# INTRODUCTION TO SECURITY

# HOW AM I

**Santiago Figueroa Lorenzo:**

- Senior Industrial Cybersecurity Engineer at Siemens Gamesa
- PhD at University of Navarra
- Lecturer at University of Navarra (UNAV)
- Lecturer at Inkorformación
- Web page: sfl0r3nz05.github.io
- LinkedIn: sfl0r3nz05

# LECTURE CONTENT

- Students' presentation (Turn on the camera during it)
- Lecture overview
- Lecture resources
- Quick introduction
- Network security definition
- Important definitions
- Why cryptography
- Goals of the cryptography

# LECTURE OVERVIEW

- Lecture:
  - Theory
  - Practice
- Test exam
- Ordinary evaluation
- Extraordinary evaluation

| No. | Date | Category | Theory | Practice |
|---|---|---|---|---|
| 1 | 01/04/2025 | Crypto | Intro personal, security, lecture<br>CyberSec pillars definitions<br>Crypto history | |
| 2 | 02/04/2025 | | Symetric Encryption | Lab: Python AES |
| 3 | 03/04/2025 | | Message Integrity<br>Autenticated encryption | Lab: Python hashing<br>Lab: Docker images hash |
| | 04/04/2025 | | | |
| | 05/04/2025 | | | |
| | 06/04/2025 | | | |
| 4 | 07/04/2025 | | Public Key Encryption | Lab: OpenSSL |
| 5 | 08/04/2025 | | Public Key Encryption | Lab: Signing docker images on github |
| 6 | 09/04/2025 | | Key derivation<br>Key exhange | Lab: Python Diffie Hellman |
| 7 | 10/04/2025 | | Digital Certificates<br>PgP, GPG o CryptoLoop<br>Law 59/2003<br>Digital Signature | Lab: secure git commits with openPGP<br>Lab: Kali sslscan<br>Test exam for crypto |
| | 11/04/2025 | | | |
| | 12/04/2025 | | | |
| | 13/04/2025 | | | |
| 8 | 14/04/2025 | PKI | Identification of PKI components<br>Certified Authority and Elements<br>Self signed certificates | Lab: Self signed certificates based on OpenSSL |
| 9 | 15/04/2025 | | Attribute certificate fields, including description of their common uses and relationship with digital certificates.<br>Certificate Policy and Certification Practice Statement (CPS). | Lab: Knowing Let's encrypt |
| 10 | 16/04/2025 | | Certificate Revocation List (CRL) | |
| | 17/04/2025 | | | |
| | 18/04/2025 | | | |
| | 19/04/2025 | | | |
| | 20/04/2025 | | | |
| | 21/04/2025 | | | |
| 11 | 22/04/2025 | | Certificate Signing Request (CSR) operation<br>Privilege Management Infrastructure (PMI) | Lab: PKI standalone based on Windows 2019<br>Test exam for pki |
| 12 | 23/04/2025 | | Identity and Access Management Systems | |
| 13 | 24/04/2025 | | | Lab: Configure and IAM system using Keycloak |
| | 25/04/2025 | Secure communications | | |
| | 26/04/2025 | | | |
| | 27/04/2025 | | | |
| 14 | 28/04/2025 | | Web Security Model<br>Web Attack<br>Web Defense | Lab: Use have I been pwned?<br>Lab: Secure password using bycrypt JS |
| 15 | 29/04/2025 | | HTTPS Goals and pitfalls | Lab: Hacking introduction based on Juice shop and Kali Lin |
| 16 | 30/04/2025 | | SSH<br>SSL | Lab: Securing a SSH Server |
| | 01/05/2025 | | | |
| | 02/05/2025 | | | |
| | 03/05/2025 | | | |
| | 04/05/2025 | | | |
| 17 | 05/04/2025 | | SSL VPN<br>IPSEC VPN | Lab: SSL VPN<br>Lab: Intro to packet Tracer |
| 18 | 06/05/2025 | | IPSEC VPN<br>Cipher tunneling | Lab: Packet Tracer IPSec VPN<br>Test exam for secure comm |
| | 07/05/2025 | | | |
| | 08/05/2025 | | | |
| | 09/05/2025 | | | |
| 19 | 10/05/2025 | | Final exam | |
| | 11/05/2025 | | | |
| 20 | 12/05/2025 | | Retake final exam | |

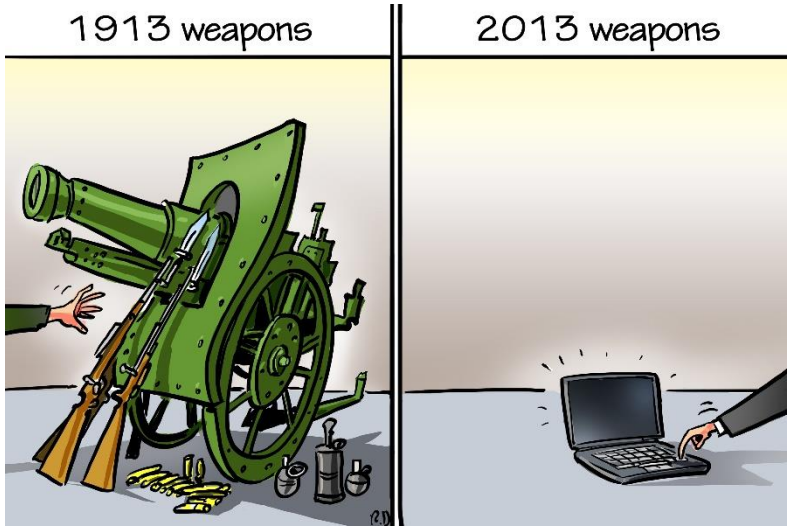
# LECTURE RESOURCES

- Linux VM:
  - Python
  - OpenSSL
  - OpenSSH
  - Git
  - OpenPGP
  - Docker containers
- GitHub account
- Packet Tracer Software

# Preconceived ideas about the Internet

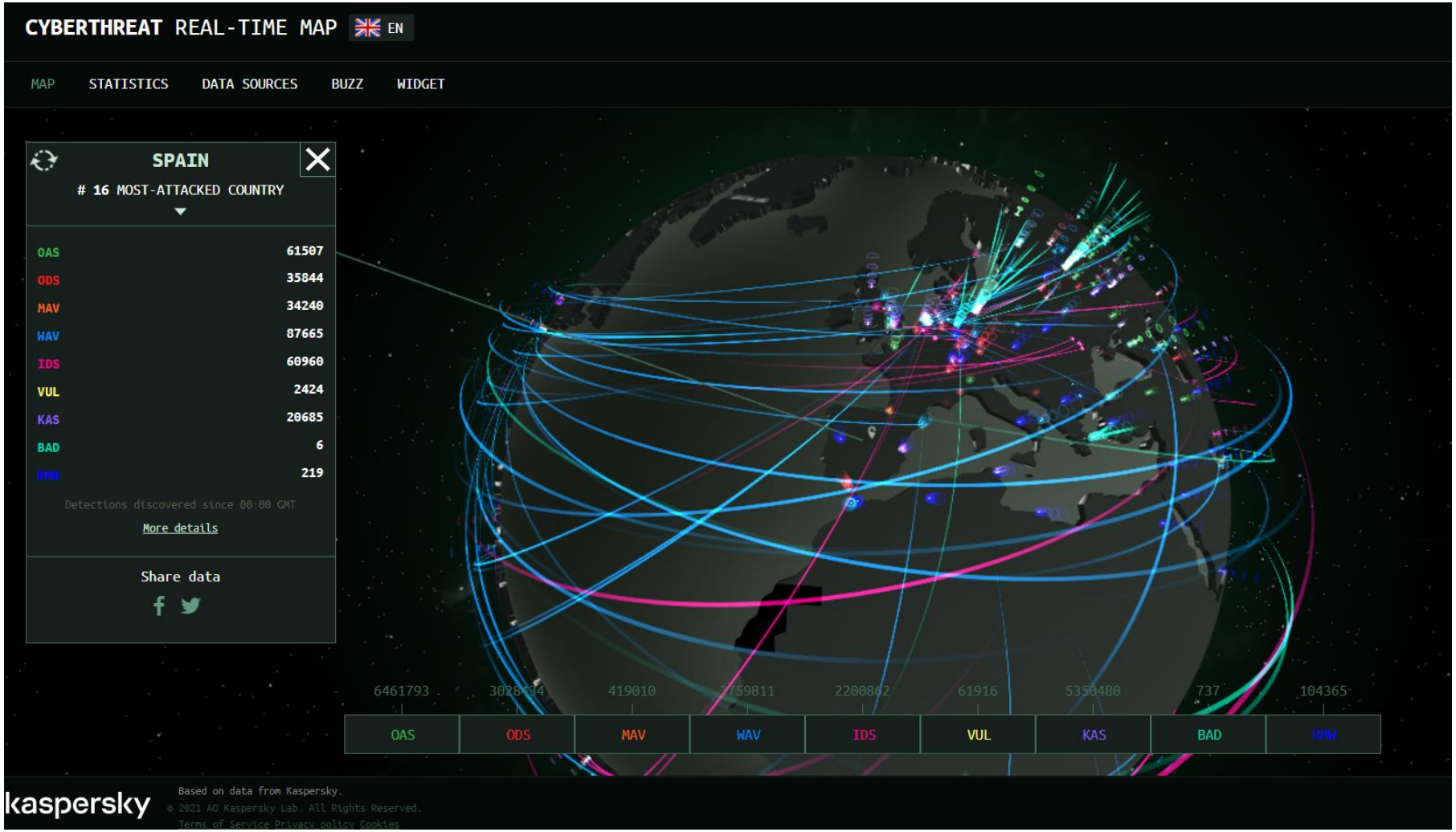
- “Network created by and for gentlemen”.

- “Functionality” is the priority.
- A hacker is a criminal.

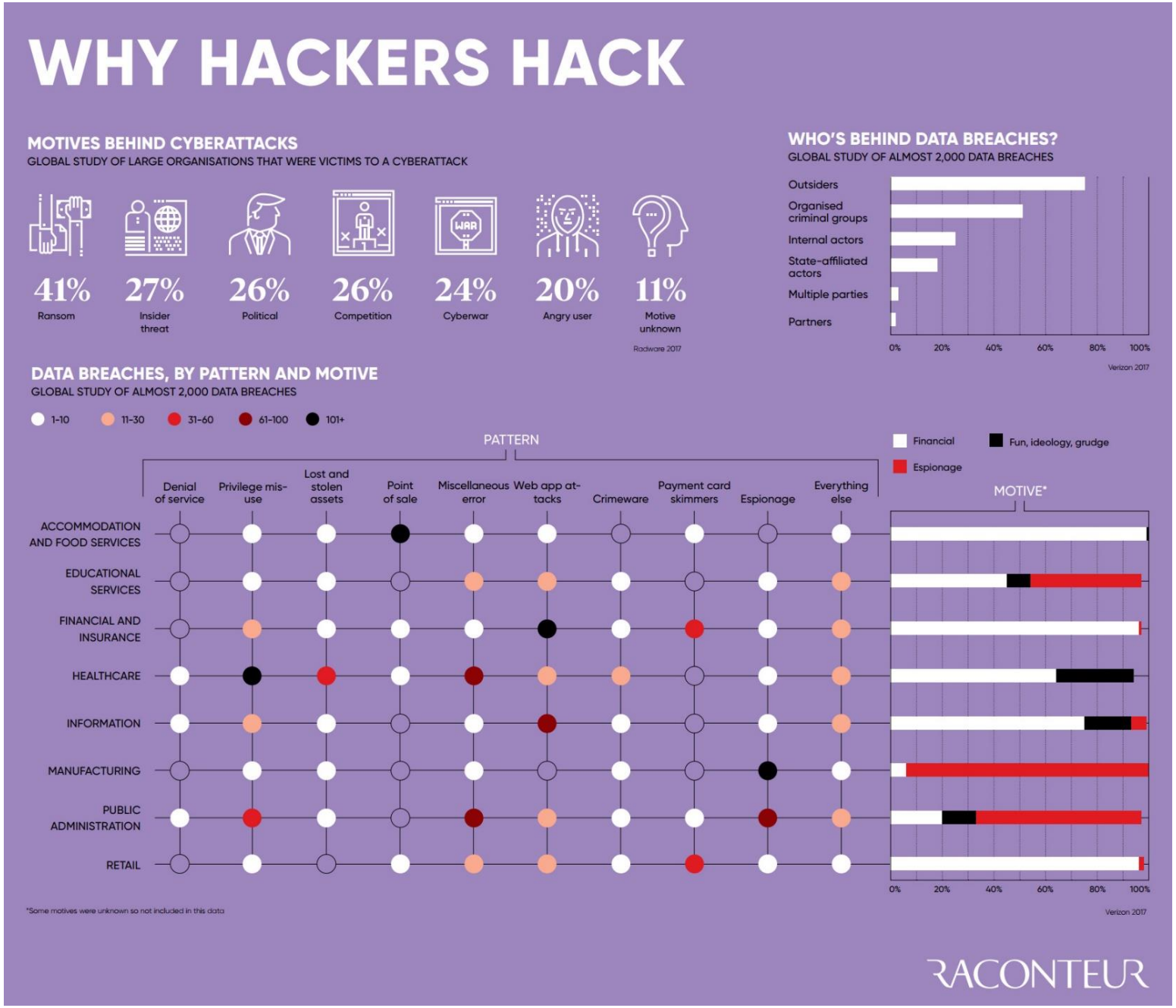


# THE REAL WORLD

https://cybermap.kaspersky.com/



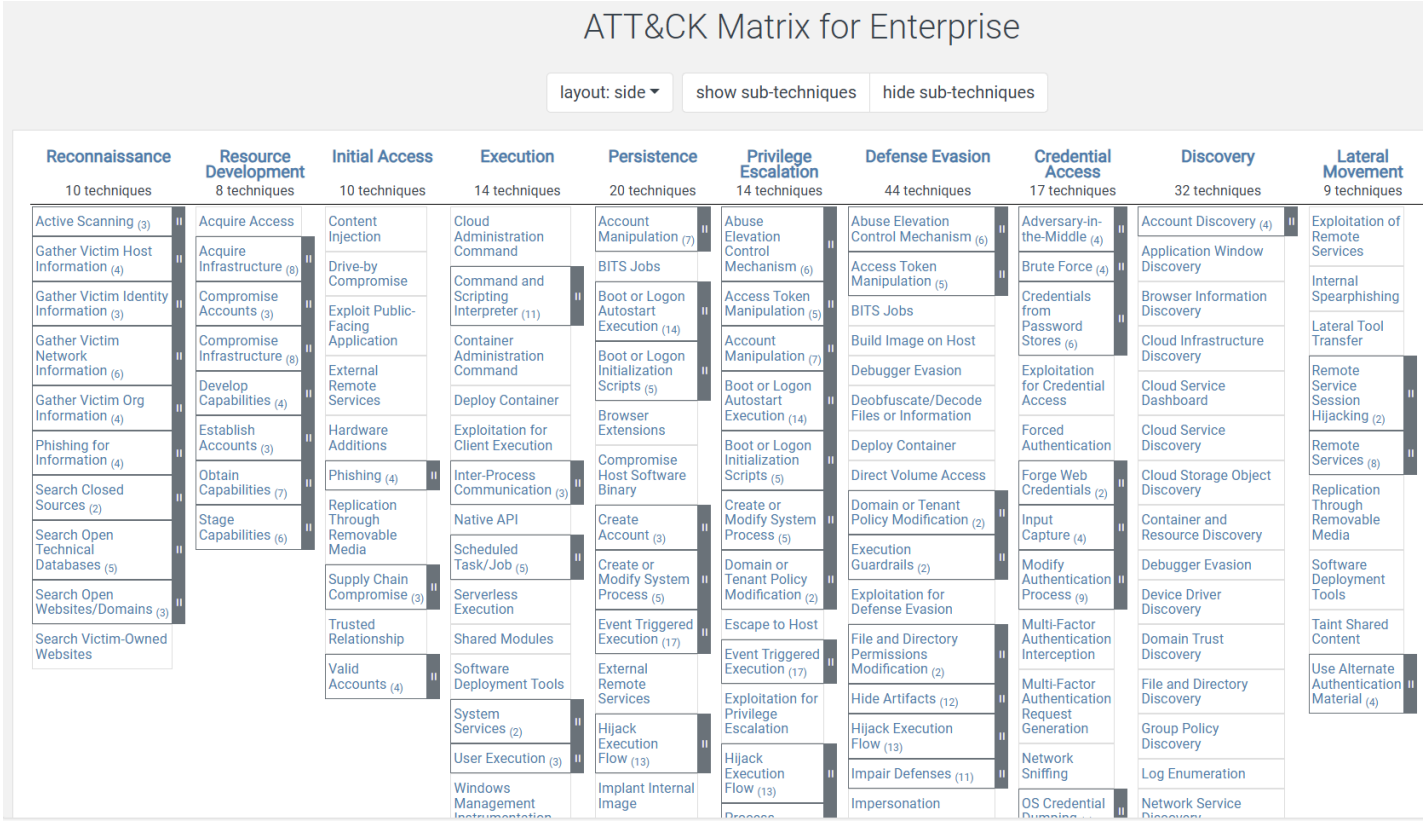
# Where attacks came from?




https://www.visualcapitalist.com/hackers-hack-motives-behind-cyberattacks/

# How to attack?: Attack patterns

- Vulnerability exploitations.
- Weakness exploitation.
- MiTM.
- Malware
- Impersonate identities.
- DoS.
- Lateral Movements.
- ...







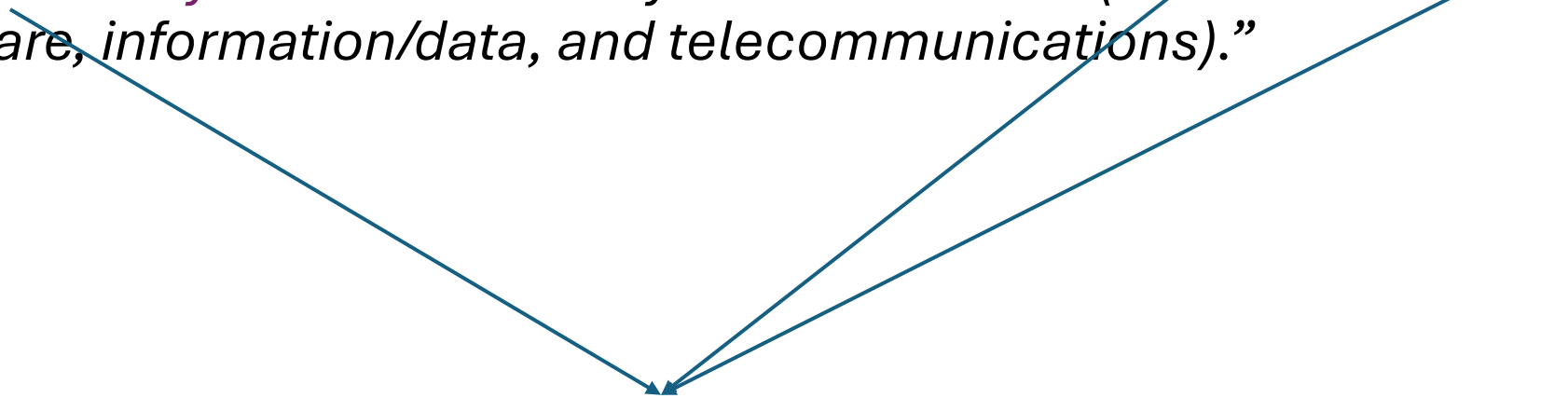



*Blank is left for the whiteboard*

# What is computer/network security?

- Definition from NIST:

*"The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)."*



Objectives of computer security

# REQUIREMENTS

- Confidentiality
  - Information is not available to or disclosed to unauthorized individuals, entities or processes.
- Data integrity
  - Information is not available to or disclosed to unauthorized individuals, entities or processes.
- Availability
  - Information is not available to or disclosed to unauthorized individuals, entities or processes.
- Authentication
  - Authentication ensures that users are identified, and those identities are appropriately verified.
- Authorization
  - Authorization ensures that users' actions are authorized in the system. User privileges allow the intended action.
- Accountability
  - The activities can be proven afterwards that the participants have no means of denying their participation.
- Non-Repudiation
  - The principle that it can be proven afterwards that the participants in a transaction really did authorize the transaction and that they have no means of denying their participation.

# CIA Triad


*Blank is left for the whiteboard*

# ENVIRONMENTAL DEPENDENT

**CIA Triad**

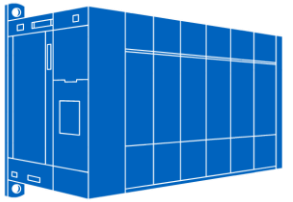
IT:

1. Confidentiality
2. Integrity
3. Availability

Proirity


OT:

1. Availability
2. Integrity
3. Confidentiality



# CRYPTOGRAPHY

Is:

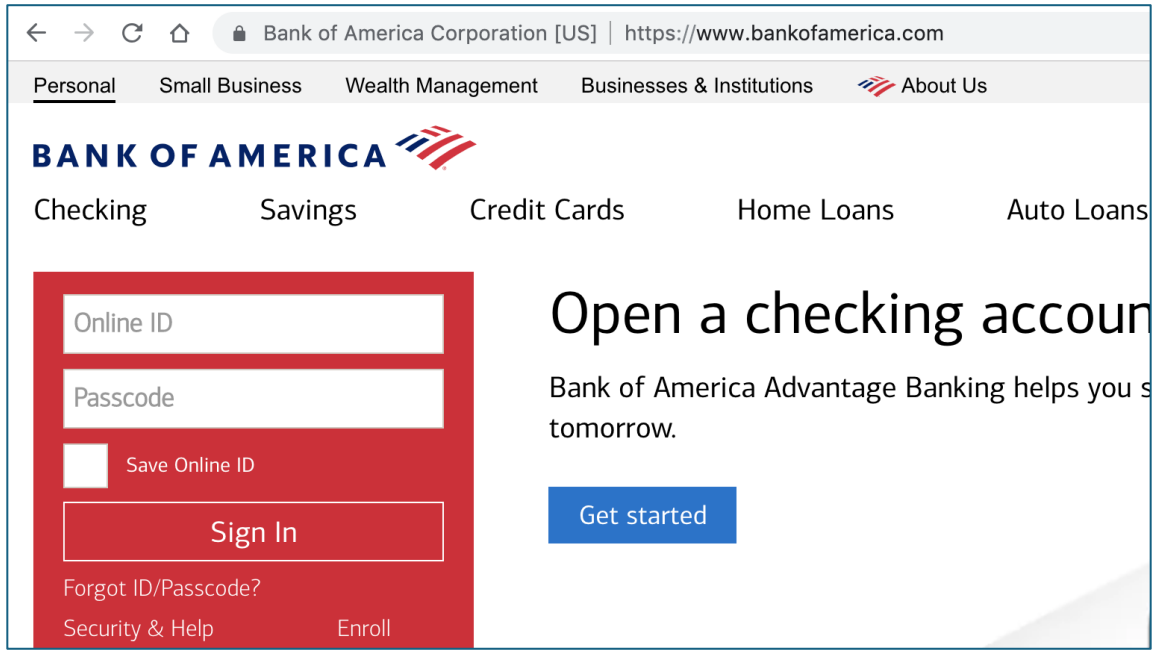
- A tremendous tool for protecting information
- The basis for many security mechanisms

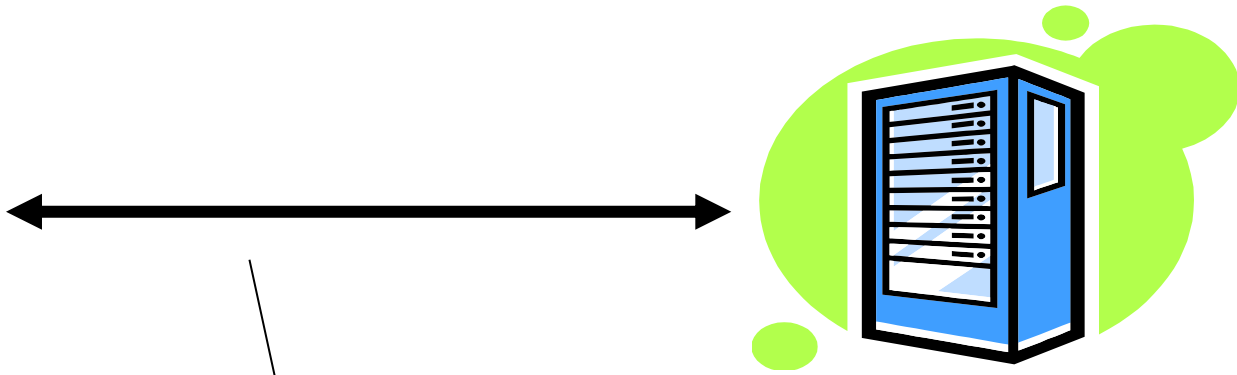
Is not:

- The solution to all security problems
- Reliable unless implemented and used properly
- Something you should try to invent yourself

# GOAL 1: SECURE COMMUNICATION

## (protecting data in transit)



no eavesdropping
no tampering

# TRANSPORT LAYER SECURITY / TLS

Standard for Internet security

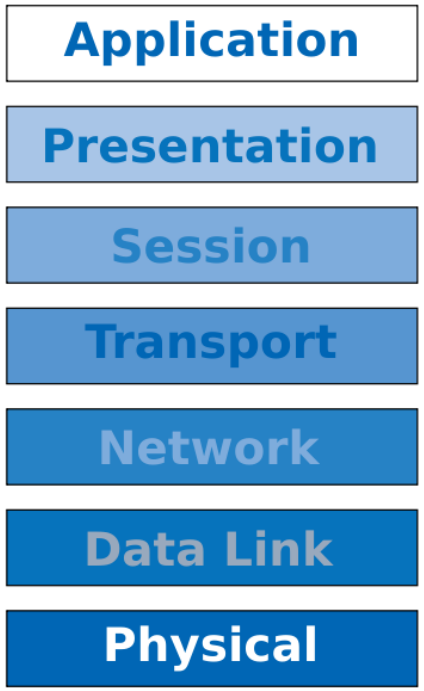
- Goal: "… provide privacy and reliability between two communicating applications"

Two main parts

1. Handshake Protocol: **Establish shared secret key using public-key cryptography**

2. Record Layer: **Transmit data using negotiated key**

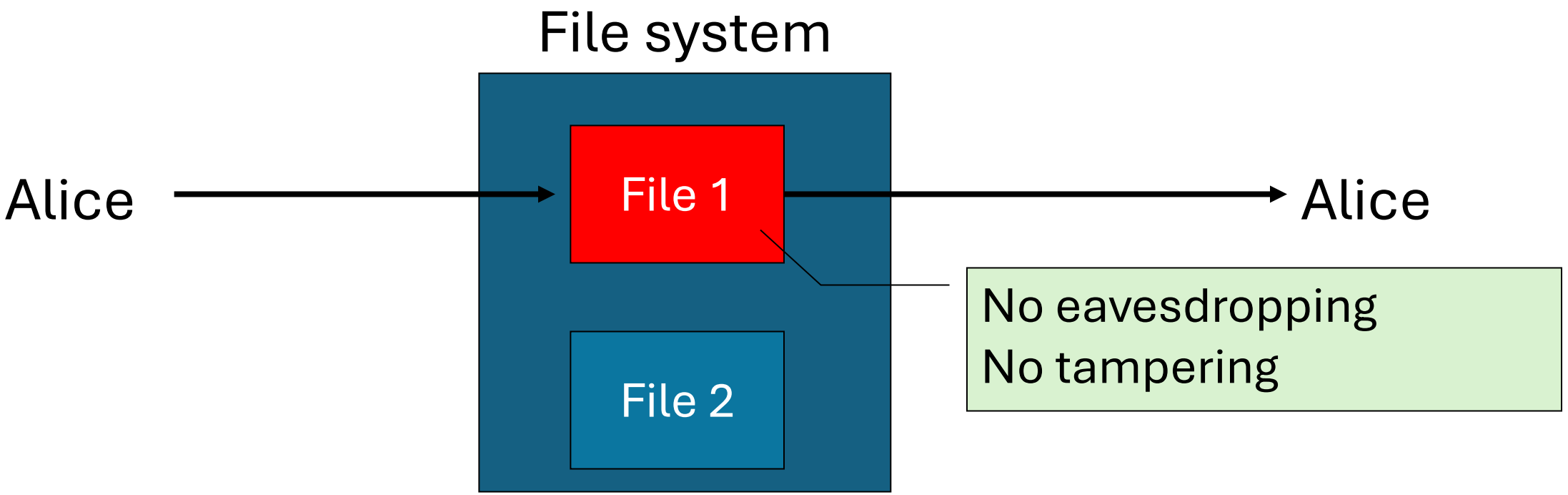
Our starting point: Using a key for encryption and integrity



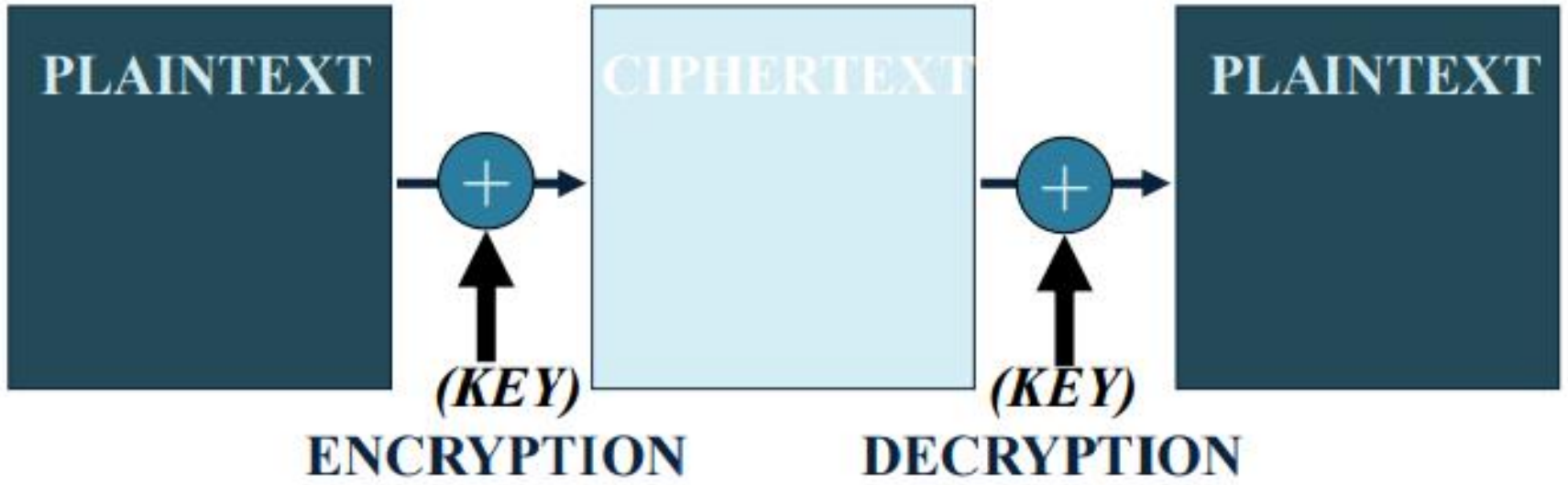

*Blank is left for the whiteboard*

# GOAL 2: PROTECTED FILES

(protecting data at rest)



# ENCRYPTION USED TO SCRAMBLE DATA




**¡Shhhhhh!**

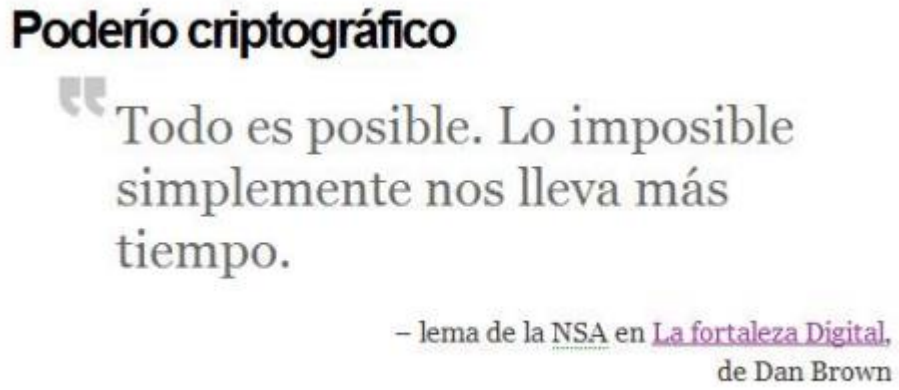
> **Secreto** = Cantidad de Información × (Número de Personas interesadas en conocer el secreto × Tiempo que pasa sin que lo conozcan) / (Personas que conocen el secreto × Tiempo que lo conocen)
>
> – Cómo medir secretos

# BASIC TERMINOLOGY

- **Plaintext** - the original message
- **Ciphertext** - the coded message
- **Cipher** - algorithm for transforming plaintext to ciphertext
- **Key** - info used in cipher known only to sender/receiver
- **Encipher (encrypt)** - converting plaintext to ciphertext
- **Decipher (decrypt)** - recovering ciphertext from plaintext
- **Cryptography** - study of encryption principles/methods
- **Cryptanalysis (codebreaking)** - the study of principles/methods of deciphering ciphertext without knowing key
- **Cryptology** - the field of both cryptography and cryptanalysis

# MORE DEFINITIONS

- **Computational security**
  - Given limited computing resources (e.g., time needed for calculations is greater than age of universe), the cipher cannot be broken.



# CRYPTOANALYSIS: BRUTE FORCE SEARCH

- Always possible to simply try every key
- Most basic attack, proportional to key size
- Assume either known / recognized plaintext

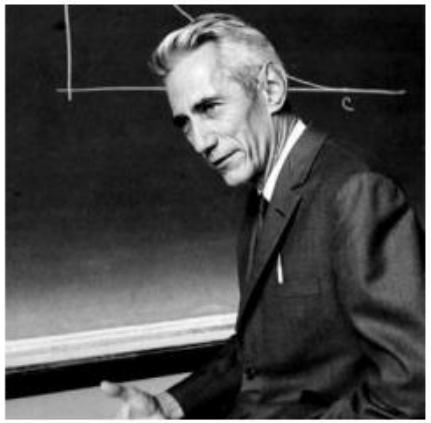
| Key Size (bits) | Number of Alternative Keys | Time required at 1 encryption/$\mu s$ | Time required at $10^6$ encryptions/$\mu s$ |
|---|---|---|---|
| 32 | $2^{32} = 4.3 \times 10^9$ | $2^{31}\ \mu s = 35.8$ minutes | 2.15 milliseconds |
| 56 | $2^{56} = 7.2 \times 10^{16}$ | $2^{55}\ \mu s = 1142$ years | 10.01 hours |
| 128 | $2^{128} = 3.4 \times 10^{38}$ | $2^{127}\ \mu s = 5.4 \times 10^{24}$ years | $5.4 \times 10^{18}$ years |
| 168 | $2^{168} = 3.7 \times 10^{50}$ | $2^{167}\ \mu s = 5.9 \times 10^{36}$ years | $5.9 \times 10^{30}$ years |
| 26 characters (permutation) | $26! = 4 \times 10^{26}$ | $2 \times 10^{26}\ \mu s = 6.4 \times 10^{12}$ years | $6.4 \times 10^6$ years |

# CRYPTOSYSTEM CLASSIFICATION

- Can be characterized by:
  - Historical and cultural (not technical)
    - Classical / modern
  - Type of encryption operations used
    - Substitution / transposition / product
  - Number of keys used
    - Single-key or secret / two-key or public / even no key
  - Way in which plaintext is processed
    - Block / stream

# Boundary between classical and modern cryptography

- We will consider the important milestones of modern cryptography.
- We must answer: when did we move from mechanical to digital encryption? when did we move from military encryption to civil encryption?



Claude Shannon: 1948 - 1949

Hortz Feistel: 1974

Whitfield Diffie y Martin Hellman: 1976

# Historical classification of cryptosystems

- This is not the best classification from the point of view of engineering and computer science.
- But it will allow us to see the development of these encryption techniques, nowadays rudimentary and simple, from a historical perspective and it is also culturally interesting for an engineer.
- Classical cryptography will allow us to cryptanalyze with some facility practically all these cipher systems.

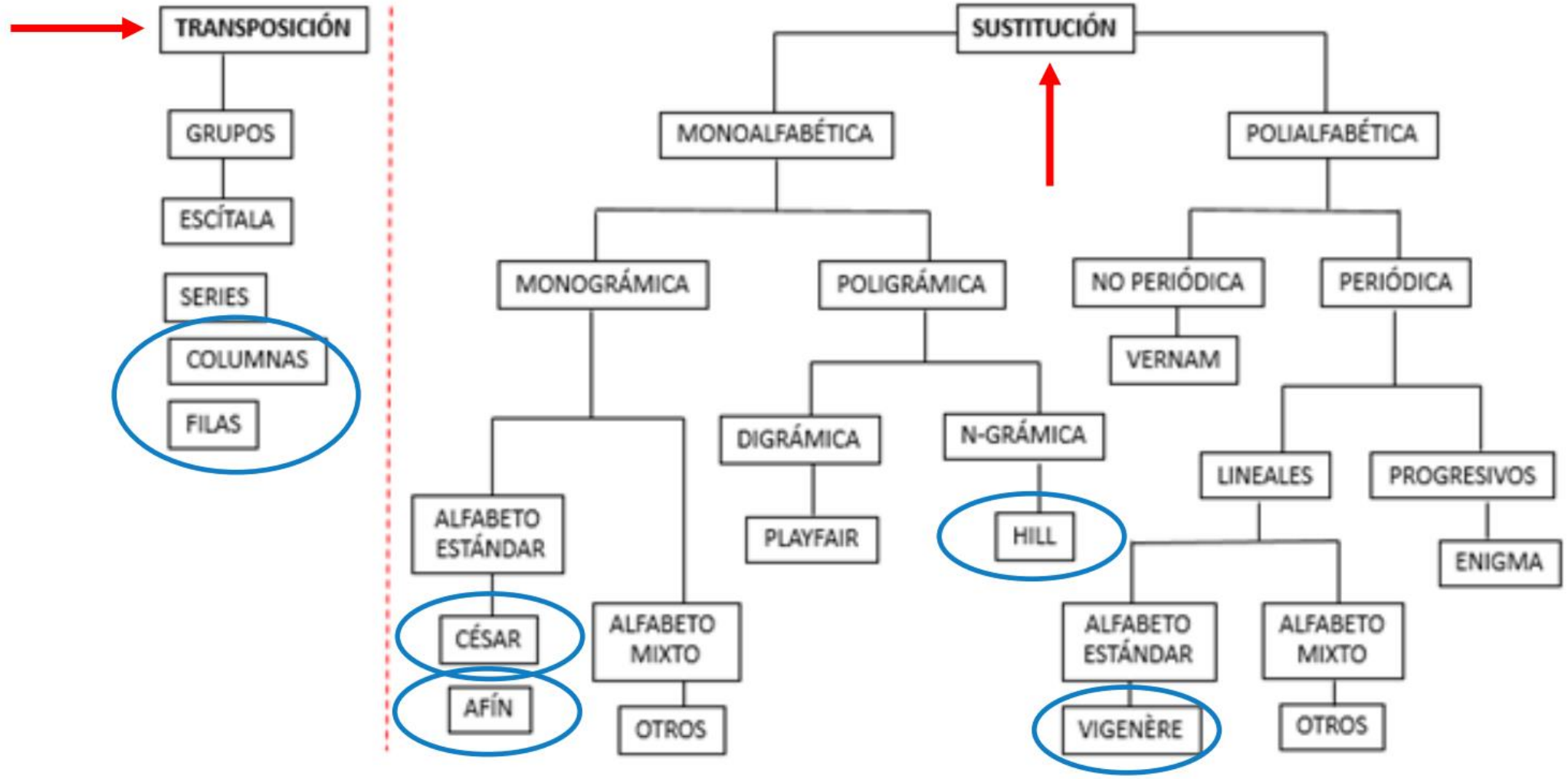
# Chronological details of the classic cypher

- In the Ancient Age (From 4,000 B.C. to the 4th century)
  - The Spartans cipher messages using the scytale.
  - The Greek historian Polybius describes the Polybius cipher.
  - Julius Caesar uses a method for encrypting his messages.
- In the Middle Ages (from the 5th to the 15th century)
  - Leon Battista Alberti publishes “Modus scribendi in ziferas” in which he speaks for the for the first time of Alberti's disk, the first polyalphabetic system.
  - The French diplomat Blaise de Vigenère publishes “Tractié de Chiffre” in which he presents the first polyalphabetic system with an autoclave, known as “Le chiffre indéchiffrable”, although it was later renamed “Le Vigenère's cipher (from the 16th century).

# Chronological details of the classic cypher

- In the contemporary age (from the end of the 18th century to today)
  - Friedrich Kasiski develops statistical methods of cryptanalysis that were able to break Vigenère's cipher.
  - La Cryptographie militaire" by Auguste Kerckhoff von Nieuwendhoff contains the "Kerckhoff principle" which requires basing the security of an encryption method solely on the encryption method solely on the secrecy of the key and not on the algorithm.
  - Lester S. Hill published the paper "Cryptography in an Algebraic Alphabet" and Hill's cipher applying algebra, modular multiplication of matrices.
  - Mechanical and electromechanical cipher machines, such as the Enigma machine that Alan Turing creates using the idea of the Turing bomb, which he conceived based on previous work of Marian Rejewski.

# CLASSICAL CRYPTOSYSTEMS CLASSIFICATION



# TWO BASIC TYPES OF OPERATIONS

- Substitution (TVCTUJUVUJPO)
  - Message broken up into units
  - Units mapped into ciphertext
    - Ex: Caesar cipher
  - First-order statistics are kept in simplest cases
  - Predominant form of encryption
- Transposition (TASOIINRNPSTO)
  - Message broken up into units
  - Units permuted in a seemingly random but reversible manner
  - Difficult to make it easily reversible, only by intended receiver
  - Exhibits same first-order statistics

# TWO BASIC BLOCKS OF ENCRYPTION TECHNIQUES

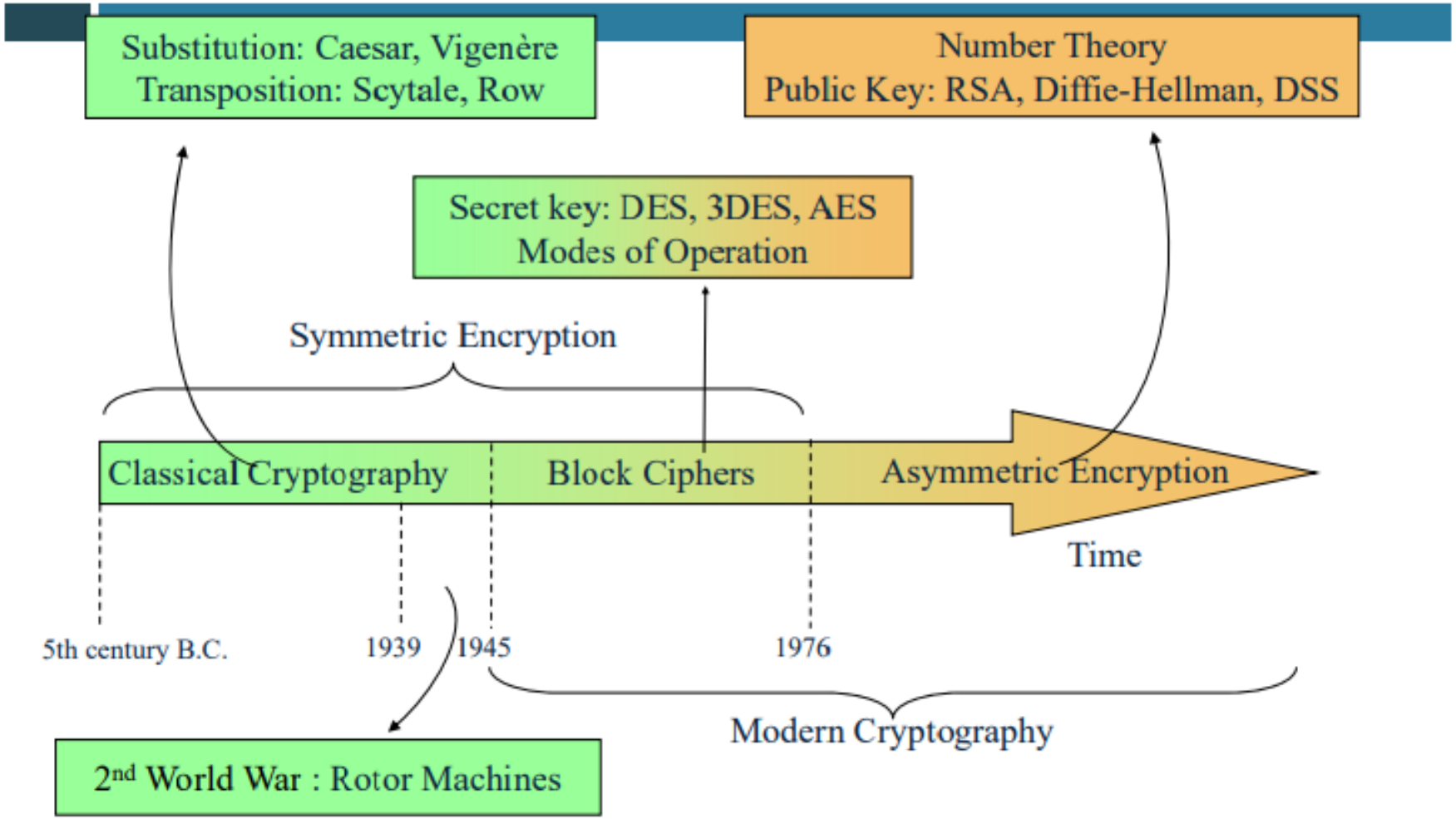
- **Substitution**
  - The letters of plaintext are replaced by other letters or by numbers or symbols, e.g.

HOME → IPNF

- **Transposition**
  - The characters (bits) are rearranged without modification, which is also called permutation, e.g.

HOME → EMOH

# CRYPTOSYSTEM CLASSIFICATION



# “TWO” BASIC CIPHER TYPES

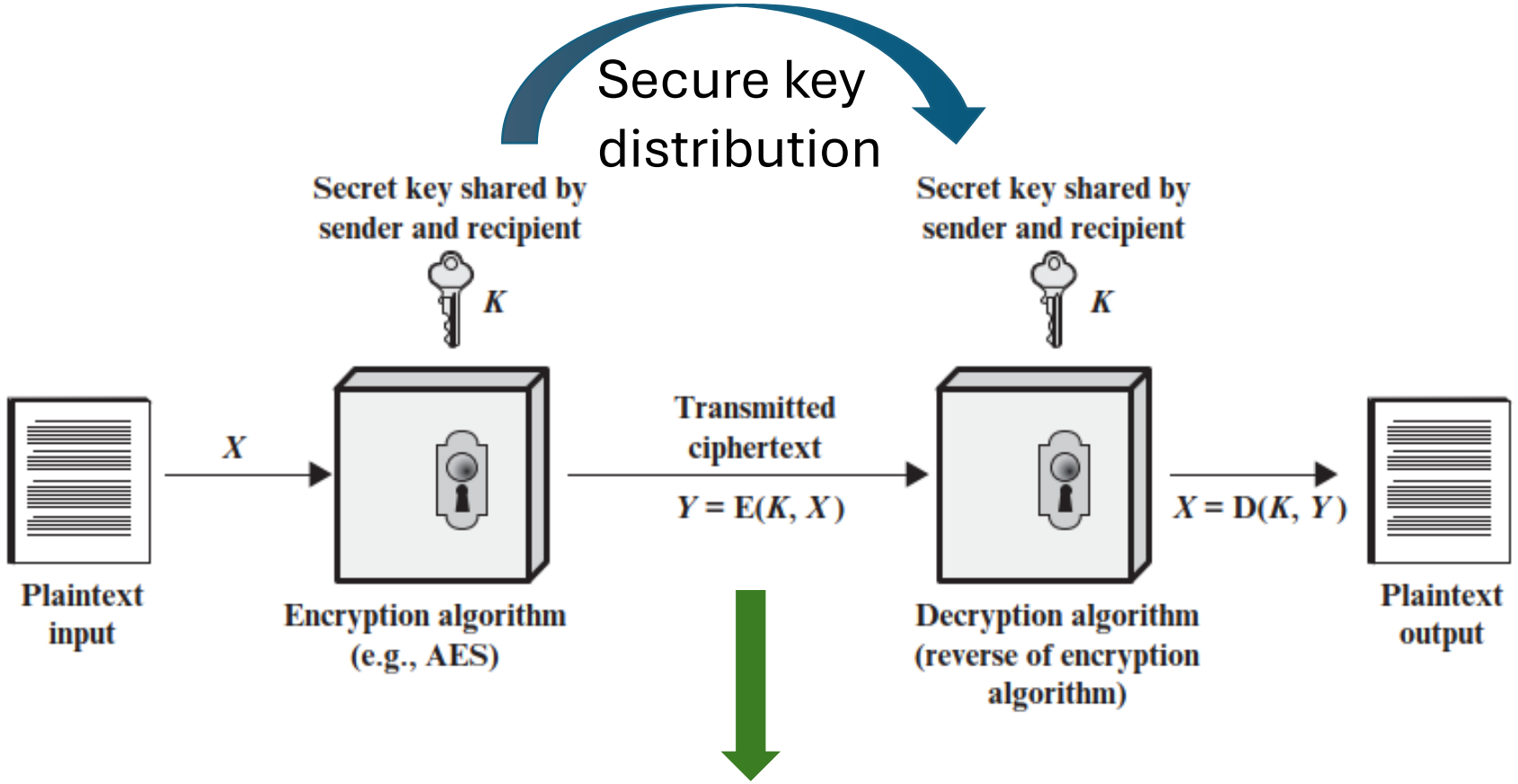
- Symmetric-key (secret key, conventional)
  - Single key used for both encryption and decryption
  - Keys are typically short, because key space is densely filled
  - Ex: DES, 3DES, AES, IDEA, Blowfish, RC5, RC4, etc.
- Public-key (asymmetric)
  - Two keys: one for encryption, one for decryption
  - Keys are typically long, because key space is sparsely filled
  - Ex: RSA, Diffie-Hellman, ElGamal, ECC, DSA, etc
- Hash Functions (no confidentiality but integrity and DS)
  - No key
  - Create a fixed-length fingerprint
  - Ex: MD4, MD5, SHA-1, etc.

# WHAT CAN WE USE?

- Symmetric vs asymmetric cipher?
- Symmetric ciphers
  - Faster but without digital signatures
- Asymmetric ciphers
  - Slower but with digital signatures

Information enciphering:
Secret key cipher
Digital signature and key distribution:
Public key cipher

# SYMMETRIC CIPHER MODEL




Cryptanalysis and brute-force attack

# REQUIREMENTS

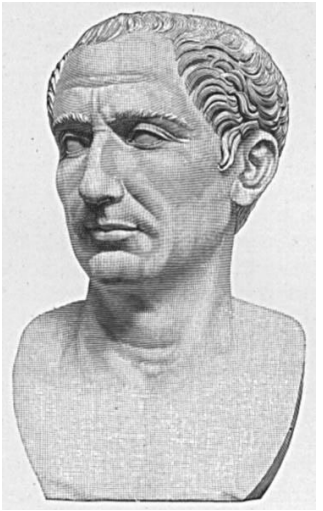
- Two requirements for secure use of symmetric encryption:
  - A strong encryption algorithm
  - A secret key known only to sender / receiver
    - $Y = E_k(X)$
    - $X = D_k(Y)$
  - Assume encryption algorithm is known
  - It needs a secure channel to distribute key

# CAESAR CIPHER

- Earliest known substitution cipher, designed by Julius Caesar
- Key idea: replaces each letter by the 3rd next letter
- Example:

meet me after the toga party

PHHW PH DIWHU WKH WRJD SDUWB



- Formal description:

$$C = E(k, p) = (p+k) \bmod 26$$

$$p = D(k, C) = (C-k) \bmod 26$$

  - C-Cipher text
  - p-plaintext
  - k-key

Numerical equivalent to each letter:

| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

| n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

# CAESAR CIPHER WEAKNESS

Plaintext: GALLIA EST OMNIS DIVISA ...

ABCDEFGHIJKLMNOPQRSTUVWXYZ

et:

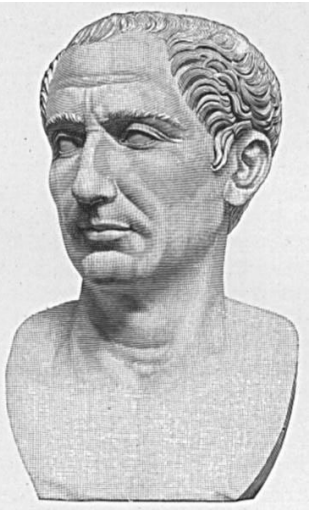
DEFGHIJKLMNOPQRSTUVWXYZABC

Ciphertext: JDOOLD HVW RPQLV GLYLVD ...

$$C_i = E(P_i) = P_i + k \bmod 26$$

$$P_i = D(C_i) = C_i - k \bmod 26$$

$k = 3$ for Caesar



Each letter is enciphered in the same way. It's a great weakness and the system can be easily attacked by means of letter frequencies.

# EXAMPLE OF CAESAR CIPHER (MOD 26)

- Plaintext: meet me after the toga party
- Ciphertext (k=3):

  PHHW PH DIWHU WKH WRJD SDUWB
- Formal description:

$$C = E(k, p) = (p+3) \bmod 26$$

$$p = D(k, C) = (C-3) \bmod 26$$

Numerical equivalent to each letter:

| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

| n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

# CRYPTANALYSIS OF CAESAR CIPHER

- Could simply try each key in turn (**brute force)**
  - Encryption/decryption algorithms are known
  - There are few keys to try (26): A maps to A, B,...Z
  - The language of the plaintext is known
- Given ciphertext, just try all shifts of letters

| KEY | PHHW PH DIWHU WKH WRJD SDUWB |
|---|---|
| 1 | oggv og chvgt vjg vqic rctva |
| 2 | nffu nf bgufs uif uphb qbsuz |
| 3 | meet me after the toga party |
| 4 | ldds ld zesdq sgd snfz ozqsx |
| 5 | kccr kc ydrcp rfc rmey nyprw |
| 6 | jbbq jb xcqbo qeb qldx mxoqv |
| 7 | iaap ia wbpan pda pkcw lwnpu |
| 8 | hzzo hz vaozm ocz ojbv kvmot |
| 9 | gyyn gy uznyl nby niau julns |
| 10 | fxxm fx tymxk max mhzt itkmr |
| 11 | ewwl ew sxlwj lzw lgys hsjlq |
| 12 | dvvk dv rwkvi kyv kfxr grikp |
| 13 | cuuj cu qvjuh jxu jewq fqhjo |
| 14 | btti bt puitg iwt idvp epgin |
| 15 | assh as othsf hvs hcuo dofhm |
| 16 | zrrg zr nsgre gur gbtn cnegl |
| 17 | yqqf yq mrfqd ftq fasm bmdfk |
| 18 | xppe xp lqepc esp ezrl alcej |
| 19 | wood wo kpdob dro dyqk zkbdi |
| 20 | vnnc vn jocna cqn cxpj yjach |
| 21 | ummb um inbmz bpm bwoi xizbg |
| 22 | tlla tl hmaly aol avnh whyaf |
| 23 | skkz sk glzkx znk zumg vgxze |
| 24 | rjjy rj fkyjw ymj ytlf ufwyd |
| 25 | qiix qi ejxiv xli xske tevxc |

# MONOALPHABETIC SUBSTITUTION CIPHER

- Could shuffle (jumble) the letters arbitrarily
- Each plaintext letter maps to a different random ciphertext letter

Original letter: 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
Random key: D K VQ F I B J W P E S C X H T M Y A U O L R G Z N

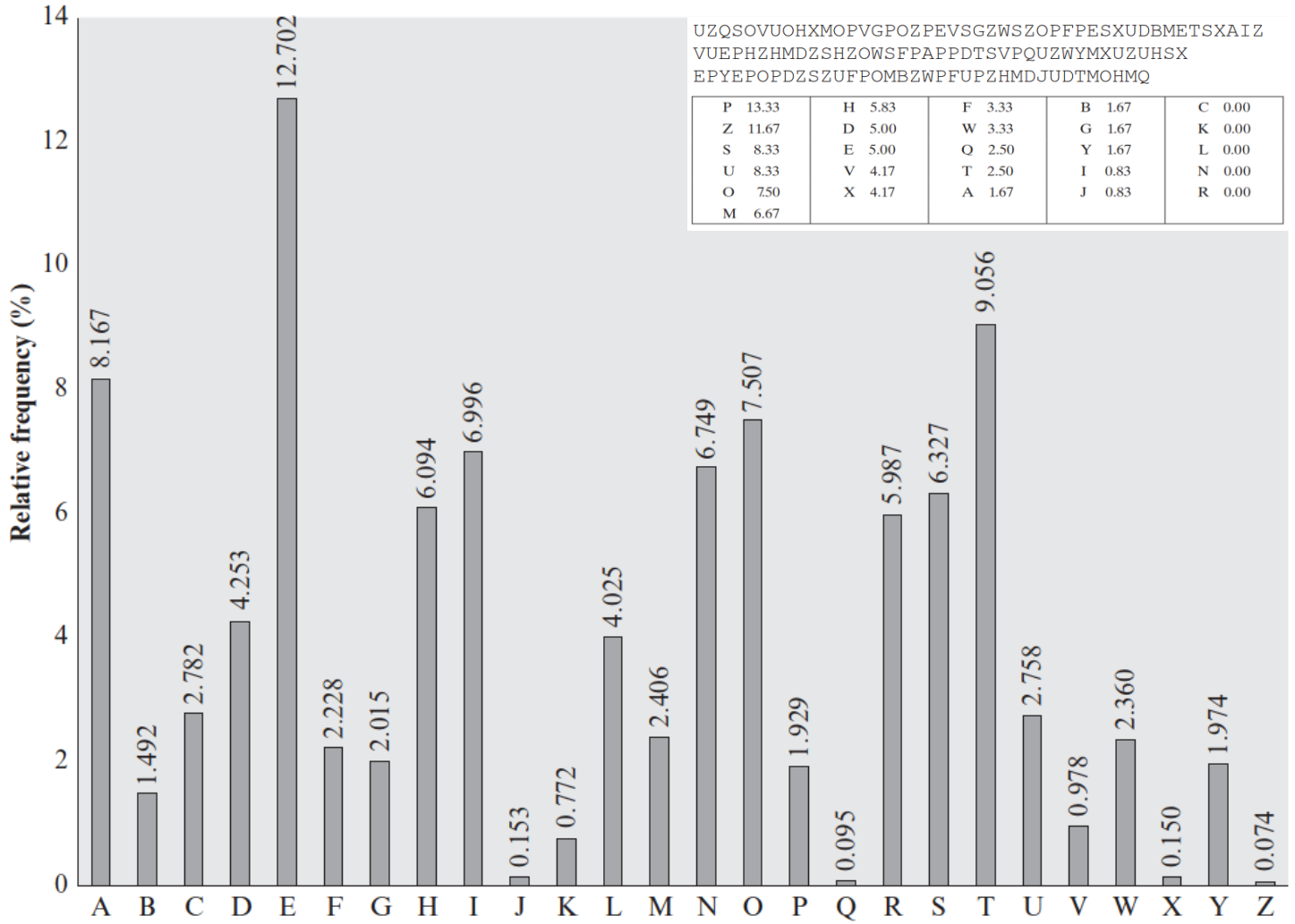
Plaintext: if we wish to replace letters
Ciphertext: WI RF RWAJ UH YFTSDVF SFUUFYA

# MONOALPHABETIC CIPHER SECURITY

- The key size is 26 letters long
- 26! different permutations
- Each permutation considered a *key*
- Key space contains 26! = $4x10^{26}$ keys, difficult to try every possible key
- With so many keys, you might think it is secure

**WRONG!!!** Problem is language characteristics!

# ENGLISH LETTER FREQUENCIES



# VIGENÈRE CIPHER

- Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message.
- Simplest polyalphabetic substitution cipher is the Vigenère Cipher

$$C_i = (p_i + k_{i \bmod m}) \bmod 26$$
$$p_i = (C_i - k_{i \bmod m}) \bmod 26$$

An example with the key as ‘deceptive’:

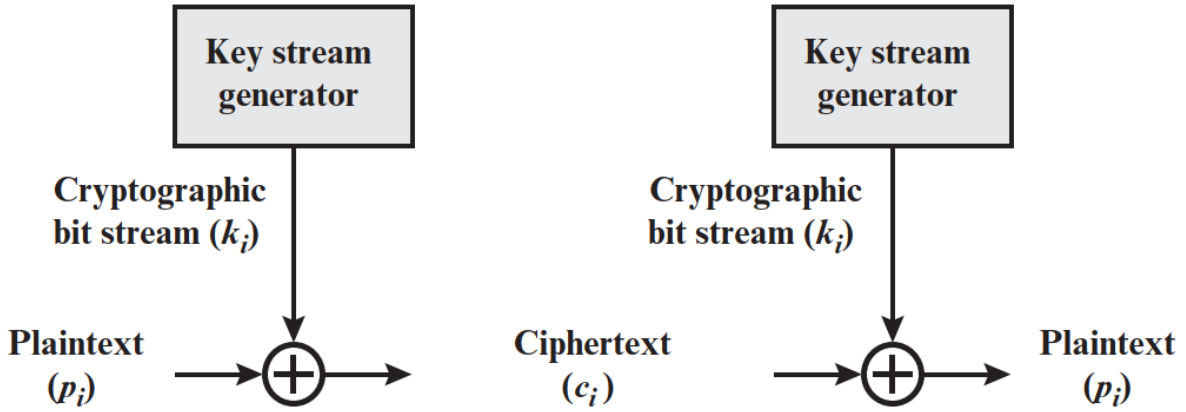
```
key:          deceptivedeceptivedeceptive
plaintext:    wearediscoveredsaveyourself
ciphertext:   ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

| key | 3 | 4 | 2 | 4 | 15 | 19 | 8 | 21 | 4 | 3 | 4 | 2 | 4 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| plaintext | 22 | 4 | 0 | 17 | 4 | 3 | 8 | 18 | 2 | 14 | 21 | 4 | 17 | 4 |
| ciphertext | 25 | 8 | 2 | 21 | 19 | 22 | 16 | 13 | 6 | 17 | 25 | 6 | 21 | 19 |

| key | 19 | 8 | 21 | 4 | 3 | 4 | 2 | 4 | 15 | 19 | 8 | 21 | 4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| plaintext | 3 | 18 | 0 | 21 | 4 | 24 | 14 | 20 | 17 | 18 | 4 | 11 | 5 |
| ciphertext | 22 | 0 | 21 | 25 | 7 | 2 | 16 | 24 | 6 | 11 | 12 | 6 | 9 |

# VERNAM CIPHER

- The ultimate solution is to choose a key that is as long as the plaintext and has no statistical relationship to it
- Gilbert Vernam firstly introduced such a system in 1918
- The essence of this technique is the means of construction of the key, which eventually repeated




$$c_i = p_i \oplus k_i \qquad p_i = c_i \oplus k_i$$

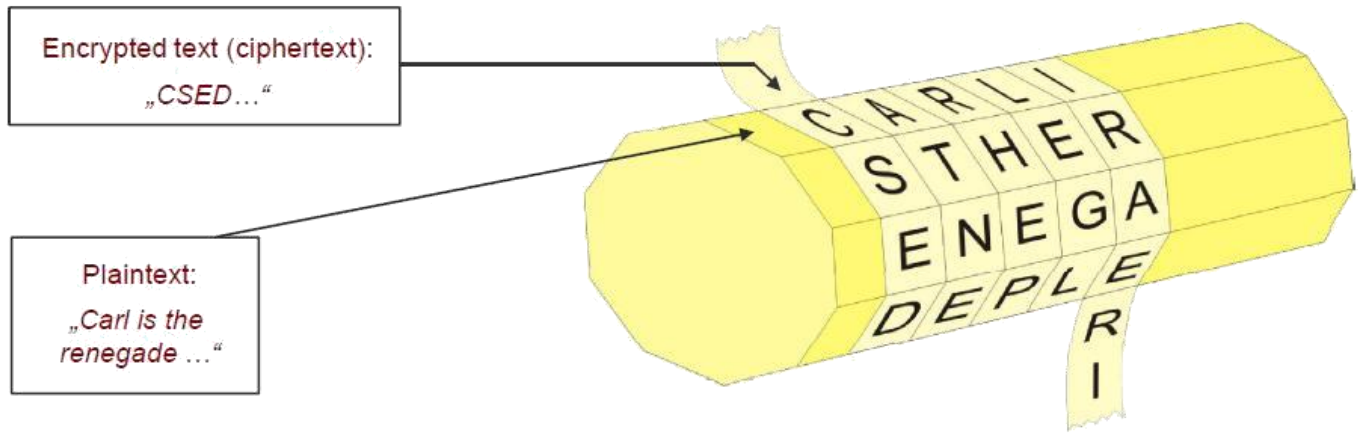
# ONE-TIME PAD

- An Army Signal Corp officer, Joseph Mauborgne, proposed an improvement to the Vernam cipher that yields the ultimate in security:
  - Mauborgne suggested using a random key that is as long as the message, so that the key need not be repeated.
  - The key is to be used to encrypt and decrypt a single message and then is discarded.
  - Each new message requires a new key of the same length as the new message.
- Such a scheme is known as a one-time pad, which is unbreakable
- Problems:
  - Make large quantities of random keys
  - Safe distribution of key
  - Can only use the key **once** though

# CLASSICAL TRANSPOSITION TECHNIQUES

- All the techniques examined so far involve the substitution of a ciphertext symbol for a plaintext symbol.
- A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters → Transposition

# FIRST TRANSPOSITION CIPHER: SKYTALE




# SKYTALE CIPHER METHOD

- The Skytale was used in the 5th century B.C. by the Greeks.
- It consisted of a stick with a leather ribbon and the message was written lengthwise
- When the ribbon is unrolled, letters appear without order
- The only way of recovering the plaintext was rolling back the ribbon along a stick with the same diameter as the original.
- The key was the diameter.
- It is a transposition cipher because characters are the same but distributed along the text by another way

# RAIL FENCE CIPHER

- Write message letters out diagonally over a number of rows
- Then read off cipher row by row
- Eg. write message “meet me after the toga party” out with a rail fence of depth 2 as:

```
m e m a t r h t g p r y
  e t e f e t e o a a t
```

- Giving ciphertext

```
MEMATRHTGPRYETEFETEOAAT
```

# COLUMN TRANSPOSITION CIPHERS

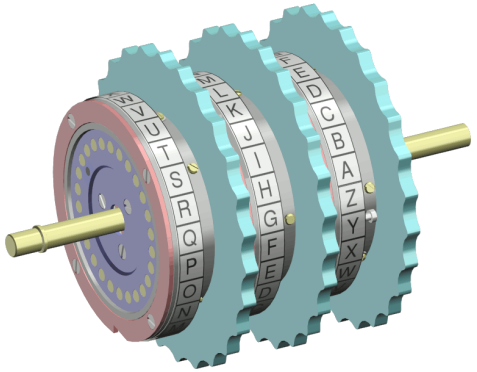
- A more complex scheme
- Write letters of message ‘attack postponed until two am’ out in rows over a specified number of columns
- The order of the columns becomes the key to the algorithm

```
Key:        4 3 1 2 5 6 7
Plaintext: a t t a c k p
           o s t p o n e
           d u n t i l t
           w o a m x y z
Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

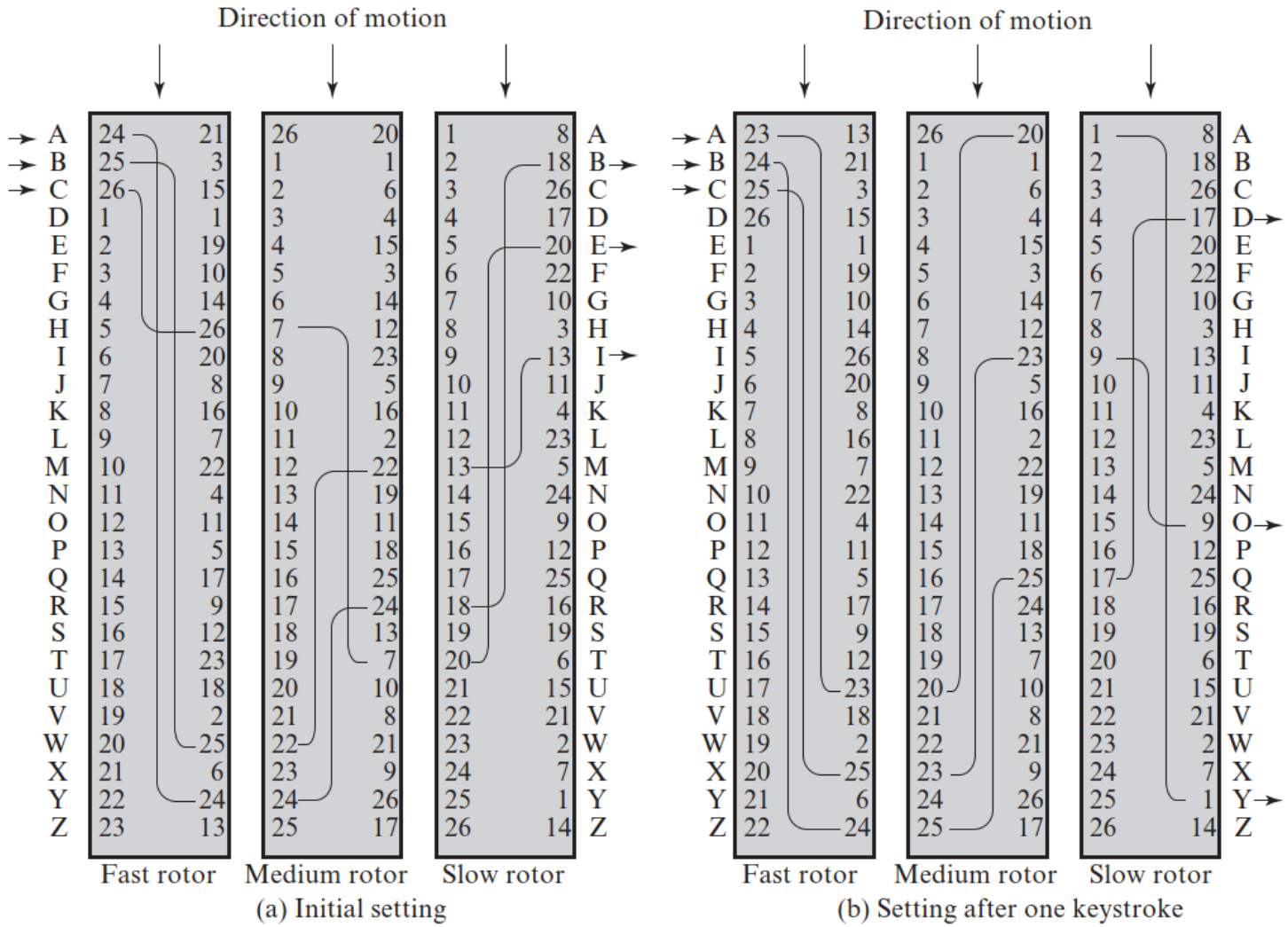
- Can be made significantly more secure by performing more than one stage of transposition.

# ROTOR MACHINES

- Before modern ciphers, rotor machines (electromechanical) were the most common product cipher
- The machine consists of a set of independently rotating cylinders through which electrical pulses can flow.



# ROTOR MACHINES




(a) Initial setting

(b) Setting after one keystroke

# ROTOR MACHINES

- Single cylinder → monoalphabetic substitution
- Rotation → different monoalphabetic substitution cipher is defined
- 1 cylinder is a polyalphabetic cipher with 26 associated monoalphabetic ciphers (period of 26)
- With 3 cylinders have $26^3$=17576 alphabets!!
- The addition of 4th and 5th rotors results in periods of 456,976 and 11,881,376 letters, respectively.

# CLASSICAL CRYPTOSYSTEMS CLASSIFICATION