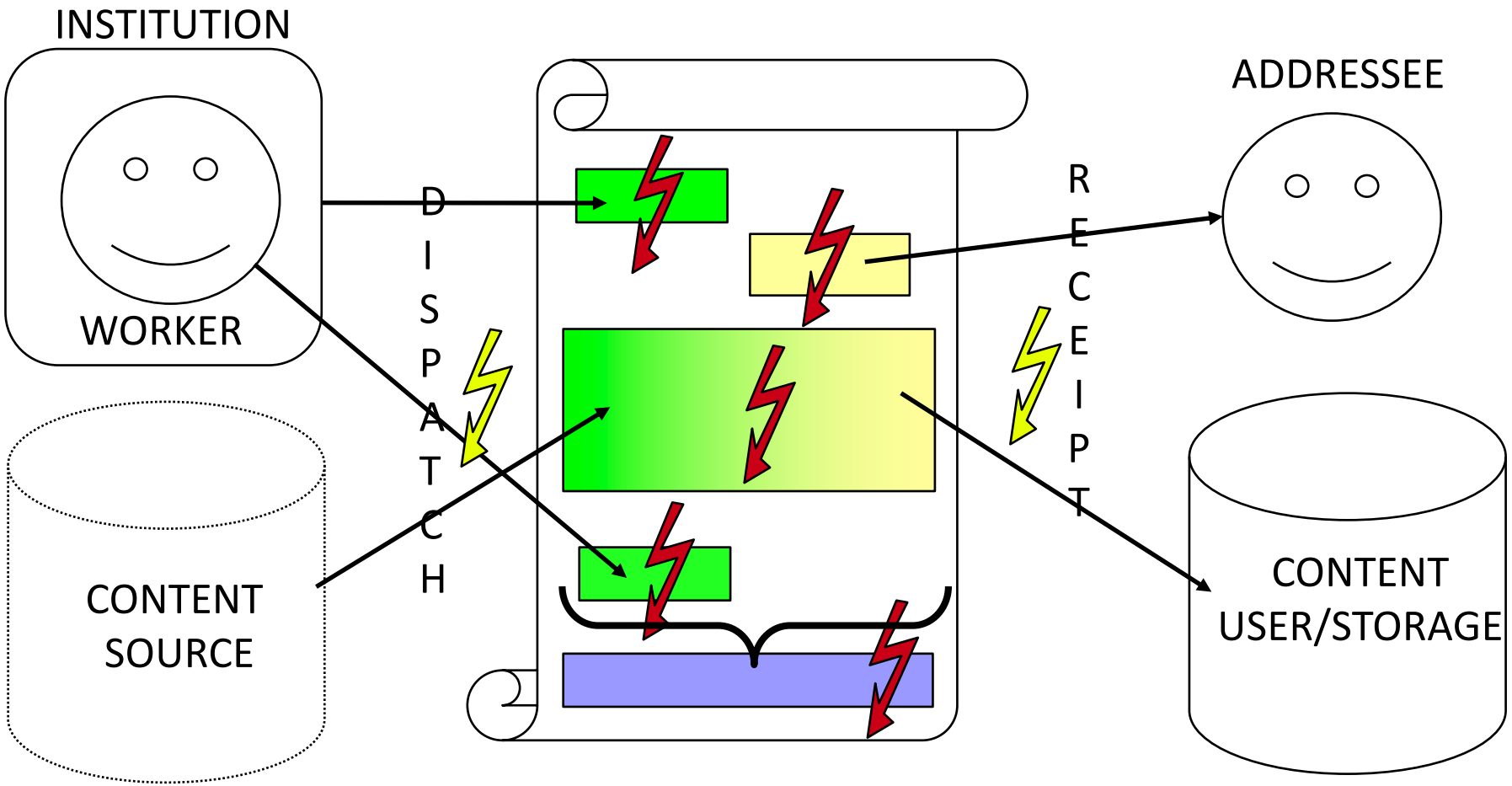
UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Documents can be changed with an impact on
  - Professional ethics
  - Coherence
  - Legal implications

- All documents parts can be counterfeit

- To detect forgery, each single document has to be verified.

FALSIFICAZION TYPES



FALSIFICATION EXAMPLES

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

HEADER:

- Ensures that the document has been issued by an Institution who takes the responsibility for its content
- The institution can be fake
- There are lists of accredited institutions to verify

ADDRESSEE

- Ensures that the docuement is received by whom was intended to
- Privacy concerns
- Difficult to verify

CONTENT

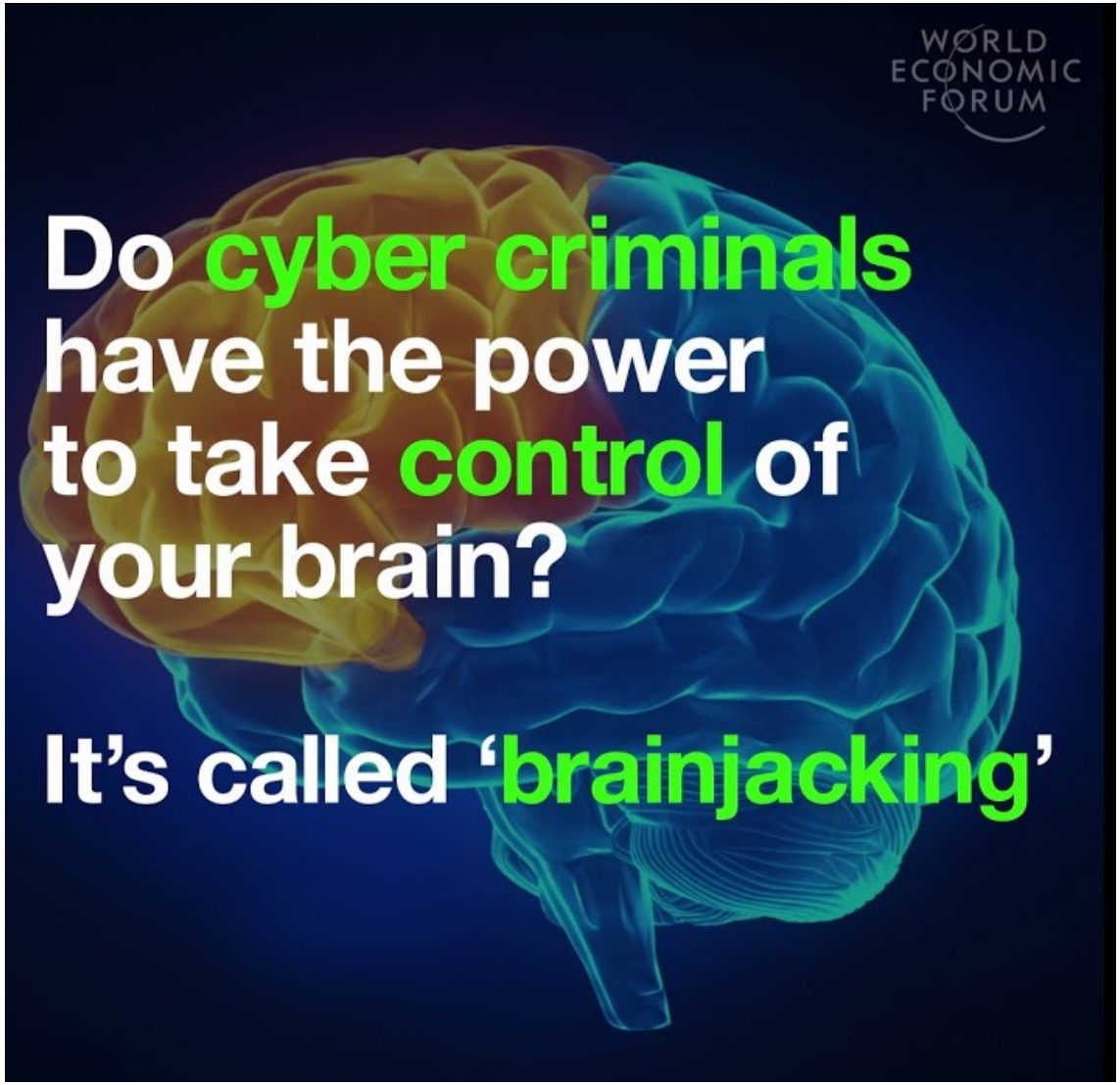
- Information delivered in the document
- Problem of data reliability

SIGNATURE/AUTHENTICATION

- Ensures that the document has signed by someone who takes the responsibility for its content
- The person signing can be not authorized to sign
- There are lists of accredited healthcare professionals to verify

OTHER RISKS

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

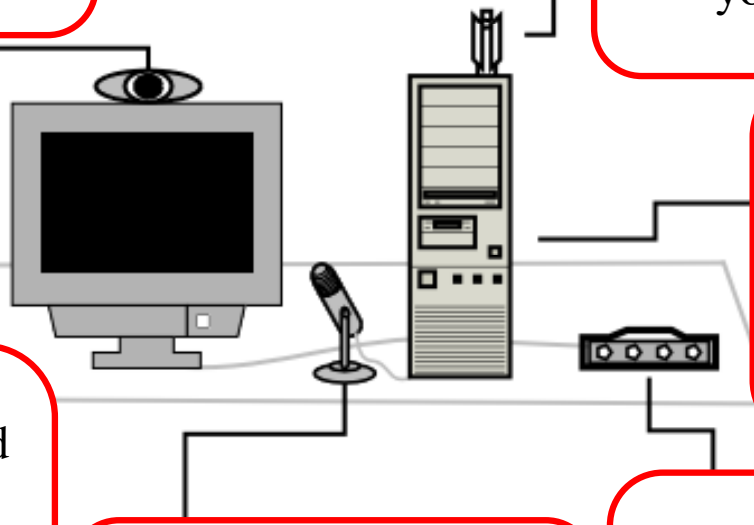


- Neuromodulation devices
- Pacemakers
- Implantable defibrillators

SOME SIMPLE ATTACK TOOLS

The computer webcam can be used remotely to capture personal images

WiFi networks can be used by others to enter your computer



Software virus and malware can be hidden in email messages

Spyware are used to detect passwords and other confidential information

The microphone can be remotely controlled and used to capture information

Internet is the major source of malware and spy programs

SIMPLE MALWARE TYPES (1)

1. VIRUS: data disruption

2. SPYWARE: collection of user's information that are then given to others

3. BACKDOOR: allow the unwanted access to the system or its remote control

4. AD HOC PROGRAMS: to access the system, forgery, knowledge theft, sabotage

SIMPLE MALWARE TYPES (2)

MALWARE TYPE	DAMAGE TYPE (1 to 5)				SPREADING (1 to 5)
	Integrity disruption	*Privacy violation*	*Knowledge theft*	*Falsification*	
VIRUS	4	2	2	1	5
SPYWARE	2	5	3	1	4
BACKDOOR	4	5	5	4	3
AD HOC PROGRAMS	5	5	5	5	1

DEFENSE STRATEGIES: BEST PRACTICES

- Preserve personal data
  - Only when necessary and using safe channels
- Be suspicious
  - Do not act when the identification of the object/person you are interacting with is not certain
- Defend the workstation
  - Firewall
  - Antivirus/Antimalware
  - Antispam
- Regular software update
  - Operative system/software update often fix security/privacy issues
- Verify attachments
  - They can include malware
- Choose the software
  - Better if open source

THE GENERAL SECURITY MODEL

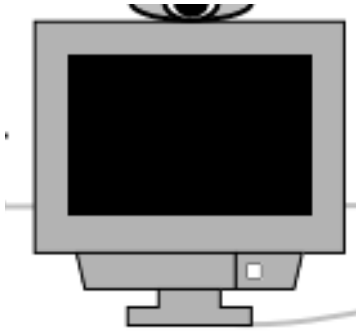
UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Working station

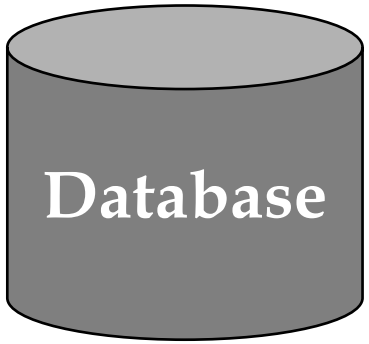
- Document generation
- Document request/use

Central domain

- Document Archiving
- Document Preservation



TRANSMISSION



APPLICATION SECURITY:
Authorization
Access Control
Availability
Integrity
Accountability
Confidentiality
Notary's function
Audit
Accuracy

COMMUNICATION SECURITY:
Identification
Authentication
Access Control
Integrity
Confidentiality
Notary's function
Availability
Accountability

APPLICATION SECURITY:
Authorization
Access Control
Availability
Integrity
Accountability
Confidentiality
Notary's function
Audit
Accuracy

Data protection: basic concepts

Authentication:

- Process of verifying the identity of an object/actor

Identification

- Autentication that defines univocally the identity of an object/actor

Authorization

- Process of allowing to use a specific object or accessing a specific information

Access control

- Process guaranteeing that the content of an object is known only to its creator or to whom is allowed to use it

Integrity

- Property of not being changed from its original form

Accountability

- Signature of who is responsible for the content of an object (cannot be denied)

Confidentiality

- The content of an object is known only to its creator or to whom is allowed to use it

Audit

- Process that guarantee that the security measures declared are properly set up and working

IMPLEMENTING A SECURE INFORMATION SYSTEM

STEP 1: Unambiguous authentication and identification

STEP 2: Guarantee the integrity of the communicated information

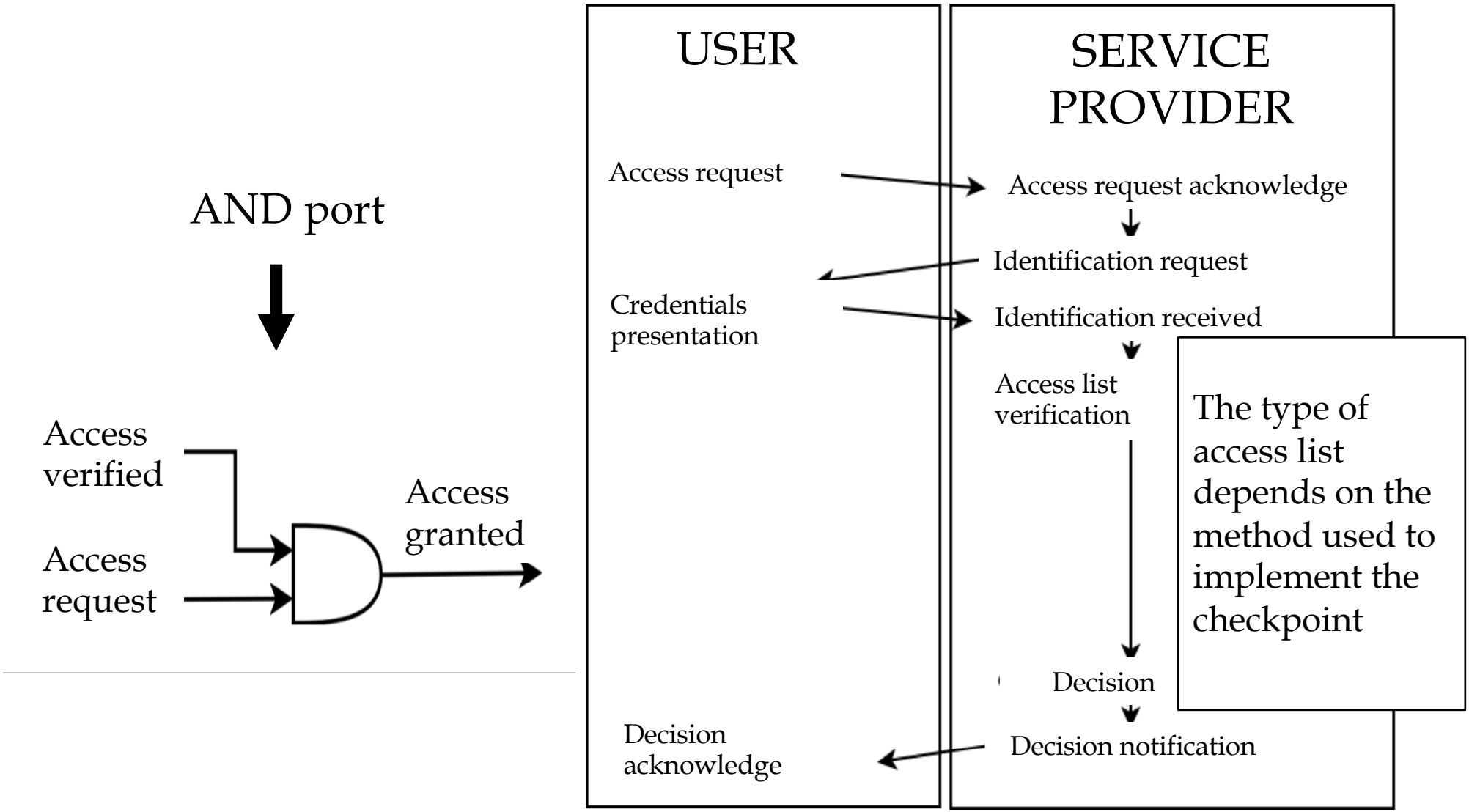
STEP 3: Ensuring the confidentiality of communicated, processed, and stored information

STEP 4: Guarantee the availability, accuracy, and reliability of the information

STEP 1: AUTHENTICATION AND IDENTIFICATION

- In the model of object-to-object communication identification and authentication are “communication services” and are pre-requisite for a secure information system
- Data access rights are at the application level (they must be defined for each specific object that is accessed)
- Authentication should be in general certified:
  - Non-repudiation of origin, receipt, and use of the communicated information
  - Detection of attackers

AUTHENTICATION AND IDENTIFICATION



EXAMPLE: THE FIREWALL

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Detection of unwanted connections from other network users or from applications running on the same computer
- Detection of dangerous web content by checking Java Applets and ActiveX controls to suggest whether or not running the application
- Port hiding → it hides the unused computer ports and monitors port scanning and access attempts
- Block of intrusions and of the attacks coming from the network

STEP 2: INTEGRITY OF THE COMMUNICATED INFORMATION

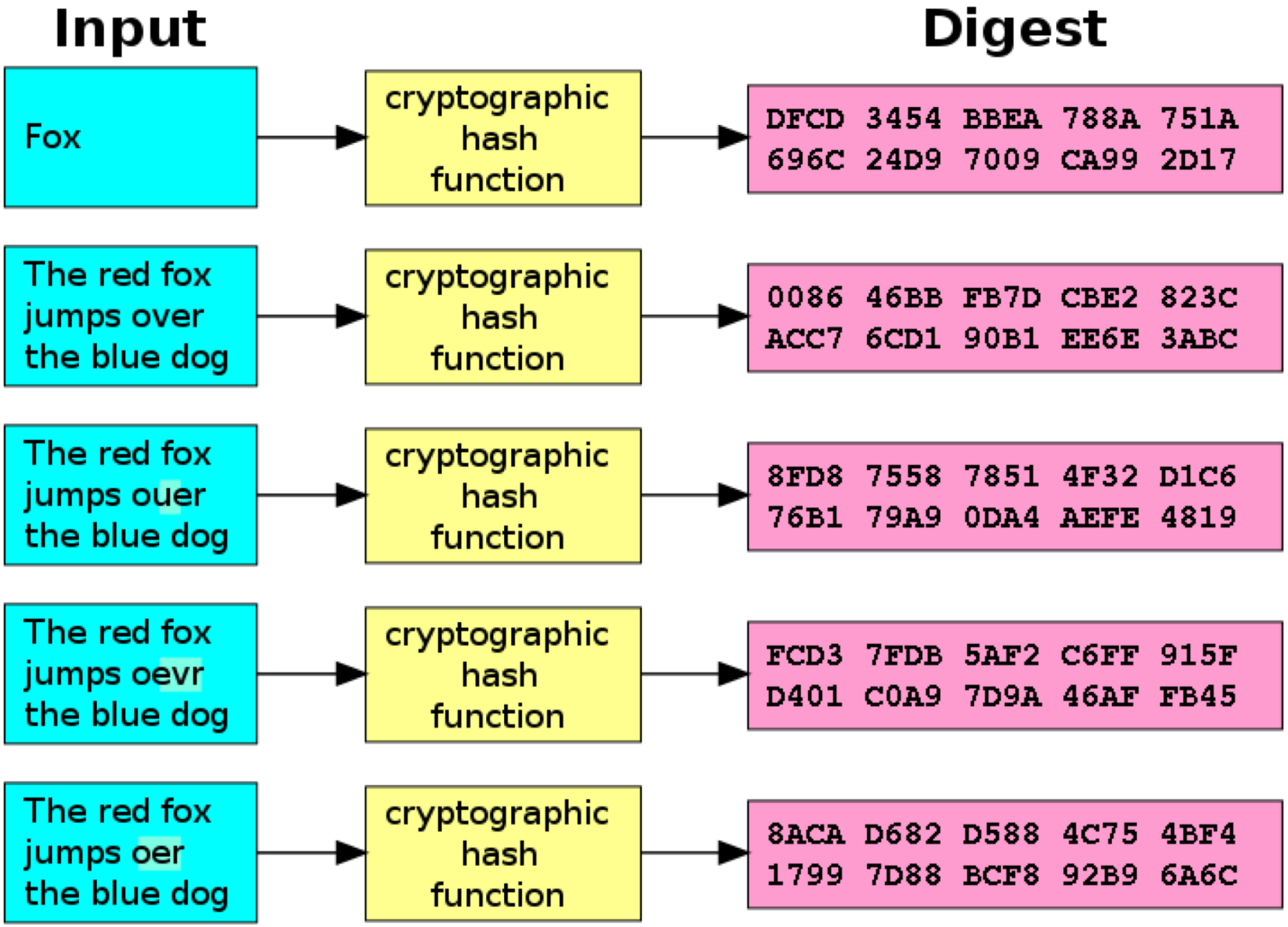
- Detection of any attacks to the communication infrastructure or the application systems
- To ensure document integrity it is possible to use HASH FUNCTIONS (implementing message DIGEST):
- **DIGEST →**
  - Short string of predefined length
  - Characterizes the document
  - Verify the integrity of the document itself
  - Calculated by the sender, sent to the receiver, calculated by the receiver and compared to the one that the receiver received → if the two match → the integrity of the document is preserved

HASH FUNCTIONS

- Message/Document digests are created through hash functions

- The ideal hash function **has four main properties**:
  - it is **easy to compute** the hash value for any given message
  - it is **infeasible to generate a message from its hash**
  - it is **infeasible to modify a message without changing the hash**
  - it is **infeasible to find two different messages with the same hash**.

MESSAGE DIGEST EXAMPLE



STEP 3: ENSURING CONFIDENTIALITY

CRYPTOGRAPHY is the practice and study of techniques for **secure communication** in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that prevent adversaries to understand the content of the message

CRYPTOGRAPHY HISTORY

The word *cryptography* comes from the Greek words *kryptos* meaning hidden and *graphein* meaning writing.
Cryptography is the study of hidden writing, or the science of encrypting and decrypting text.
Nineteenth century scholars decrypted ancient Egyptian hieroglyphics when Napoleon's soldiers found the Rosetta Stone in 1799 near Rosetta, Egypt. Its inscription praising King Ptolemy V was in three ancient languages: Demotic, hieroglyphics, and Greek. The scholars who could read ancient Greek, decrypted the other languages by translating the Greek and comparing the three inscriptions.

http://www.pawlan.com/monica/articles/crypto/

THE NAVAJO CODE TALKERS

The United States Marine Corps
Navajo Code Talkers
World War II

The Navajo Nation, when called upon to serve the United States, contributed a precious commodity never before used.
In the midst of the fighting in the South Pacific, a gallant group of young men from the Navajo Reservation utilized our language in coded form to help speed the allied victory.

Equipped with the only fool proof, unbreakable code in the history of warfare, the Navajo Code Talkers confused the enemy with an earful of sounds never before heard by code experts.

The dedication and devotion to duty shown by the men of the Navajo Nation in serving as radio code talkers
in the United States Marine Corps during World War II is an example for all Americans, the Navajo Nation and graduates of WRHS.

It is fitting that at this time we also express appreciation for the Navajo Code Talkers who lived among the communities of Fort Defiance, Old Sawmill, St. Michaels and the Window Rock areas, and the families
who served the population with their children being former students and alumni of Window Rock High School.

http://www.wrscouts.com/code_talkers.htm

Navajo Code Talkers' Dictionary

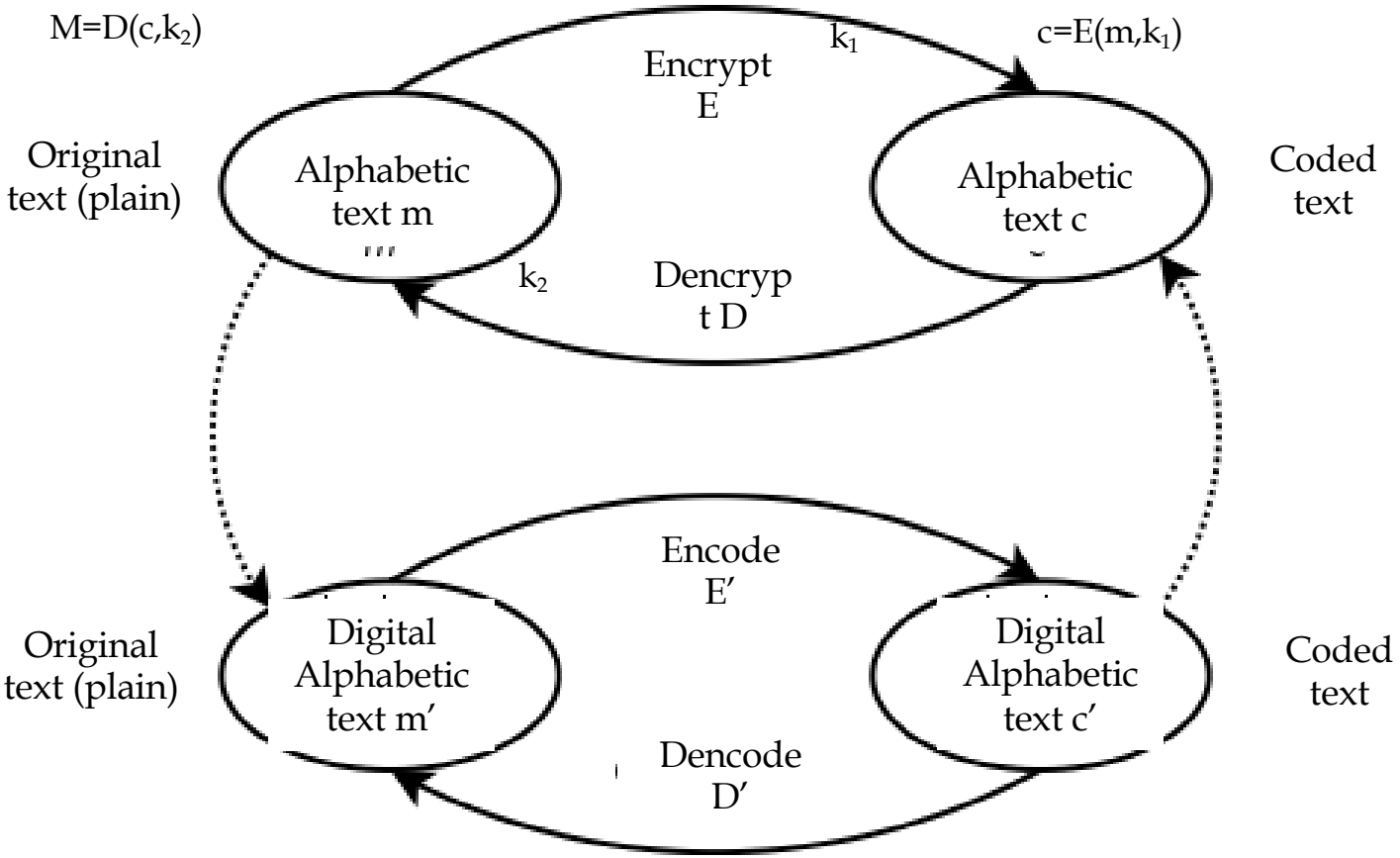
http://www.history.navy.mil/faqs/faq61-4.htm

CRYPTOGRAPHY ARCHITECTURE

UNIVERSITÀ DEGLI STUDI DI TRIESTE

ALGORITHM → Mathematical process or method that transforms a plain text into a non-readable text

KEY (k_i) → Information (usually alphanumeric) that is able to modify te behaviour of the cryptographyc algorithm.

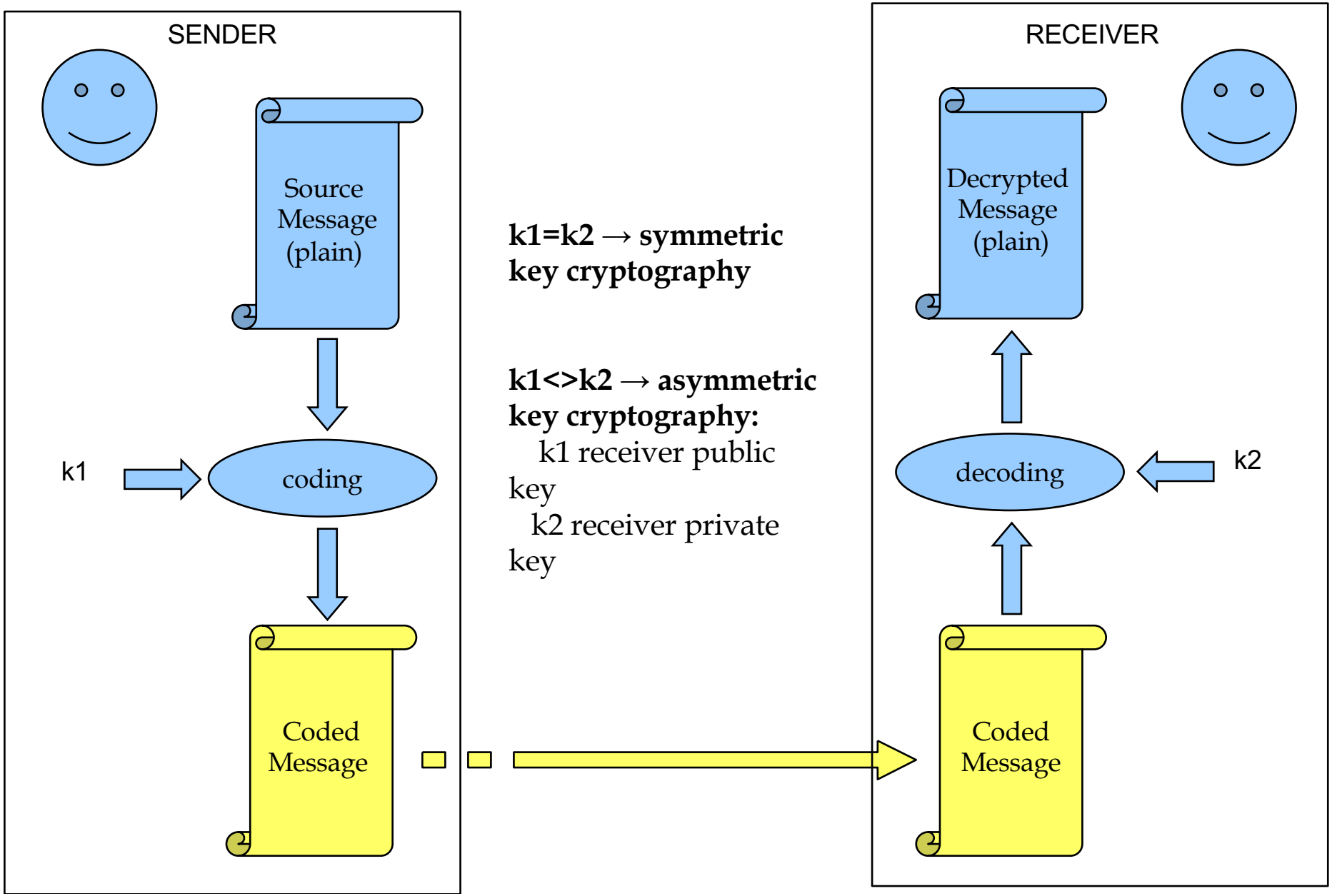


D e k_2 devono essere corretti rispetto ai corrispondenti E e k_1, per cui avremo M=m

KERCKHOFFS PRINCIPLE

- The security of a cryptosystem should depend solely on the secrecy of the key and the private randomizer.
- A method of secretly coding and transmitting information should be secure even if everyone knows how it works

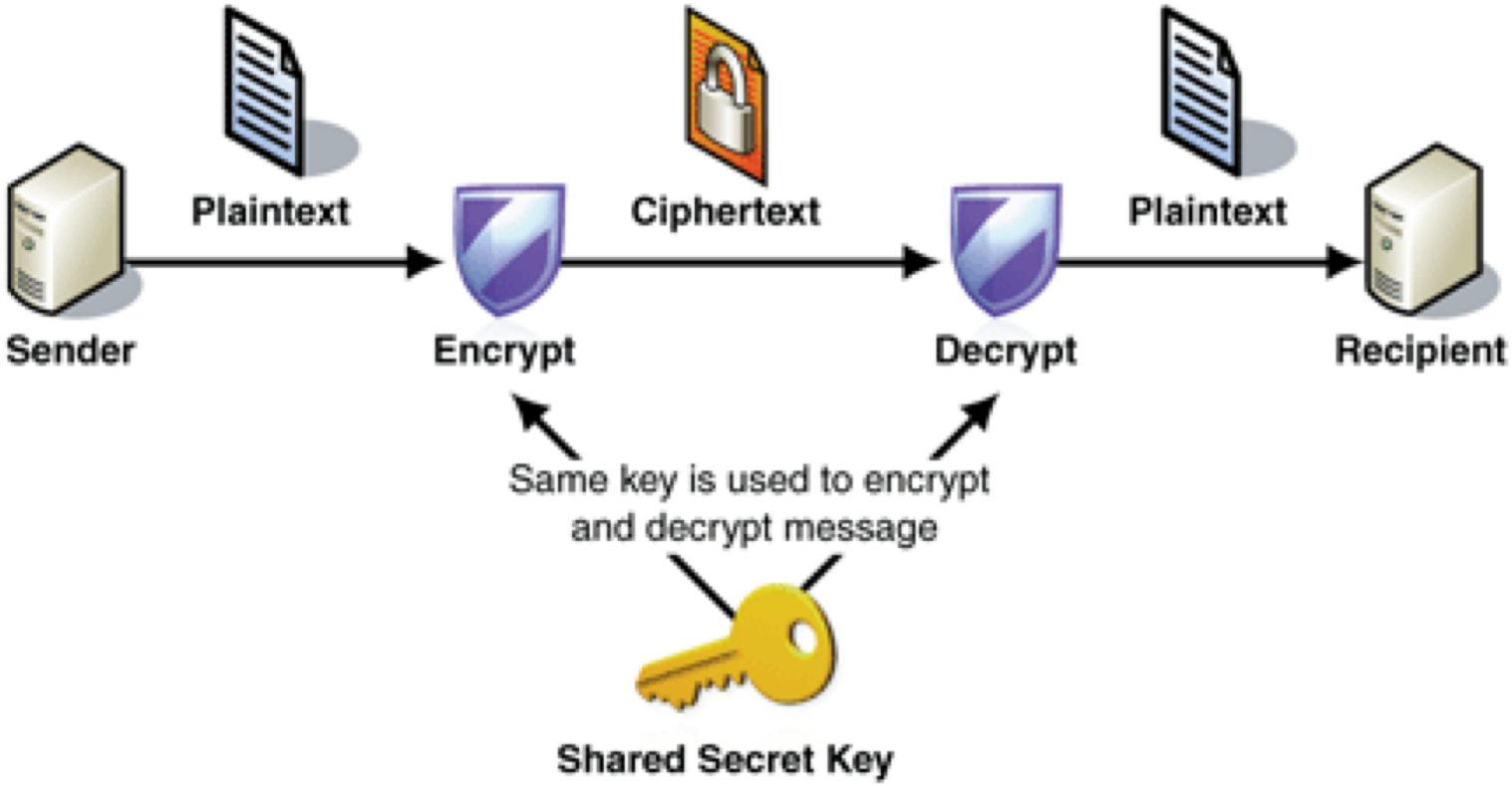
SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY



k1=k2 → symmetric key cryptography

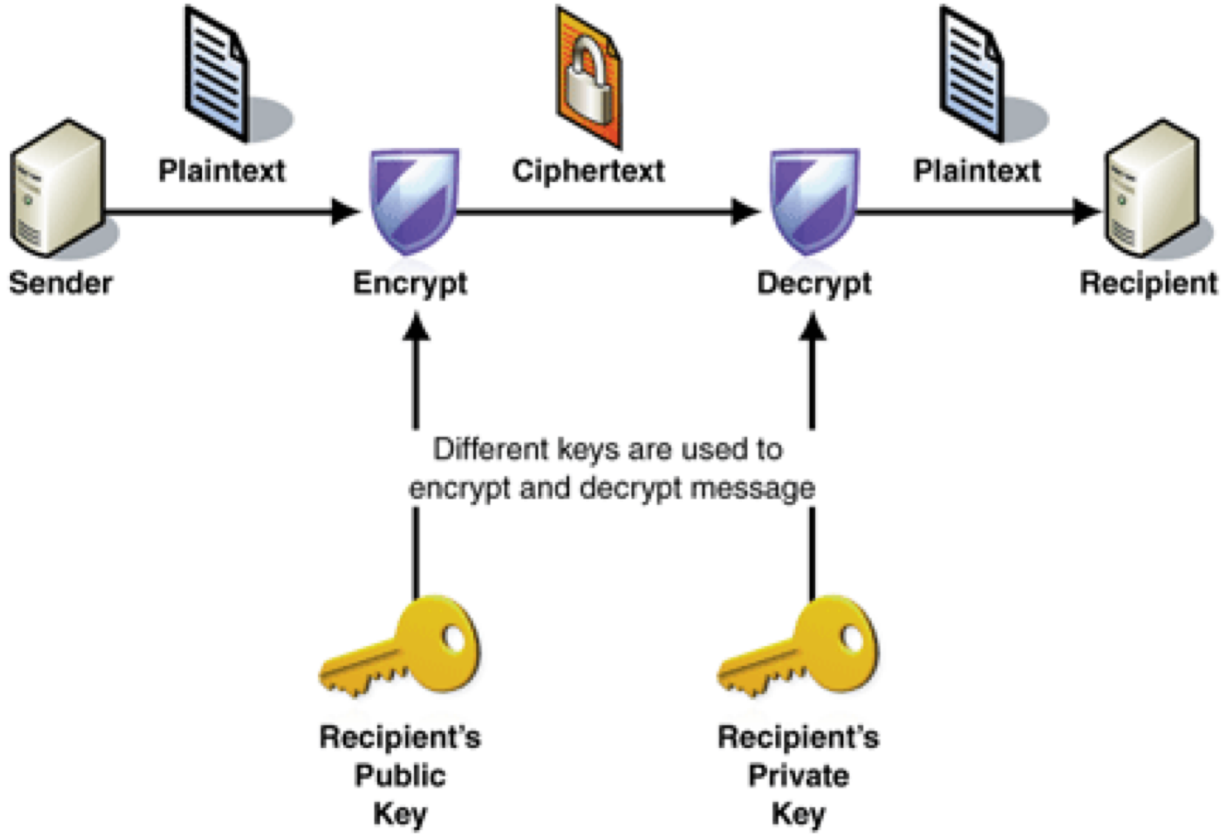
k1<>k2 → asymmetric key cryptography:
k1 receiver public key
k2 receiver private key

SYMMETRIC ENCRYPTION



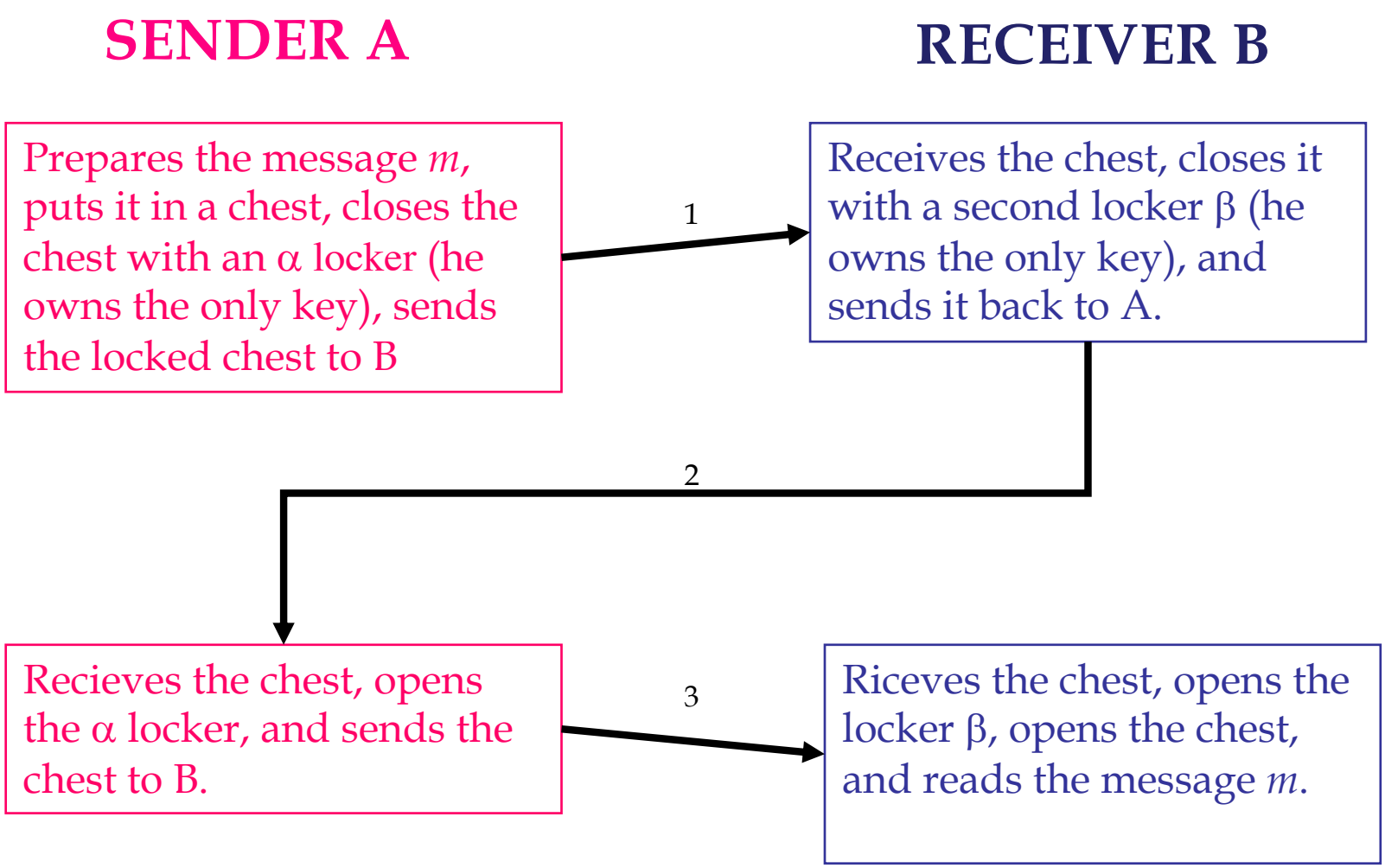
- The sender and the recipient have to share the key
- The key is used both to encrypt and to decrypt

ASYMMETRIC ENCRYPTION



- The public key of the recipient is used only to encrypt data (cannot decrypt). It can be openly distributed to those who want to encrypt a message to the recipient.
- The private key of the recipient is used to decrypt messages, and only the recipient must be able to access it.

ASYMMETRIC ALGORITHMS: THE TWO LOCKERS MECHANISM



KEY GENERATION: THE RSA SYSTEM

It is based on a factorization problem in prime numbers of a big number

1. Choose two distinct prime numbers p and q.
   - For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.
2. Compute $n = pq$.
   - n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
3. Compute $\phi(n) = \phi(p)\phi(q) = (p - 1)(q - 1) = n - (p + q - 1)$, where ϕ is Euler's totient function. This value is kept private.
4. Choose an integer e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$; i.e., e and $\phi(n)$ are coprime.
   - e is released as the public key exponent.
   - e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65,537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.[5]
5. Determine d as $d \equiv e^{-1} \pmod{\phi(n)}$; i.e., d is the modular multiplicative inverse of e (modulo $\phi(n)$).
   - This is more clearly stated as: solve for d given $d \cdot e \equiv 1 \pmod{\phi(n)}$
   - This is often computed using the extended Euclidean algorithm. Using the pseudocode in the *Modular integers* section, inputs a and n correspond to e and $\phi(n)$, respectively.
   - d is kept as the private key exponent.

The *public key* consists of the modulus n and the public (or encryption) exponent e. The *private key* consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\phi(n)$ must also be kept secret because they can be used to calculate d.

- An alternative, used by PKCS#1, is to choose d matching $de \equiv 1 \pmod{\lambda}$ with $\lambda = \text{lcm}(p - 1, q - 1)$, where lcm is the least common multiple. Using λ instead of $\phi(n)$ allows more choices for d. λ can also be defined using the Carmichael function, $\lambda(n)$.

The Advanced Encyption System (AES)

- AES is a block cipher with a block length of 128 bits.

- AES allows for three different key lengths: 128, 192, or 256 bits. Most of our discussion will assume that the key length is 128 bits.

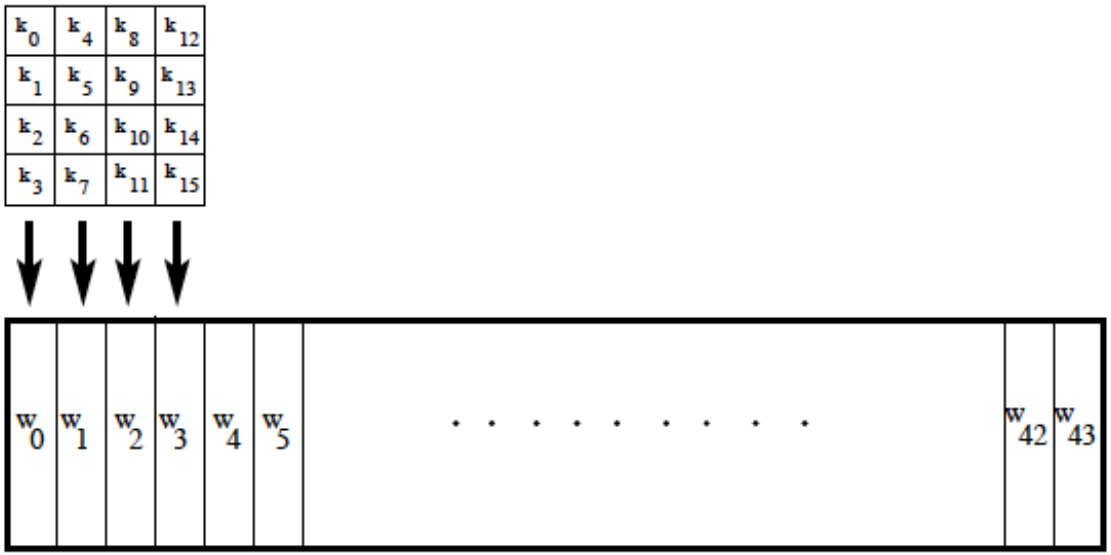
- Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

- Except for the last round in each case, all other rounds are identical.

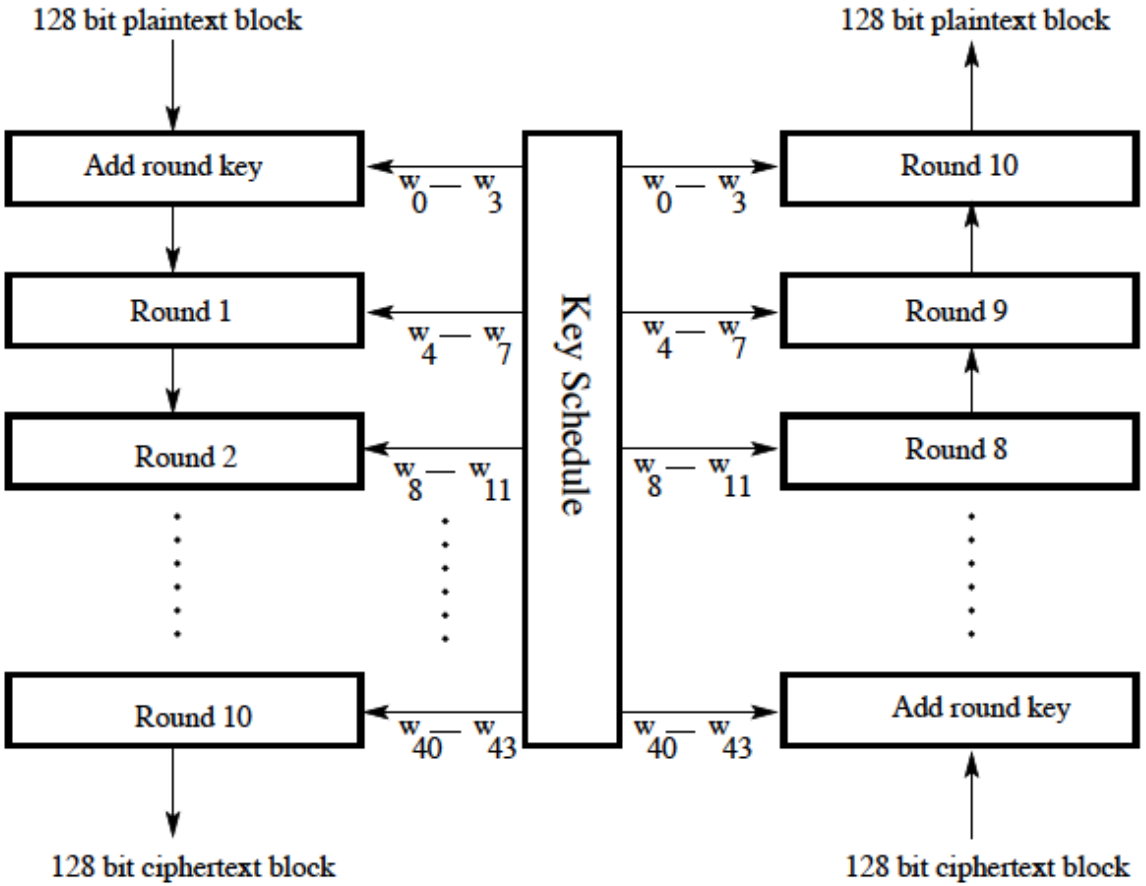
AES key

- Assuming a 128-bit key, the key is also arranged in the form of a matrix of 4×4 bytes. As with the input block, the first word from the key fills the first column of the matrix, and so on.

- The four column words of the key matrix are expanded into a schedule of 44 words. (As to how exactly this is done, we will explain that later in Section 8.8.) Each round consumes four words from the key schedule.

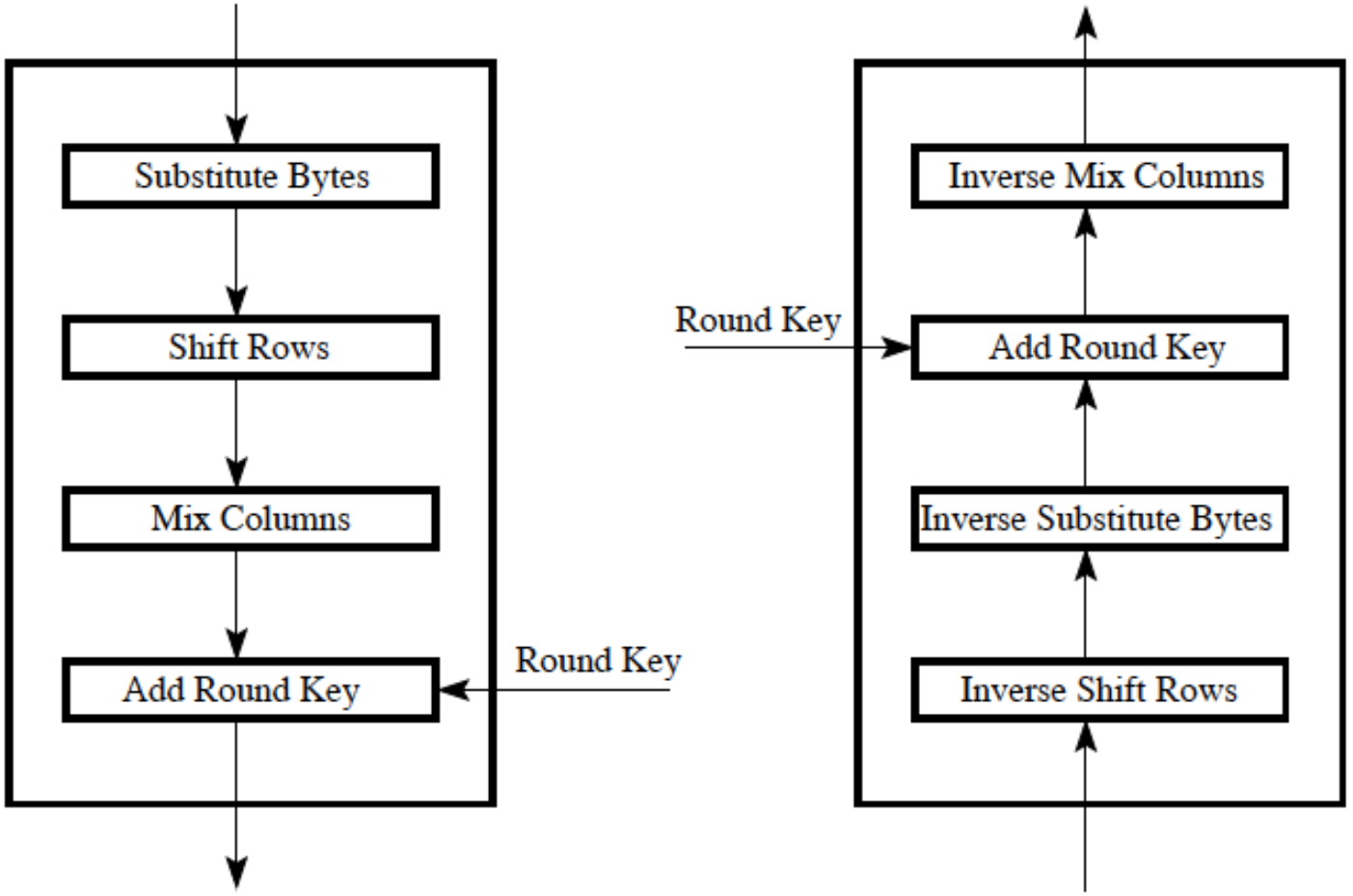


AES overall structure



AES Encryption AES Decryption

AES single round



THE FOUR STEPS

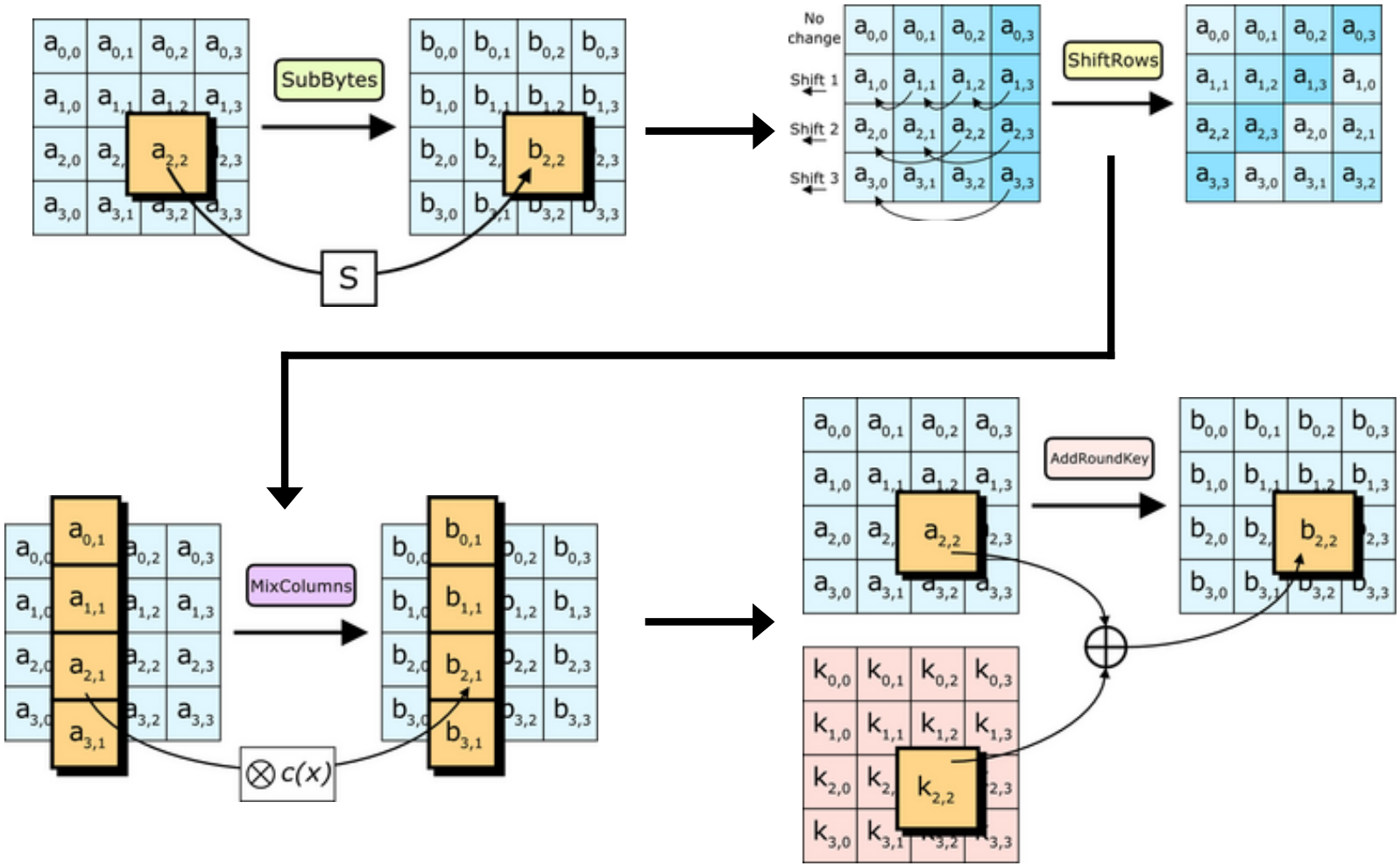
1. SubBytes — non linear substitution of all the bytes according to a specific table

2. ShiftRows — byte shifting of some positions on their row

3. MixColumns — Byte combination using a linear operation on columns.

4. AddRoundKey — each byte in the table is combined with the round key.

The 4 steps


SubBytes
S
No change
Shift 1
Shift 2
Shift 3
ShiftRows
MixColumns
⊗ c(x)
AddRoundKey

SYMMETRIC VS ASYMMETRIC CRYPTOGRAPHY

Algorithm	Advantages	Disvantages
Symmetric key	▪Easy to implement ▪Low computational requirements → speed execution	▪Need to share the key
Asymmetric key	▪Different keys for the sender and the receiver ▪Knowing the public key does not allow decrypting the message	▪More difficult to implements ▪High computational requirements → slow execution

Secure Socket Layer (SSL)

- The Secure Sockets Layer (SSL) is a computer networking protocol that manages server authentication, client authentication and encrypted communication between servers and clients.
- SSL uses a combination of public-key and symmetric-key encryption to secure a connection between two machines, typically a Web or mail server and a client machine, communicating over the Internet or an internal network.

How SSL works

- The SSL protocol includes two sub-protocols: the record protocol and the "handshake" protocol.
- These protocols allow a client to authenticate a server and establish an encrypted SSL connection: a server that supports SSL presents its digital certificate to the client to authenticate the server's identity.
- The authentication process uses public-key encryption to validate the digital certificate and confirm that a server is in fact the server it claims to be.
- Once the server has been authenticated, the client and server establish cipher settings and a shared key to encrypt the information they exchange during the remainder of the session.
- The handshake also allows the client to authenticate itself to the server. In this case, after server authentication is successfully completed, the client must present its certificate to the server to authenticate the client's identity before the encrypted SSL session can be established.

STEP 4: AVAILABILITY, ACCURACY, AND RELIABILITY

- It is not always possible to have a detailed pre-definition of individual access conditions

- A class-based or role-based access policy can ensure better availability, accuracy and reliability

- ROLE = set of functions/access privileges associated to a specific class

DEFINITION OF ROLES

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Current Users

System Id	Username	Given	Family Name	Roles
5-9	doctor	Jake	Smith	Organizational: Doctor
4-2	nurse	Jane	Smith	Organizational: Nurse
3-4	clerk	John	Smith	Organizational: Registration Clerk
6-7	sysadmin	Julie	Smith	Organizational: System Administrator

OpenMRS

Administration

Users

- Manage Users
- Manage Roles
- Manage Privileges
- Manage Alerts

Add/Edit User

Demographic Info

Given * Jane

Middle

Family Name * Smith

Gender* Male Female

Provider Account

Provider Identifier(s): nurse

Login Info

System Id 4-2

Username nurse *User can log in with either Username or Sys*

User's Password* ••••••••••••••• *Password should be 8 characters long and*

Confirm Password* ••••••••••••••• *Retype the password (for accuracy)*

Force Password Change *Optionally require that this user change their password on next lo*

Roles

Anonymous	Application: Administers System
Application: Configures Appointment Scheduling	Application: Configures Forms
Application: Configures Metadata	Application: Edits Existing Encounters
Application: Enters ADT Events	Application: Enters Vitals
	Application: Has Super User Privileges

DEFINITION OF ROLES

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Role* Organizational: Nurse

Description Nurse

Inherited Roles

Organizational: Nurse inherits privileges from these roles

- [ ] Application: Administers System
- [ ] Application: Configures Appointment Scheduling
- [ ] Application: Configures Forms
- [ ] Application: Configures Metadata
- [ ] Application: Edits Existing Encounters
- [x] Application: Enters ADT Events
- [x] Application: Enters Vitals
- [ ] Application: Has Super User Privileges
- [ ] Application: Manages Atlas
- [ ] Application: Manages Provider Schedules
- [x] Application: Records Allergies
- [ ] Application: Registers Patients
- [x] Application: Requests Appointments
- [ ] Application: Schedules And Overbooks Appointments
- [ ] Application: Schedules Appointments
- [x] Application: Sees Appointment Schedule
- [x] Application: Uses Capture Vitals App
- [x] Application: Uses Patient Summary
- [ ] Application: Writes Clinical Notes
- [ ] Organizational: Doctor
- [ ] Organizational: Hospital Administrator
- [ ] Organizational: Registration Clerk
- [ ] Organizational: System Administrator
- [ ] Privilege Level: Full
- [ ] Privilege Level: High
- [ ] Provider
- [ ] System Developer

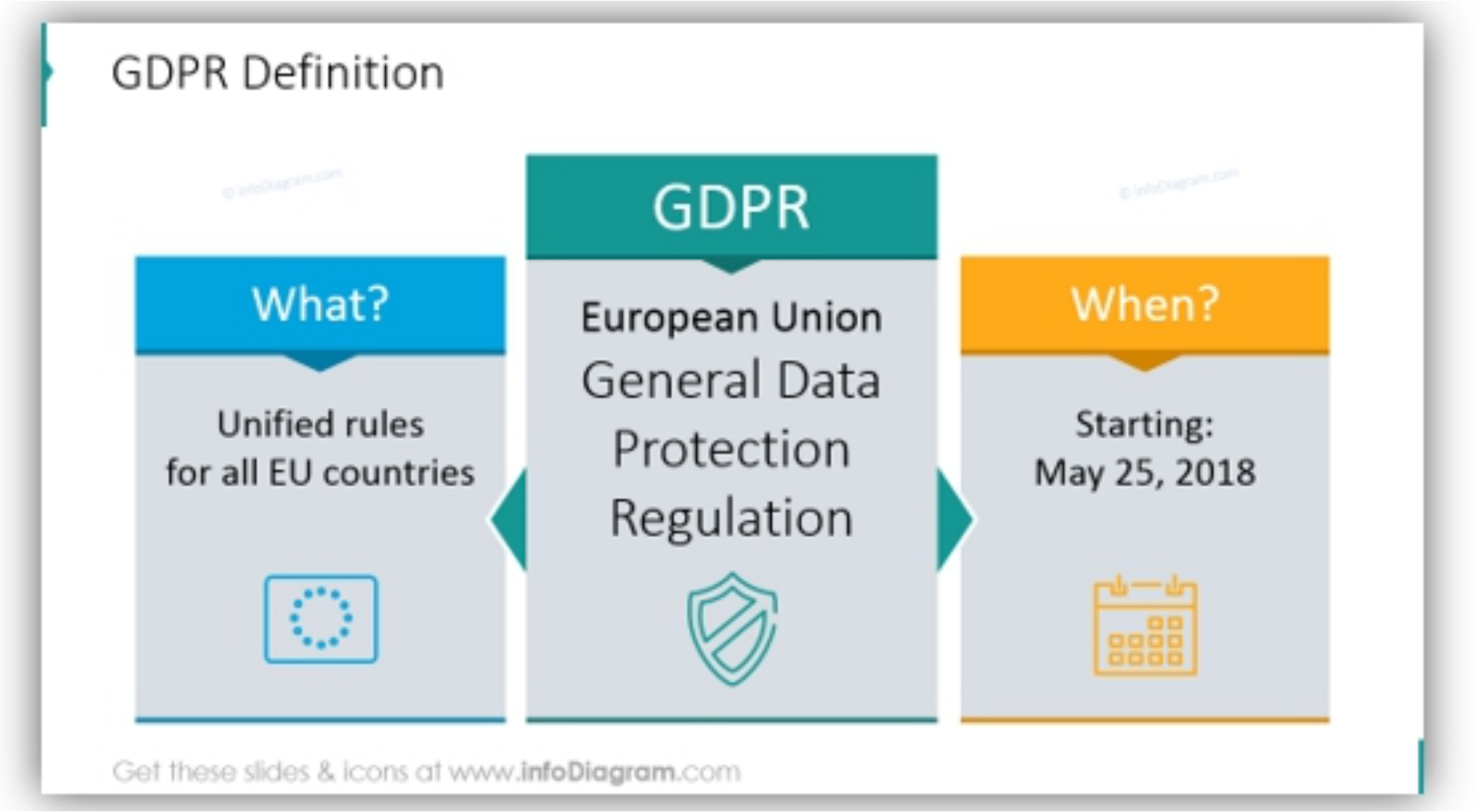
Privileges

Greyed out checkboxes represent privileges inherited from other role

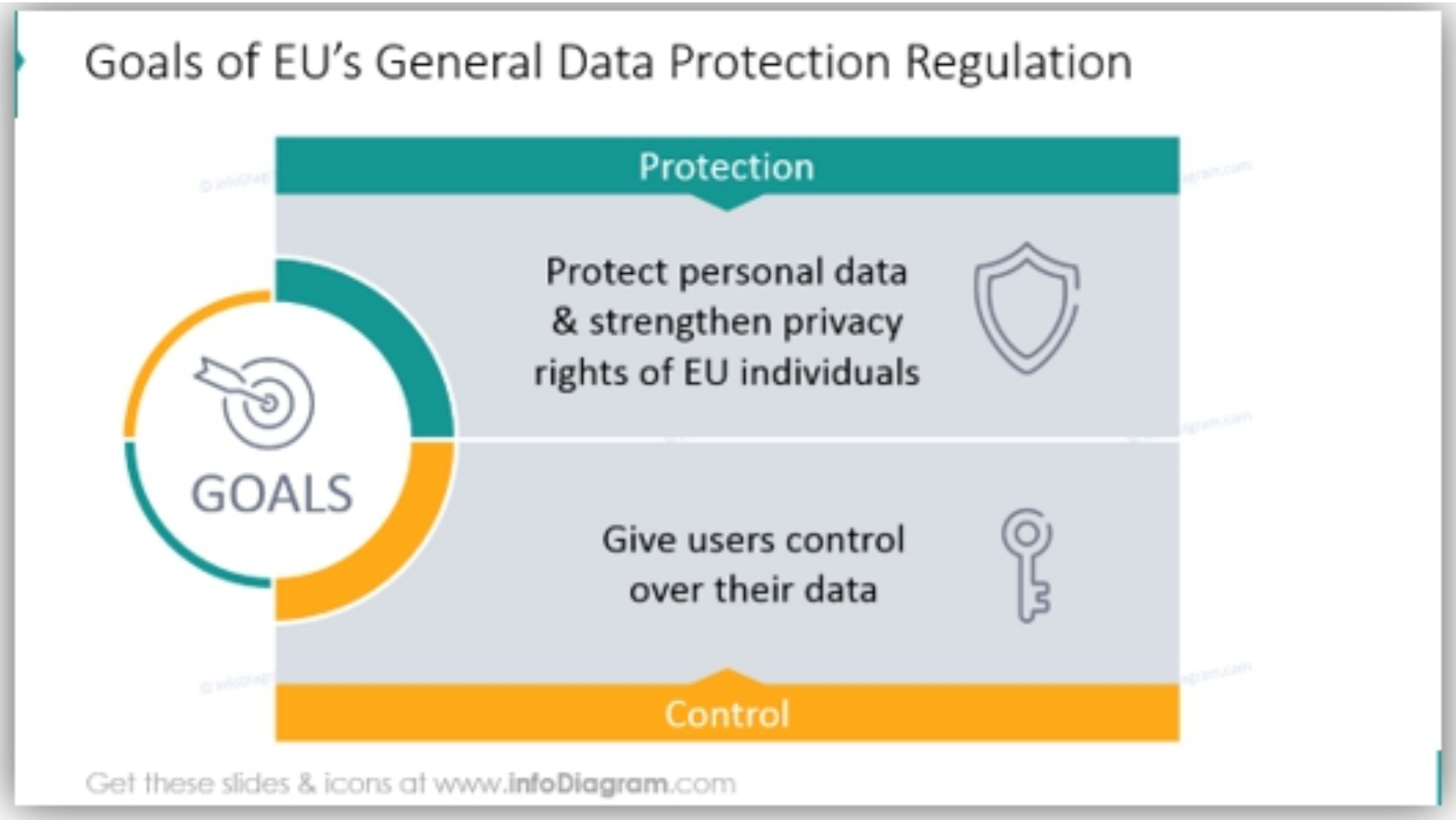
- [ ] Select/Unselect All
- [x] Add Allergies
- [x] Add Cohorts
- [x] Add Concept Proposals
- [x] Add Encounters
- [x] Add HL7 Inbound Archive
- [x] Add HL7 Inbound Exception
- [x] Add HL7 Inbound Queue
- [x] Add HL7 Source
- [x] Add Observations
- [x] Add Orders
- [x] Add Patient Identifiers
- [x] Add Patient Programs
- [x] Add Patients
- [x] Add People
- [x] Add Problems
- [x] Add Relationships
- [ ] Add Report Objects
- [ ] Add Reports
- [x] Add Users
- [x] Add Visits
- [ ] App: adminui.configuremetadata
- [ ] App: appointmentschedulingui.appointme
- [x] App: appointmentschedulingui.home
- [ ] App: appointmentschedulingui.providerSc
- [x] App: appointmentschedulingui.viewA
- [ ] App: atlas.manage
- [ ] App: attachments.attachments.page
- [x] App: coreapps.activeVisits
- [ ] App: coreapps.configuremetadata
- [ ] App: coreapps.dataManagement
- [x] App: coreapps.findPatient
- [ ] App: coreapps.mergePatient
- [x] App: coreapps.patientDashboard
- [x] App: coreapps.patientVisits
- [ ] App: coreapps.summaryDashboard
- [ ] App: coreapps.systemAdministration
- [ ] App: formentryapp.forms

GENERAL DATA PROTECTION REGULATION (GDPR)

UNIVERSITÀ
DEGLI STUDI DI TRIESTE



GDPR: GOALS


Goals of EU's General Data Protection Regulation
Protection
Protect personal data & strengthen privacy rights of EU individuals
GOALS
Give users control over their data
Control
Get these slides & icons at www.infoDiagram.com

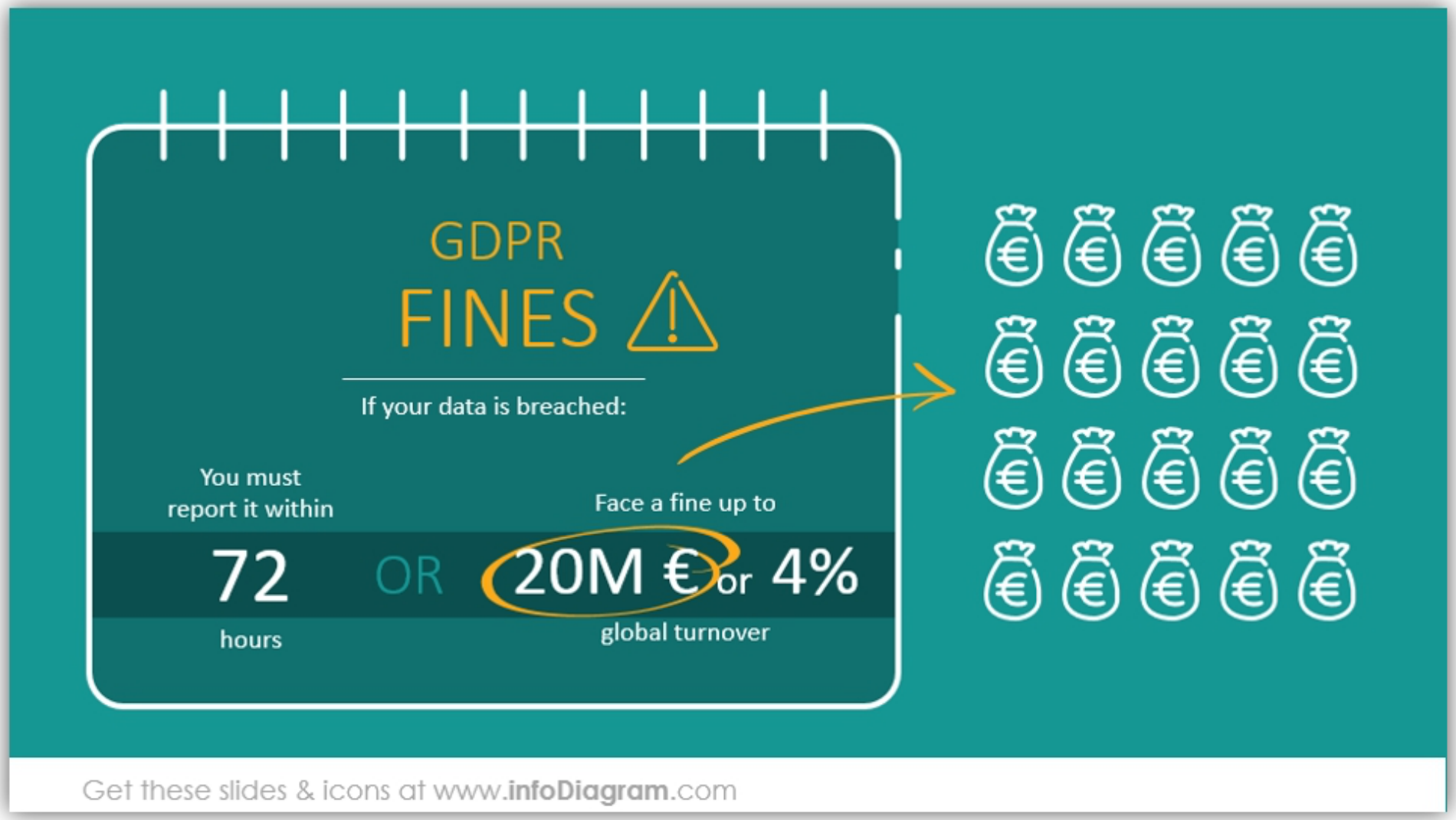
GDPR: PERSONAL DATA AND PROCESSING

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Processing: operations performed on personal data, including by manual or automated means. It includes the **collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination** or otherwise making available, **alignment or combination, restriction, erasure or destruction** of personal data.

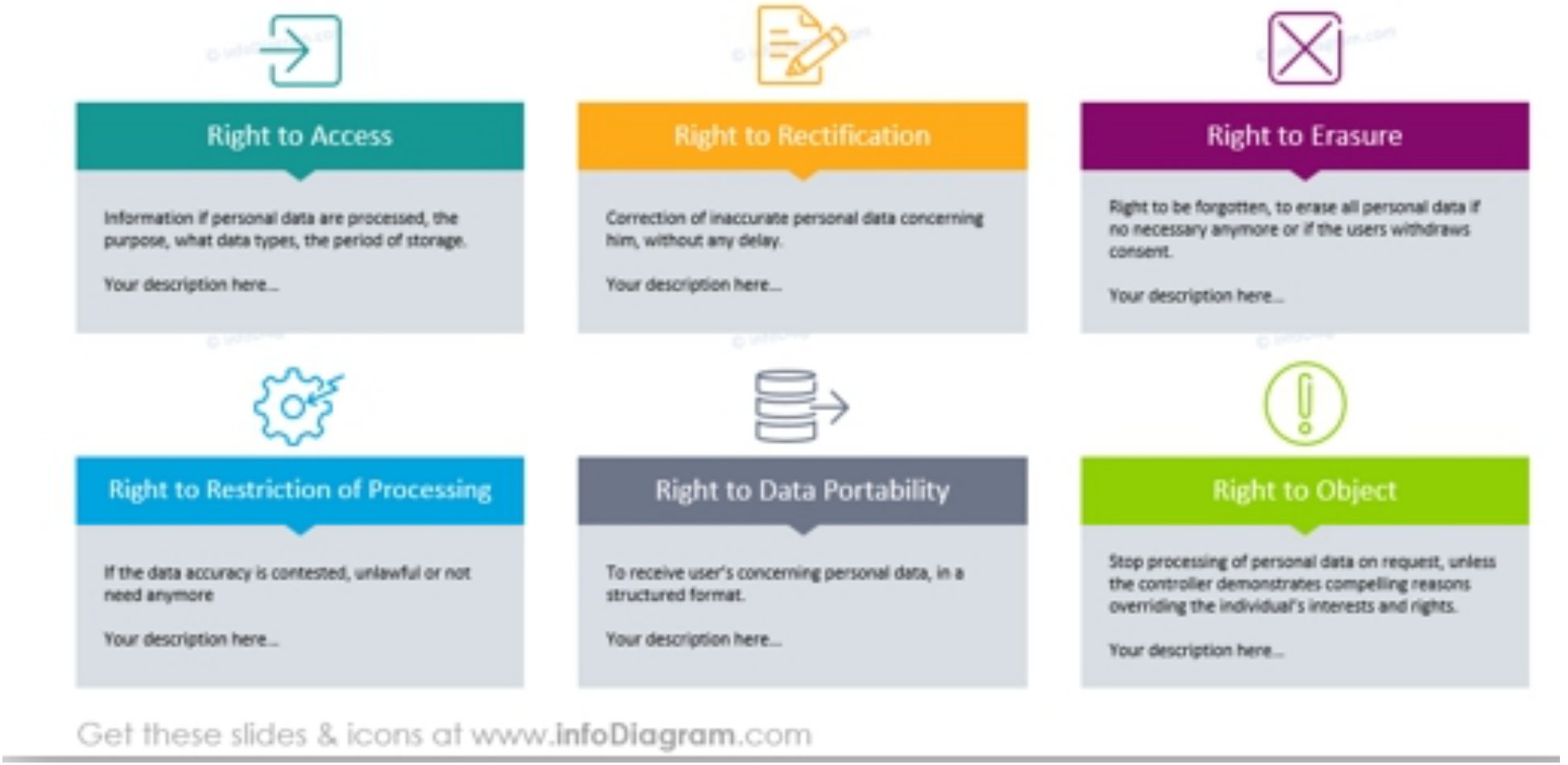
GDPR: FINES

UNIVERSITÀ
DEGLI STUDI DI TRIESTE



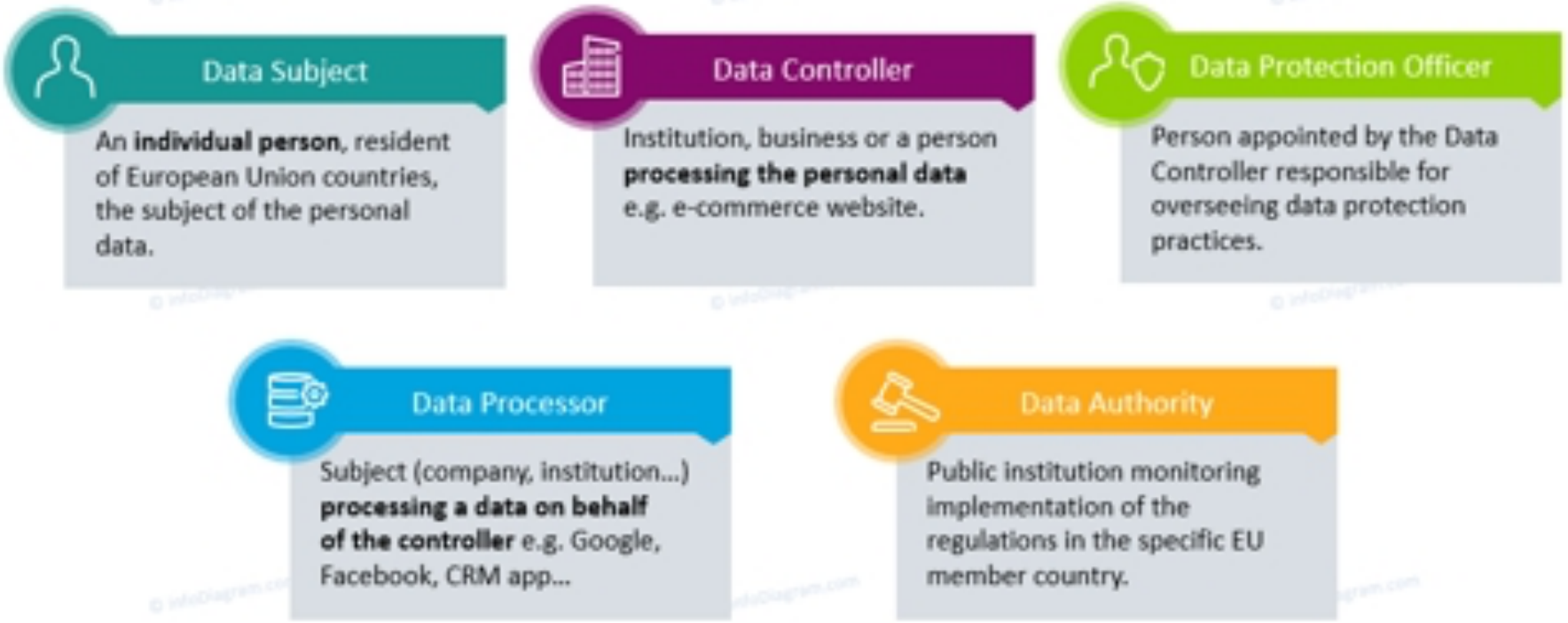
GDPR: INDIVIDUAL RIGHTS

UNIVERSITÀ
DEGLI STUDI DI TRIESTE



GDPR SUBJECTS

UNIVERSITÀ
DEGLI STUDI DI TRIESTE



GDPR SUBJECTS