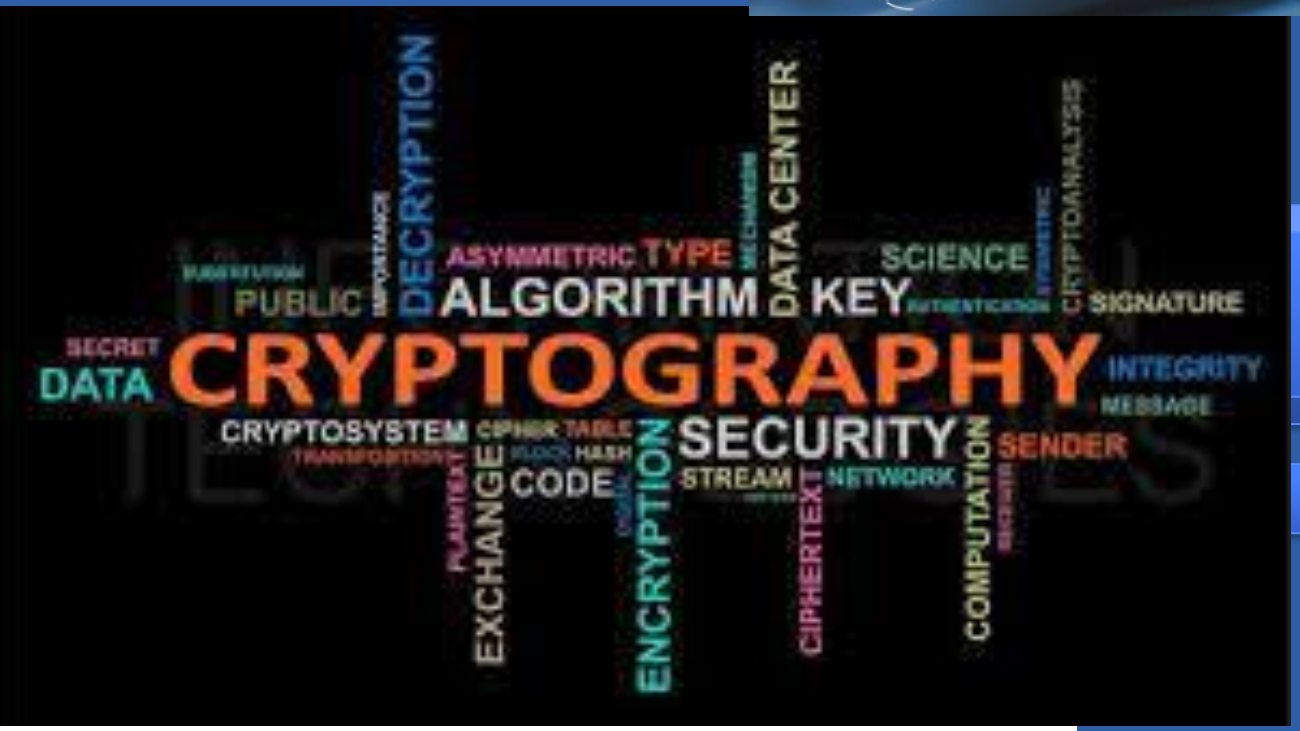
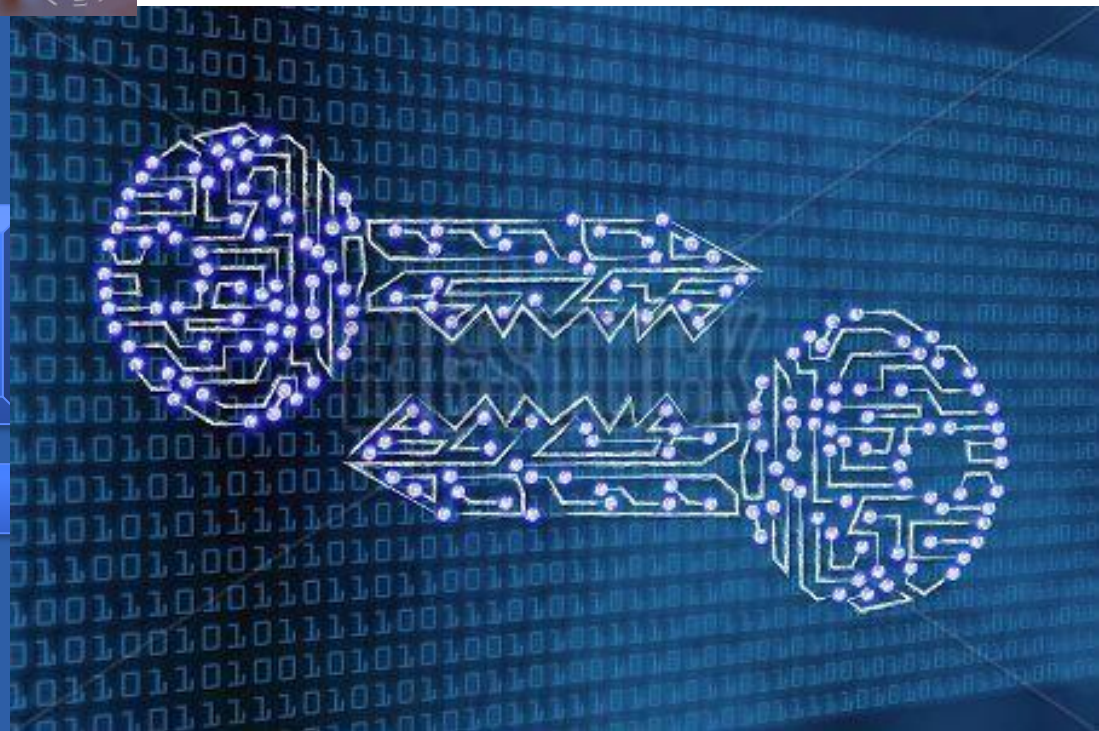
Criptografía

Universidad Francisco de Vitoria
UFV Madrid

Tema 2
Criptografía Clásica





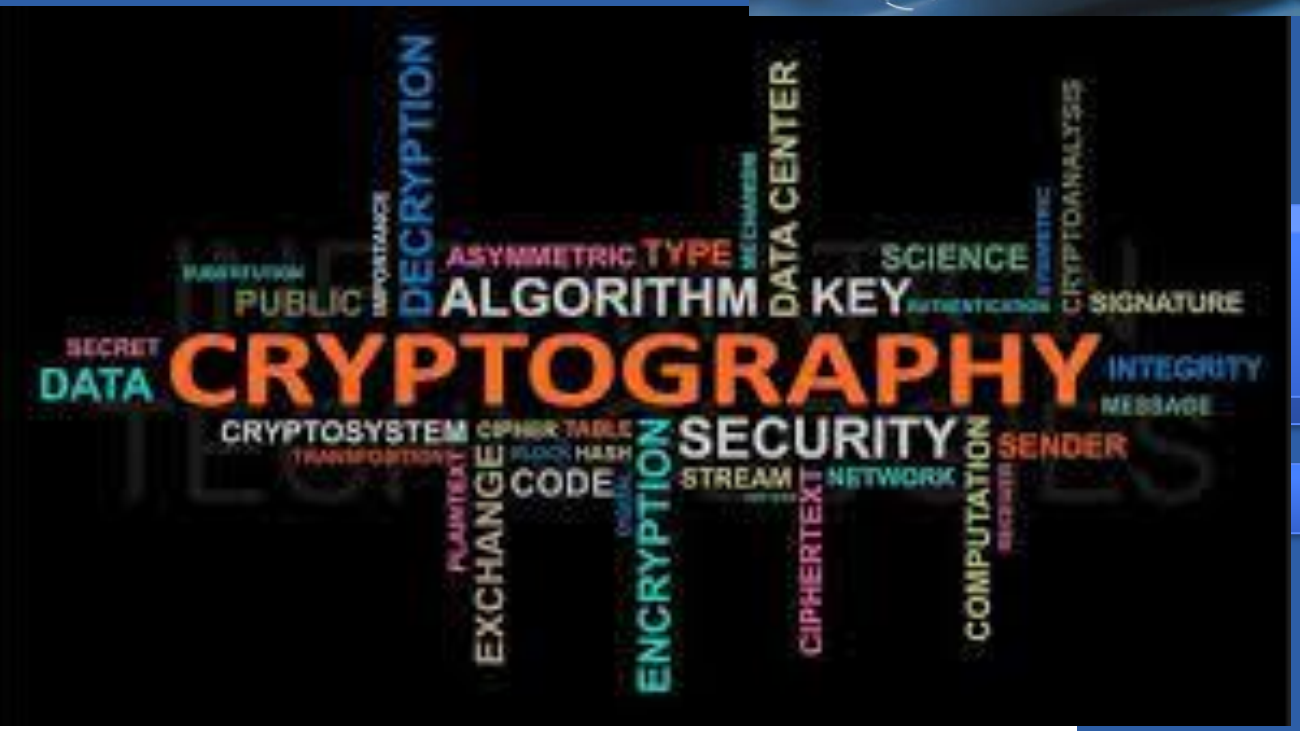
Criptografía Clásica

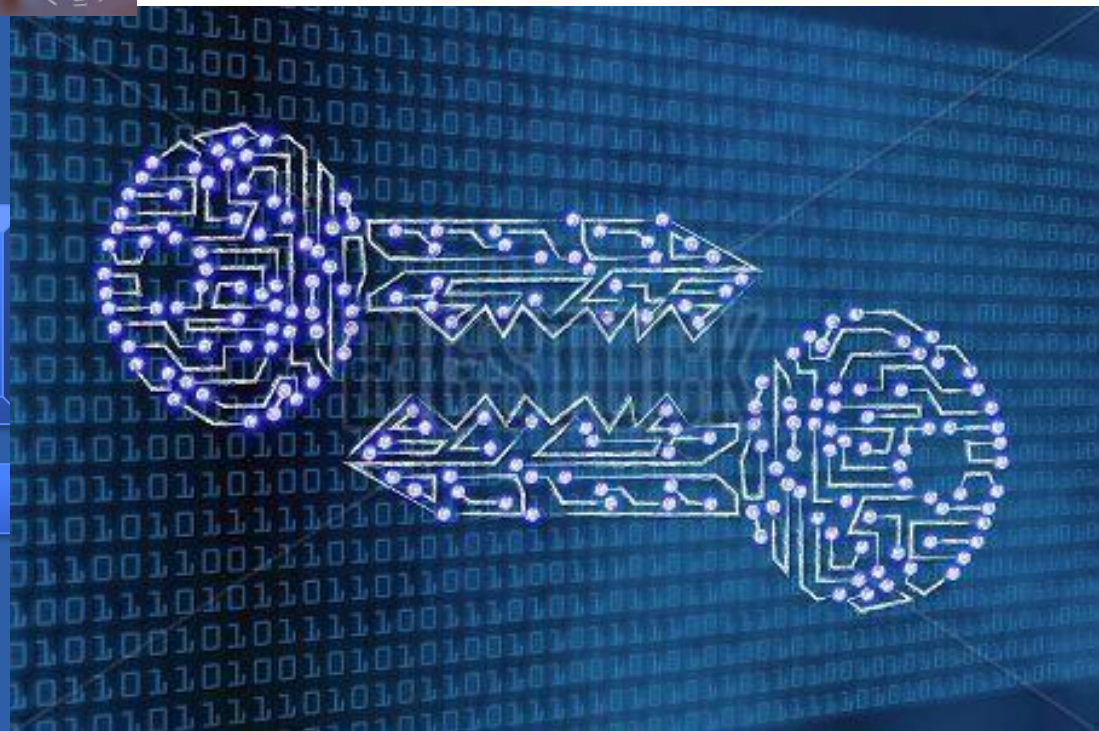
- Introducción
- Métodos de cifrado clásico
- Criptoanálisis

Criptografía

Universidad Francisco de Vitoria
UFV Madrid

Tema 1.1
Introducción a la Criptografía Clásica





Criptografía Clásica

- **Criptografía**
  - del griego κρύπτος (kryptós), «secreto», y
  - γραφή (graphé), «grafo» o «escritura»,
    - literalmente «***escritura secreta***»

➢ ámbito de la **criptología** que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

Criptografía Clásica

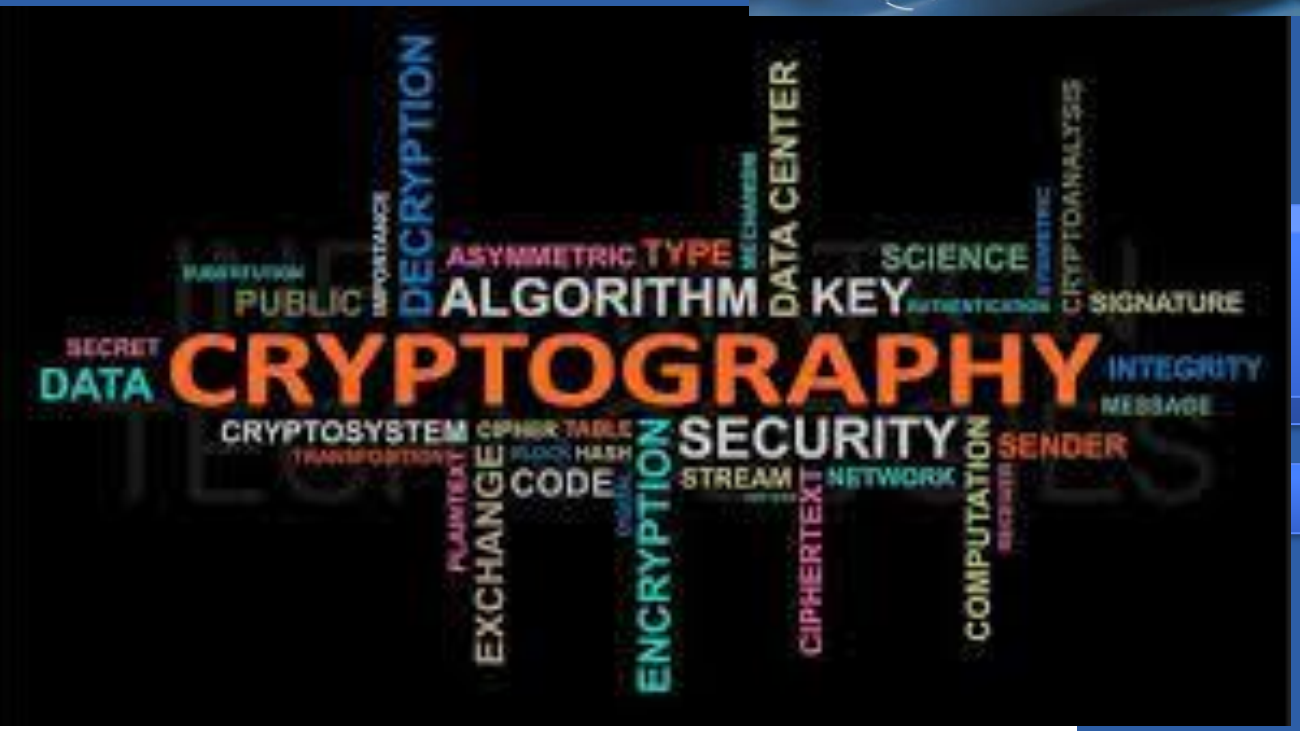
- ***¿Criptografía vs Criptología?***

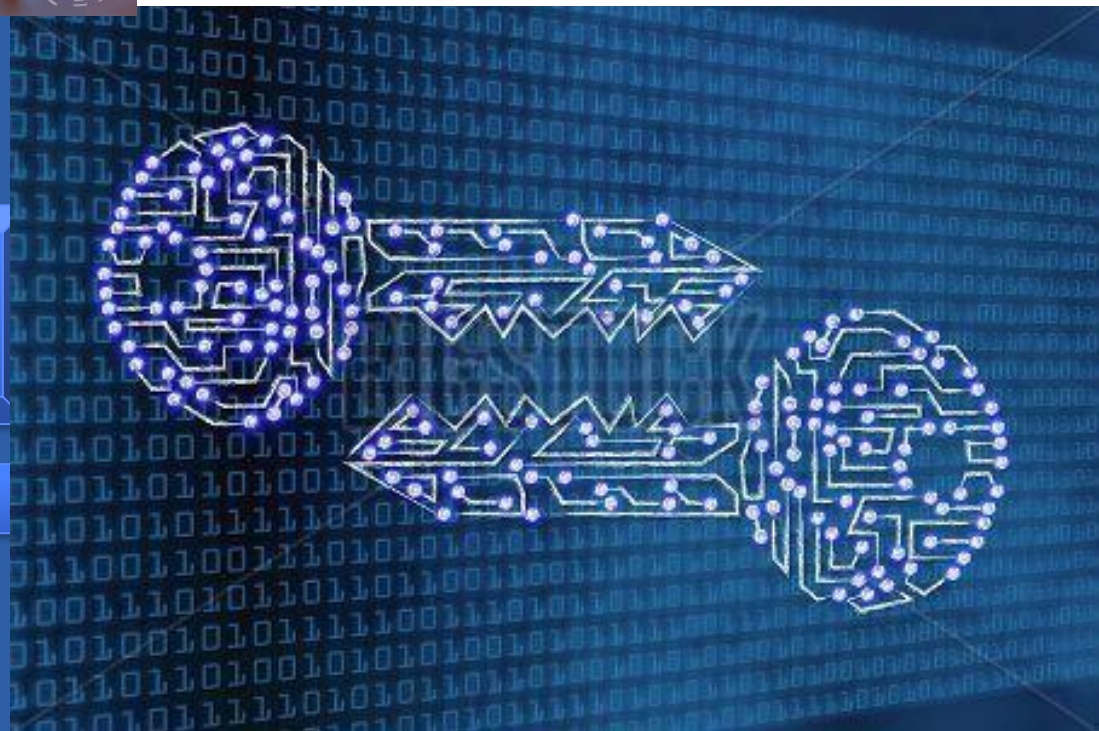
Criptología = Criptografía + Criptoanálisis

Criptografía

Universidad Francisco de Vitoria
UFV Madrid

Tema 1.2
Métodos de cifrado clásico





Criptografía Clásica

- **Métodos** de cifrado clásico

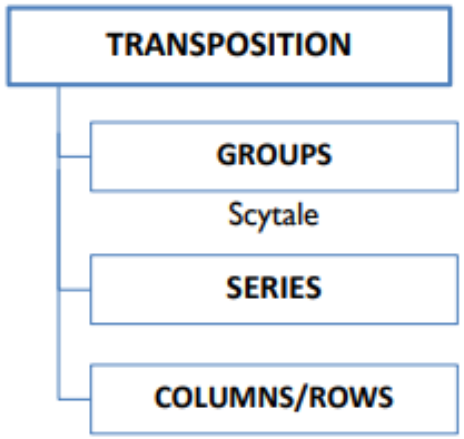
  - Los principales métodos se pueden clasificar en

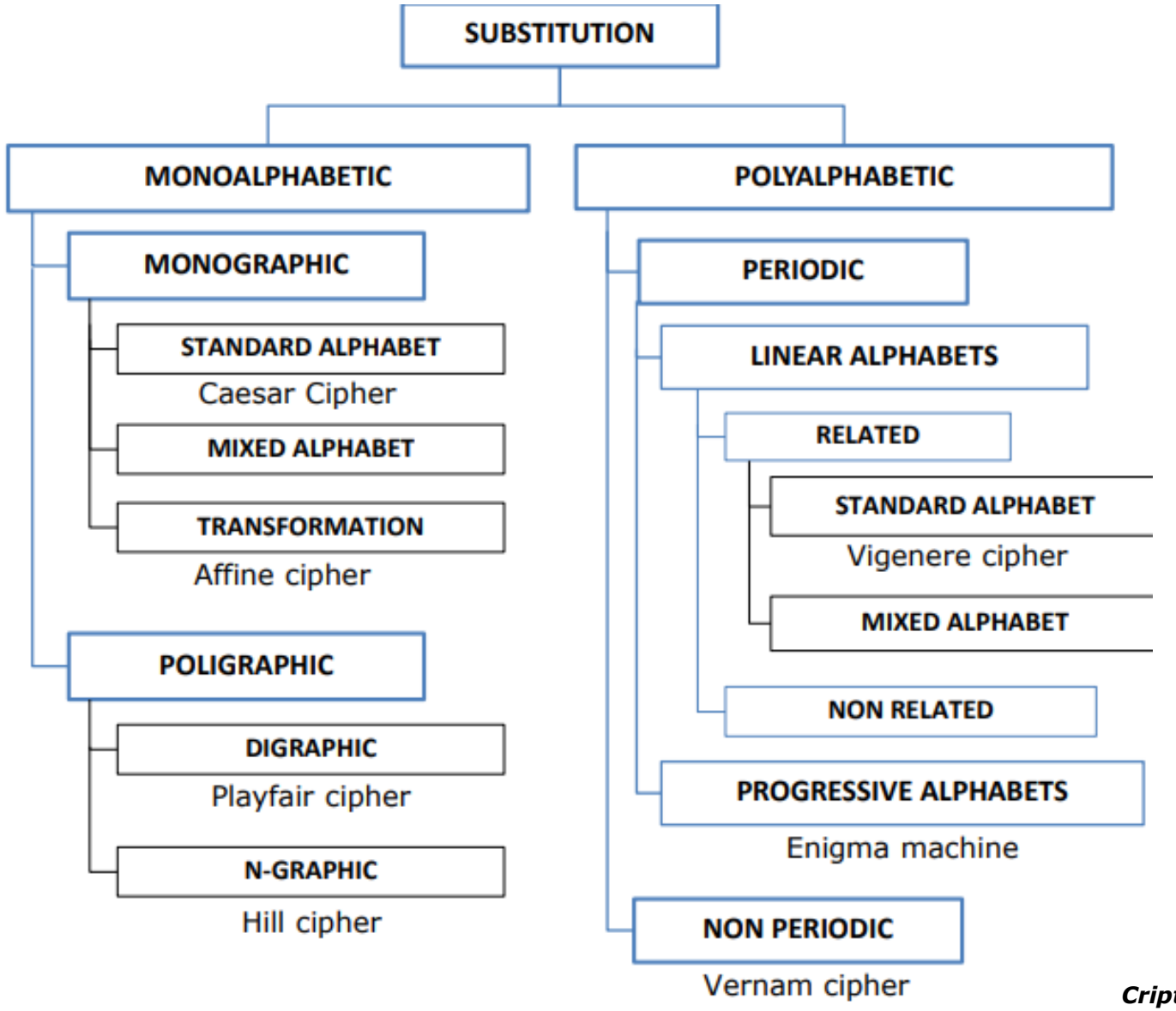
    - **Trasposición** (o permutación)
      - Todos los caracteres del texto plano aparecen en el texto cifrado, pero en diferente posición u orden, según un patrón determinado.

    - **Sustitución**
      - Cada carácter del texto plano se sustituye por otro carácter en el texto cifrado

Criptografía Clásica

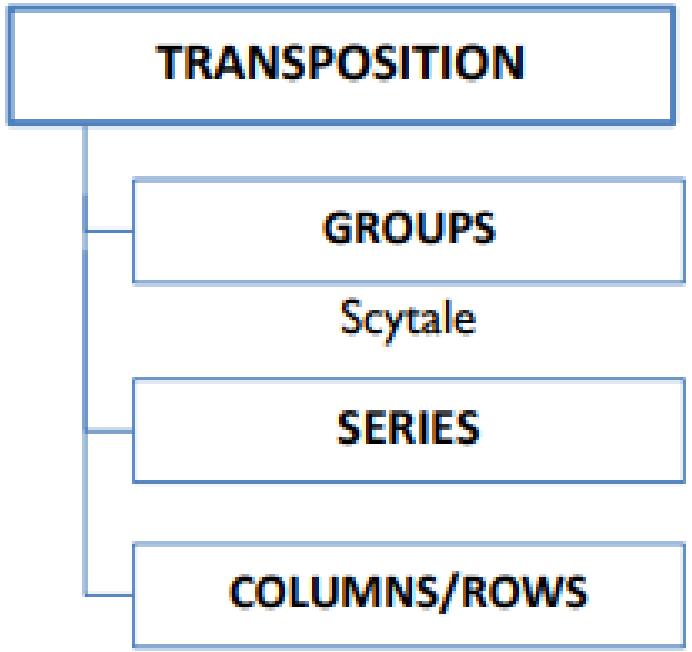
- **Clasificación**





Criptografía Clásica

- **Métodos de Trasposición**



Criptografía Clásica

- **Métodos de <u>trasposición</u>**

  - **Por grupos**
    - Las posiciones de las letras dentro de un mismo grupo se determinan por una función de permutación Π_p

  - **Por series**
    - Los caracteres del mensaje se ordenan según las posiciones determinadas por una cadena de sub-mensajes, conforme a un patrón o criterio determinado.

➢ La **frecuencia de repetición** de caracteres en el texto cifrado es la **misma** que en el texto plano

Criptografía Clásica

- **Métodos de trasposición <u>por grupos</u>**

  - El orden (posición en el mensaje cifrado) de las letras dentro de un mismo grupo (de longitud p) se determinan por una función de permutación Π_p

    - **EJEMPLO**: Π_p = 24531

      - M = BUENO SDIAS
      - C = UNOEB DASIS

- *Incrementando el periodo "p" se incrementa la seguridad del cifrado (menos vulnerable)*

Métodos de trasposición por series

- Los caracteres del mensaje se ordenan según las posiciones determinadas por una cadena de sub-mensajes, conforme a un patrón o criterio determinado.

  - **EJEMPLO**: $C = M_{S1}M_{S2}M_{S3}$
    - Siendo:
      - **M_{S1}** las posiciones pares, excepto las posiciones en número primo (4,6,8,10,12,14,16)
      - **M_{S2}** las posiciones impares, excepto las posiciones en número primo (1,9,15)
      - **M_{S3}** las posiciones en número primo (2,3,5,7,11,13,17)

        - M = BUENOSDIASEQUIPO!

        - **C = ??**

Métodos de trasposición por series

- **SOLUCIÓN**: C = $M_{S1}M_{S2}M_{S3}$
  - Siendo:
    - **M_{S1}** las posiciones pares, excepto las posiciones en número primo (4,6,8,10,12,14,16)
    - **M_{S2}** las posiciones impares, excepto las posiciones en número primo (1,9,15)
    - **M_{S3}** las posiciones en número primo (2,3,5,7,11,13,17)

➢ M = BUENOSDIASEQUIPO!

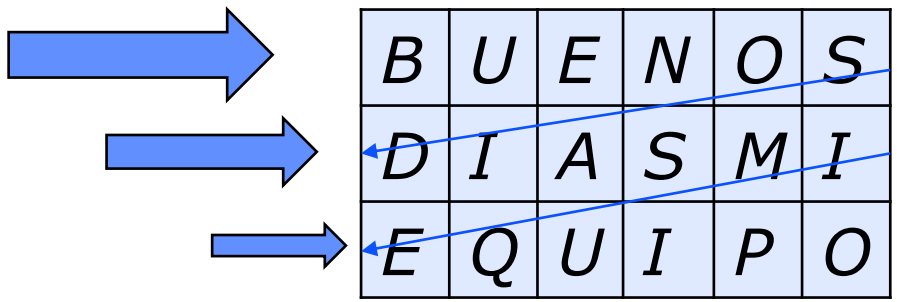
Pos:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
M	*B*	*U*	*E*	*N*	*O*	*S*	*D*	*I*	*A*	*S*	*E*	*Q*	*U*	*I*	*P*	*O*	*!*
M_{S1}				N		S		I		S		Q		I		O	
M_{S2}	B								A						P		
M_{S3}		U	E		O		D				E		U				!
C	*N*	*S*	*I*	*S*	*Q*	*I*	*O*	*B*	*A*	*P*	*U*	*E*	*O*	*D*	*E*	*U*	*!*

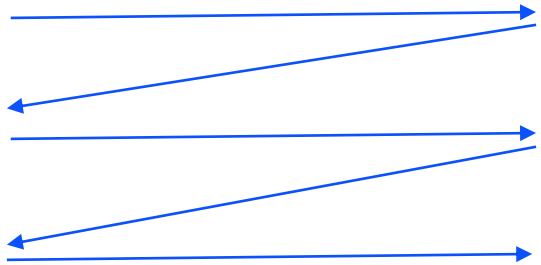
- **Métodos de trasposición <u>por filas / columnas</u>**

  - **ALGORITMO (CRITERIO):**

    - Los elementos **se introducen** según un patrón geométrico (por ejemplo, por filas)
    - Y se extraen según otro patrón (por ejemplo, por columnas)

Ejemplo: M = BUENOSDIASMIEQUIPO

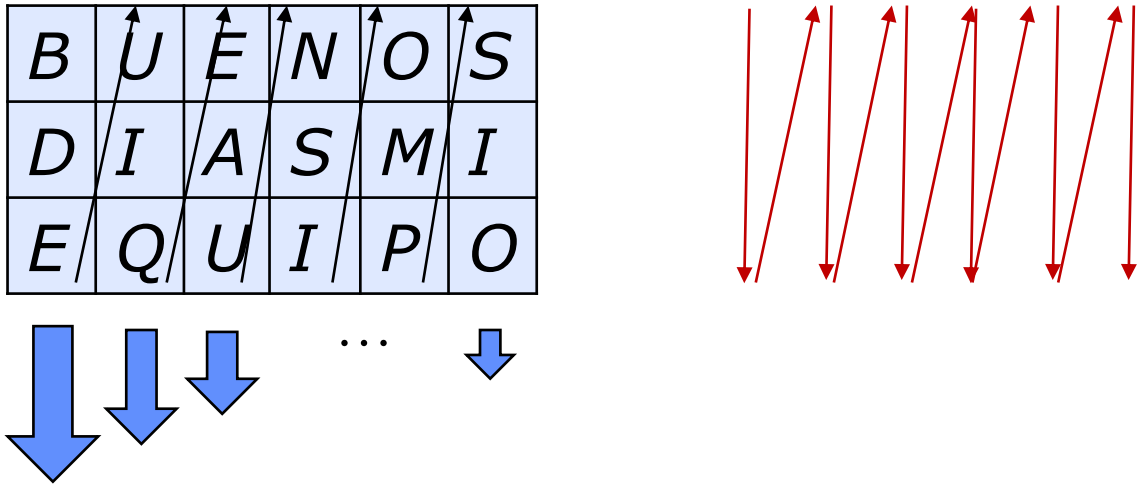




- **Métodos de trasposición <u>por filas / columnas</u>**

  - **ALGORITMO (CRITERIO):**
    - Los elementos se introducen según un patrón geométrico (por columnas)
    - Y **se extraen** según otro patrón (por ejemplo, por columnas)

Ejemplo: M = BUENOSDIASMIEQUIPO

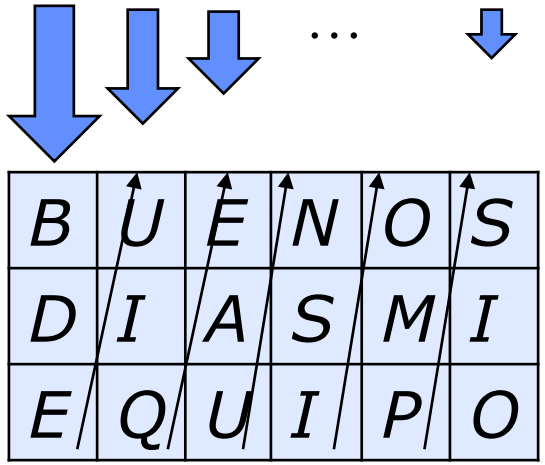


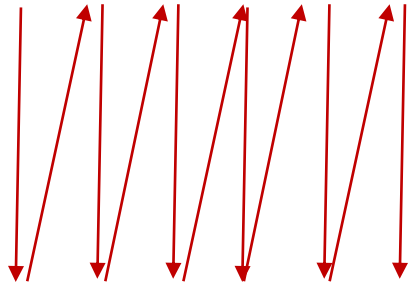
Cifrado: C = BDEUIQEAUNSIOMPSIO

- **Métodos de trasposición <u>por filas / columnas</u>**

  - **DESCIFRADO:**
    - **Se invierten los patrones**
  - Para el ejemplo anterior:
    - Los elementos **se introducen** por columnas (según el ejemplo)
    - Y **se extraen por filas (por columnas)**

Cifrado: C = BDEUIQEAUNSIOMPSIO

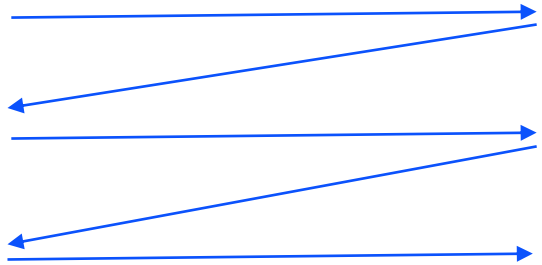




- **Métodos de trasposición por filas / columnas**

  - **DESCIFRADO:**
    - **Se invierten los patrones**
  - Para el ejemplo anterior:
    - Los elementos **se introducen por** columnas (según el ejemplo)
    - Y **se extraen por filas** (por columnas)

B	U	E	N	O	S
D	I	A	S	M	I
E	Q	U	I	P	O



M = BUENOSDIASMIEQUIPO

Criptografía Clásica

- **Métodos** de cifrado clásico

  Sustitución

  - Cada carácter del alfabeto del texto plano se sustituye por otro carácter del alfabeto del texto cifrado, según una función o algoritmo.

Criptografía Clásica

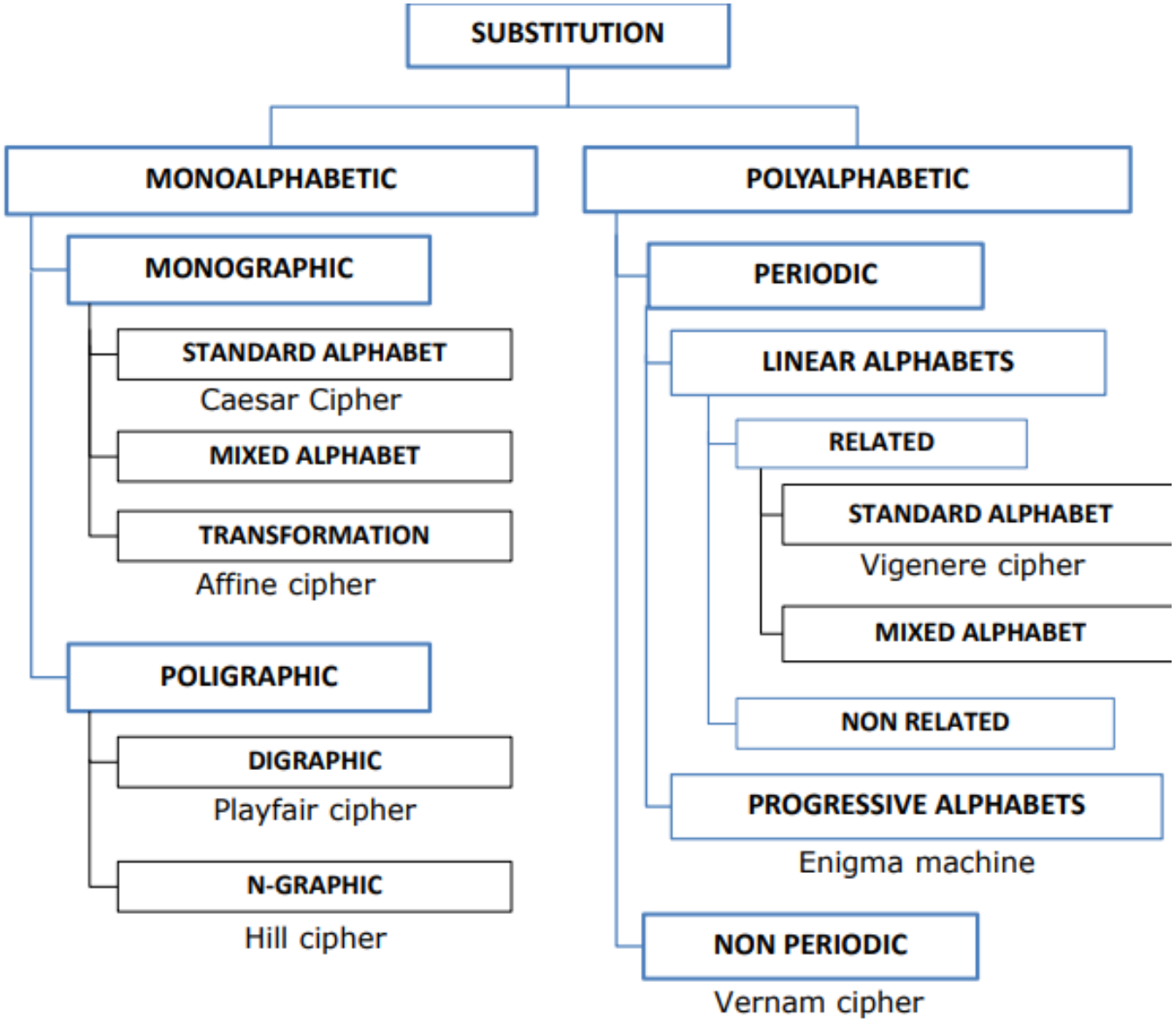
- **Métodos de <u>sustitución</u>**

  - Se define **alfabeto** como el conjunto de símbolos o caracteres utilizados.
    - Alfabeto para el texto plano
    - Alfabeto para el texto cifrado

  - Se suele emplear una conversión **numérica** para cada símbolo o carácter del alfabeto
    - para poder hacer operaciones matemáticas con ellos
    - *Ejemplo: A=0; B=1; C=2;… Z=25*

Criptografía Clásica

- **Clasificación**



Criptografía Clásica

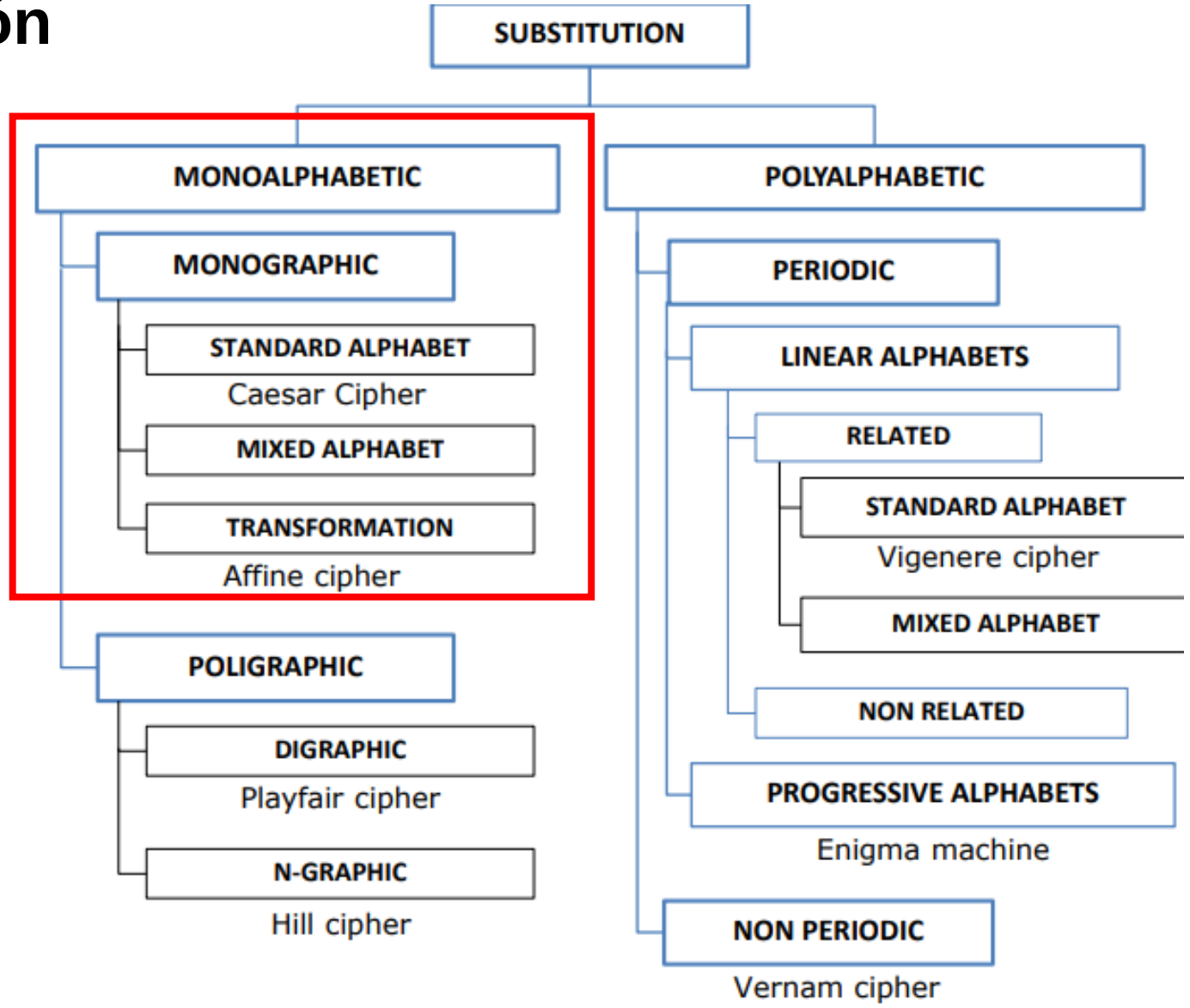
- **Métodos de sustitución**

  - **Monoalfabéticos**
    - Se sustituye un caracter del alfabeto del texto original por un carácter del alfabeto del texto cifrado

  - **Polialfabéticos**
    - La sustitución de un carácter del alfabeto del texto original se corresponde con un caracter de uno de los posibles alfabetos del texto cifrado.

Criptografía Clásica

- **Clasificación**



Criptografía Clásica

- **Métodos de <u>sustitución monoalfabéticos</u>**
  - Se sustituye un caracter del alfabeto del texto original por un carácter del alfabeto del texto cifrado
  - ***Ejemplo***, para alfabeto británico de 26 caracteres (n=26)
    - Existen **n! diferentes alfabetos** para el texto cifrado

Criptografía Clásica

- **Métodos de sustitución monoalfabéticos**
  - Se sustituye un caracter del alfabeto del texto original por un carácter del alfabeto del texto cifrado
  - ***Expresión general del cifrador afín para sustitución monoalfabética:***

$$C(m_i) = (a \cdot m_i + b) \bmod n$$

Sólo si: mcd (a,n) = 1 (coprimos!!)

- Siendo:
  - m_i = valor numérico del carácter *m* en la posición "*i*" del texo plano (mensaje)
  - *a* = constante de diezmado
  - *b* = constante de desplazamiento

  } $Clave = \{a,b\}$
  - *n* = número de elementos en el alfabeto (módulo)
  - $C(m_i)$ = valor numérico correspondiente al carácter *m* en la posición "*i*" del texto cifrado.

- **Métodos de <u>sustitución monoalfabéticos</u>**
  - Casos particulares:

➢ Cifrador **CAESAR**: *a = 1, b = 3*

$$C(m_i) = (m_i + 3) \bmod n$$

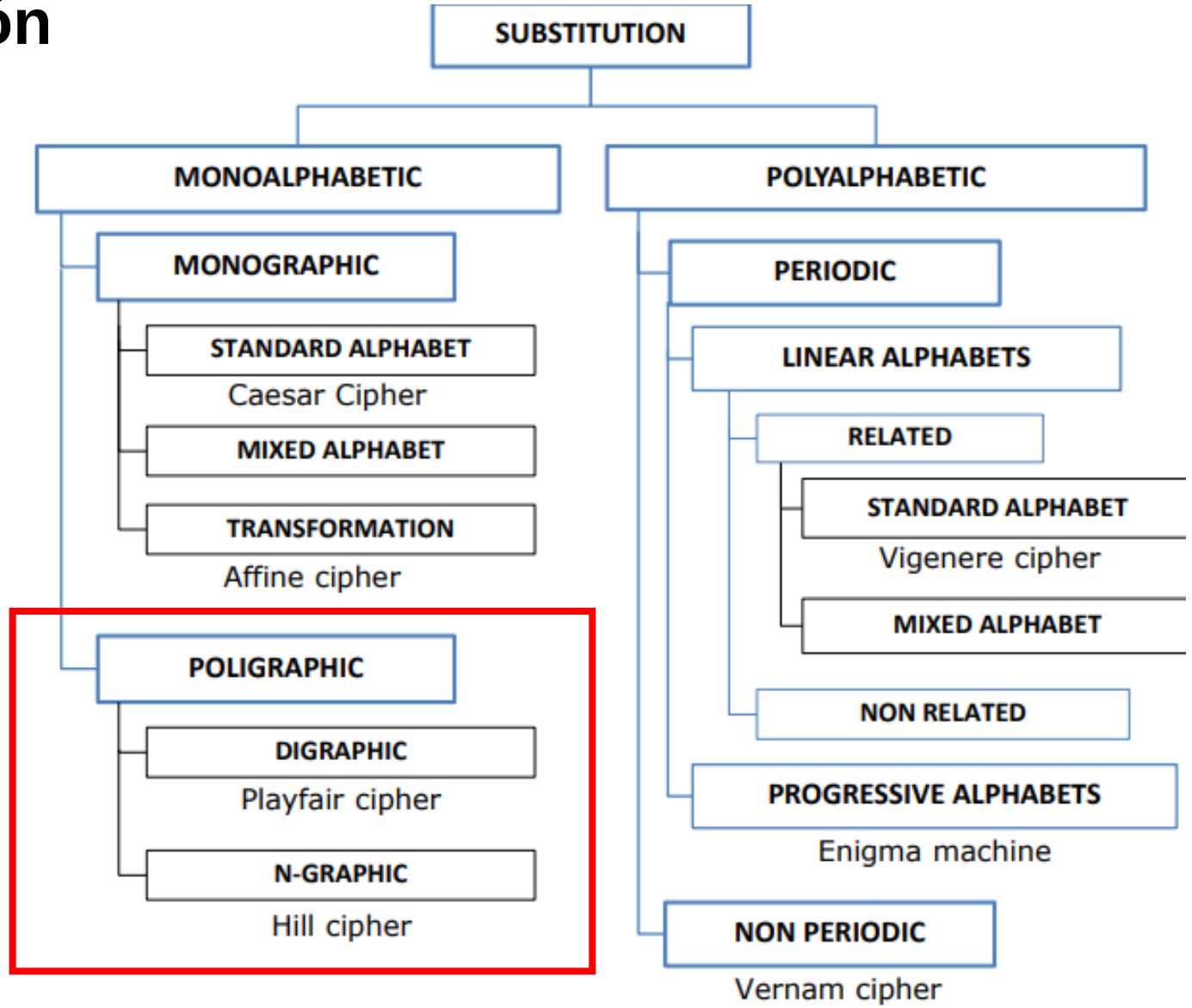
➢ Cifrador **ROT13**: *a = 1, b = 13*

$$C(m_i) = (m_i + 13) \bmod n$$

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

Criptografía Clásica

- **Clasificación**



Criptografía Clásica

- **Métodos de sustitución monoalfabéticos (poligráficos)**

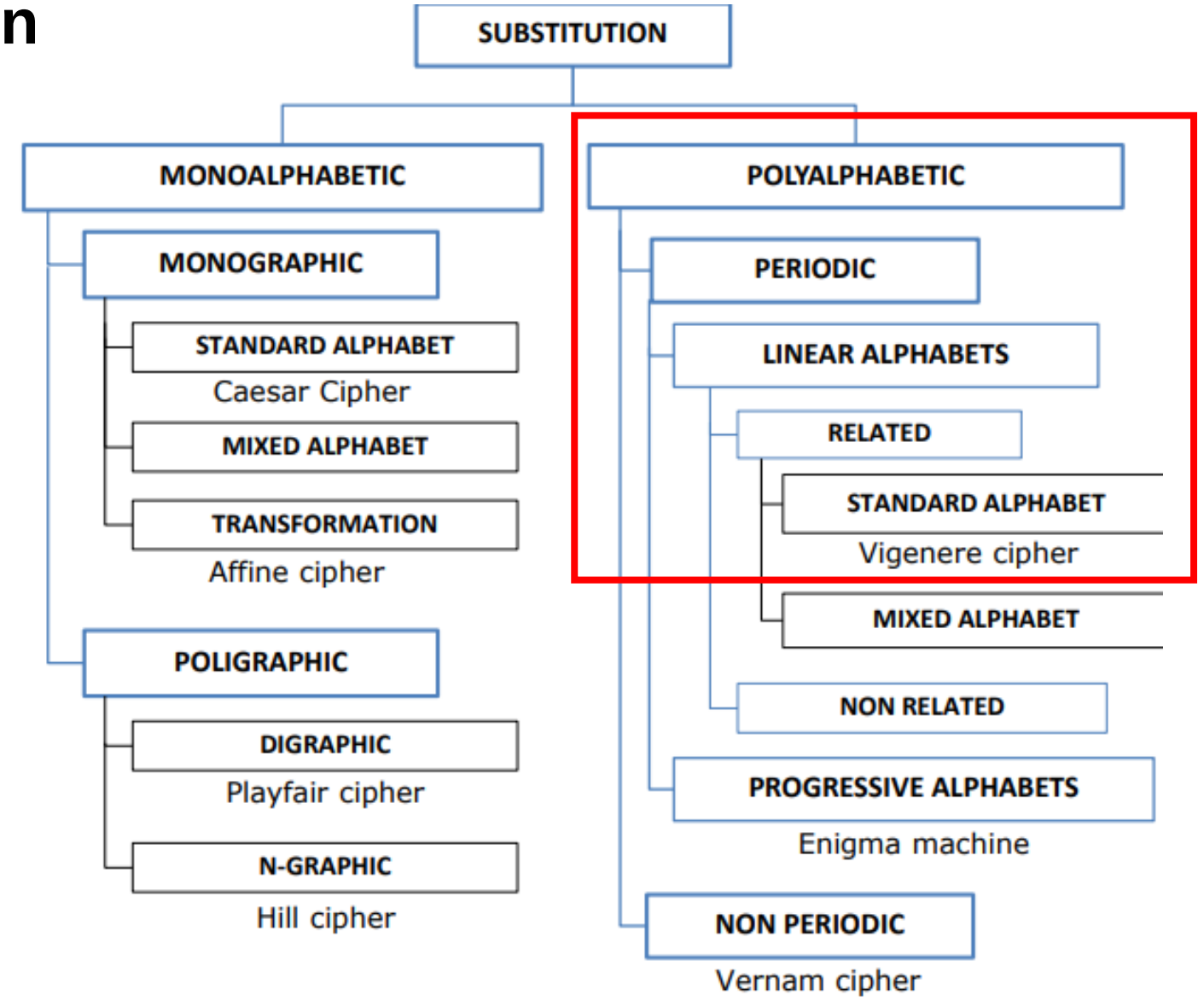
  - **PlayFair**

    - Se sustituyen **dígrafos**, no caracteres individuales
    - Reglas sencillas:
      - Misma fila → se toman los caracteres según desplazamiento a la derecha
      - Misma columna → se toman los caracteres según desplazamiento hacia abajo
      - Rectángulo → se toman los caracteres de la diagonal opuesta
      - Carácter de relleno (normalmente, la “X”), para:
        - Padding
        - Separar letras dobles

    - *https://www.youtube.com/watch?v=UURjVI5cw4g*

Criptografía Clásica

- **Clasificación**



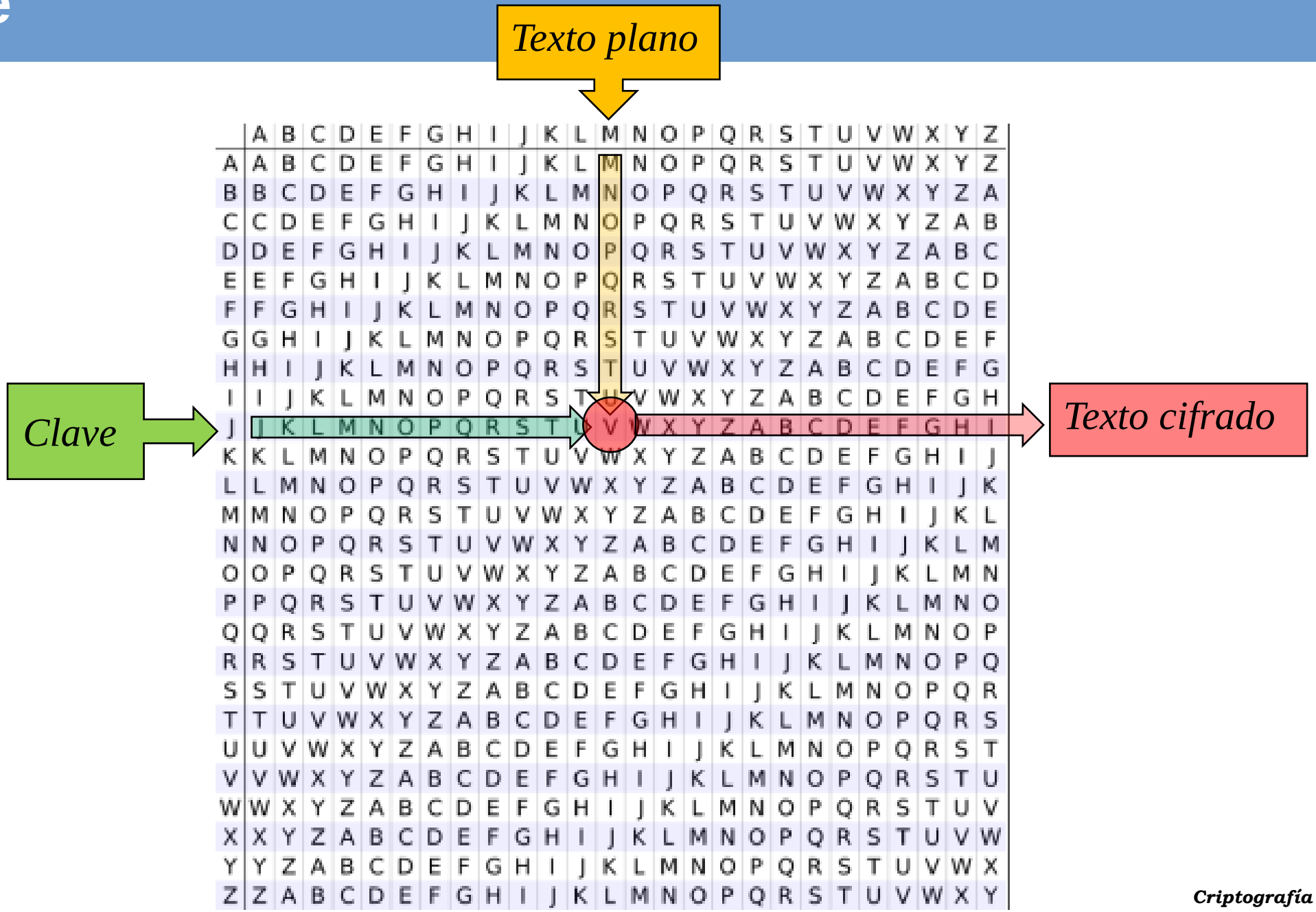
- **Métodos de sustitución polialfabéticos**
  - La sustitución de un carácter del alfabeto del texto original se corresponde con un caracter de **uno de los posibles alfabetos** del texto cifrado
  - ***Ejemplo***, ***Vigenere***

$$C(m_j) = (m_j + k_{(j \bmod n)}) \bmod 26$$

    - para alfabeto británico de 26 caracteres (n=26) → Existen **26 diferentes sustituciones de monoalfabetos**
  - Siendo:
    - m = longitud de la clave
    - k_j = desplazamiento para el alfabeto j
    - m_j = carácter en la posición j del texto plano
    - $C(m_j)$ = valor cifrado del carácter en la posición mj del texto plano

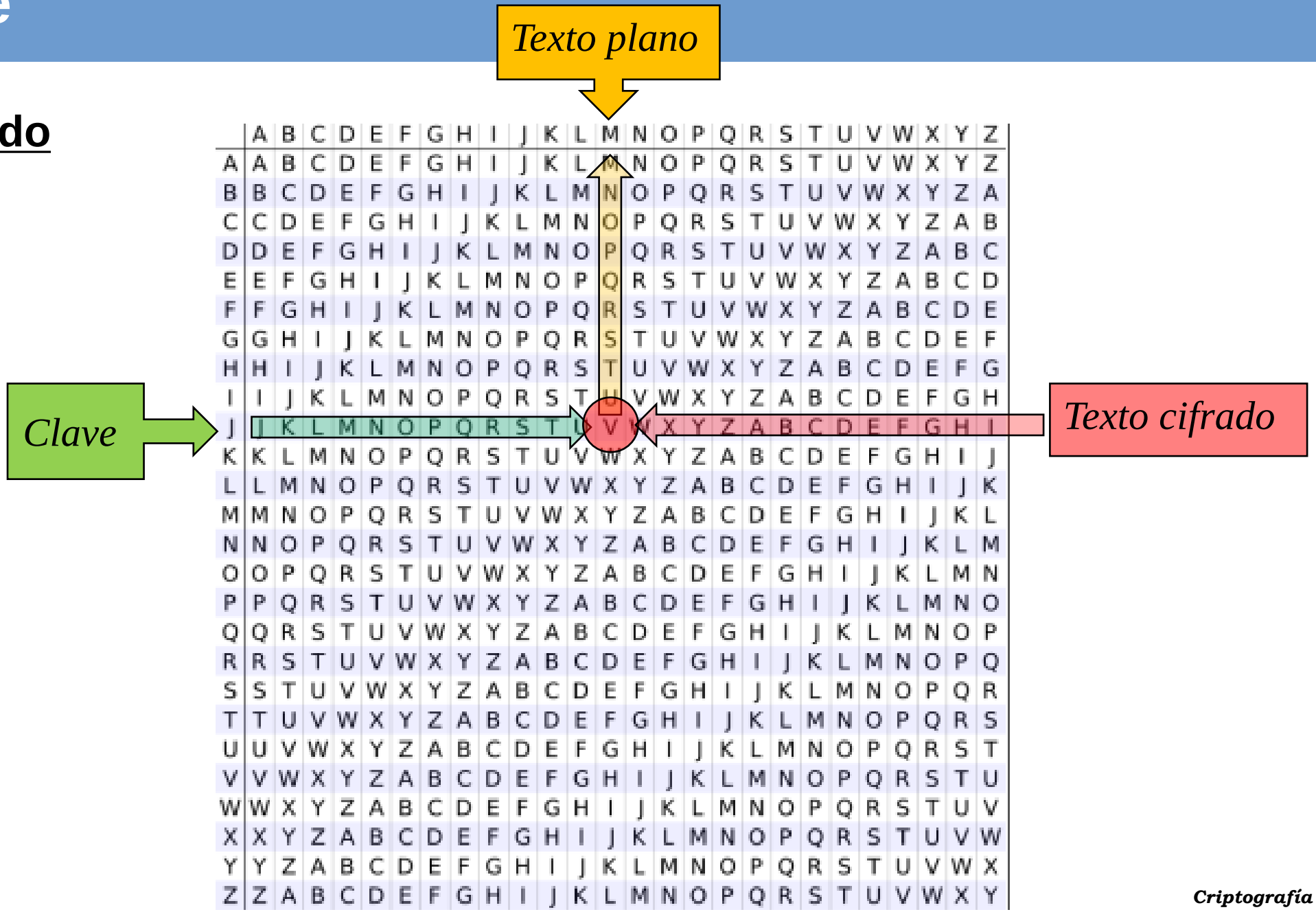
Vigenere

Cifrado



Vigenere

Descifrado



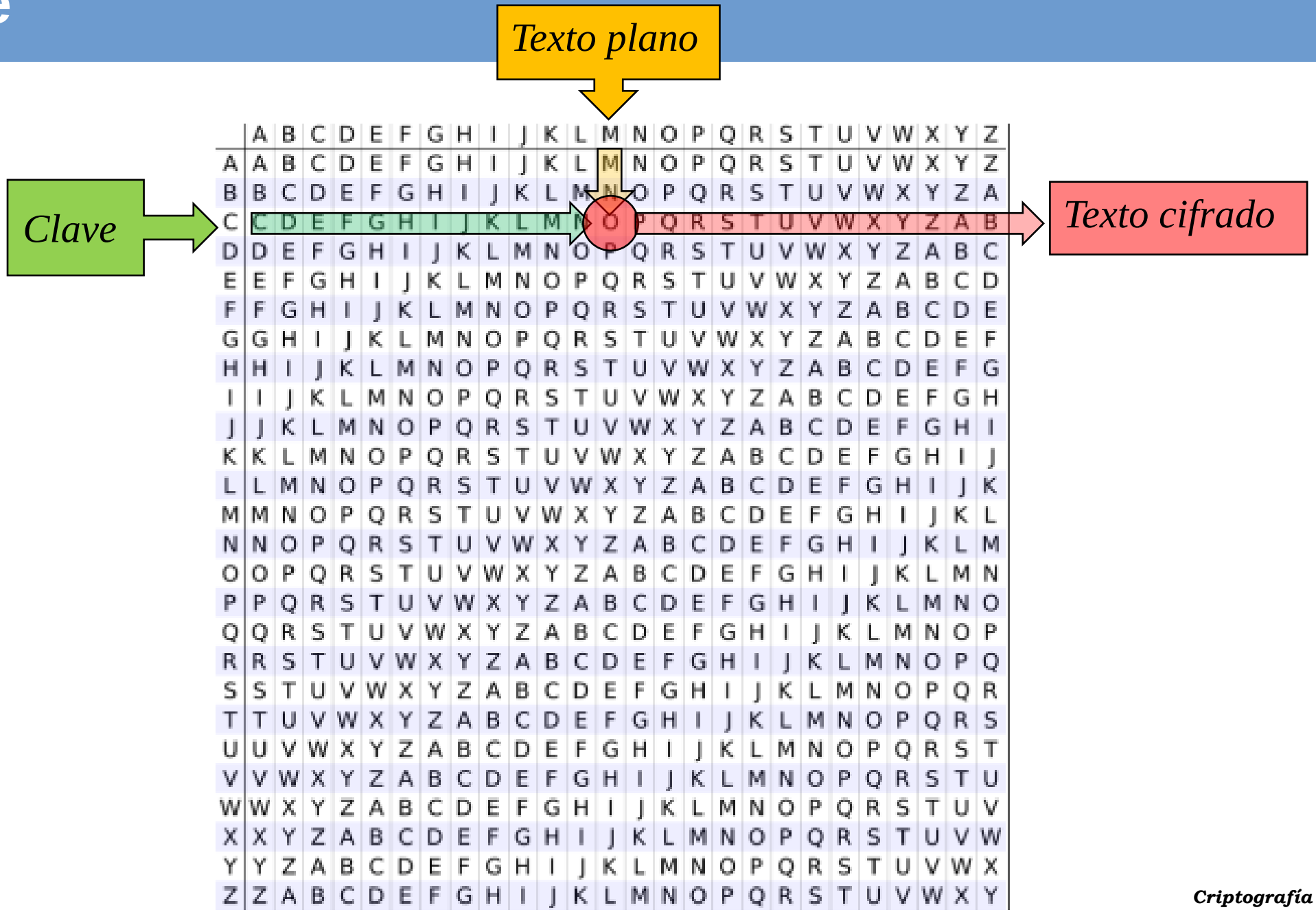
Vigenere

Ejemplo

Texto plano	***M***	*E*	*N*	*S*	*A*	*J*	*E*	*U*	*N*	*O*
Clave	***C***	*L*	*A*	*V*	*E*	*C*	*L*	*A*	*V*	*E*
Texto cifrado	***?***	*?*	*?*	*?*	*?*	*?*	*?*	*?*	*?*	*?*

Vigenere

Cifrado



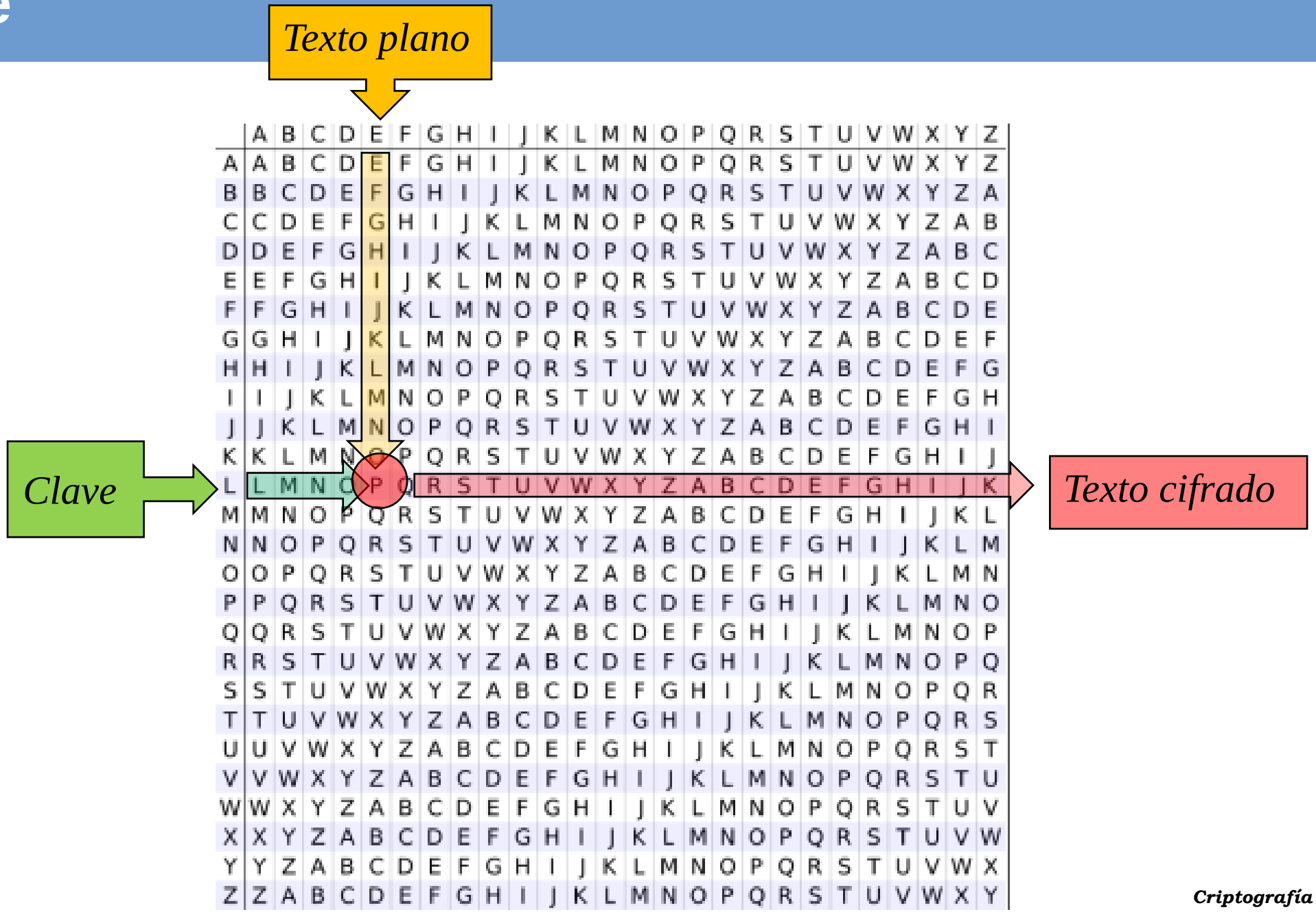
Vigenere

Ejemplo

Texto plano	***M***	*E*	*N*	*S*	*A*	*J*	*E*	*U*	*N*	*O*
Clave	***C***	*L*	*A*	*V*	*E*	*C*	*L*	*A*	*V*	*E*
Texto cifrado	***O***	*?*	*?*	*?*	*?*	*?*	*?*	*?*	*?*	*?*

Vigenere

Cifrado



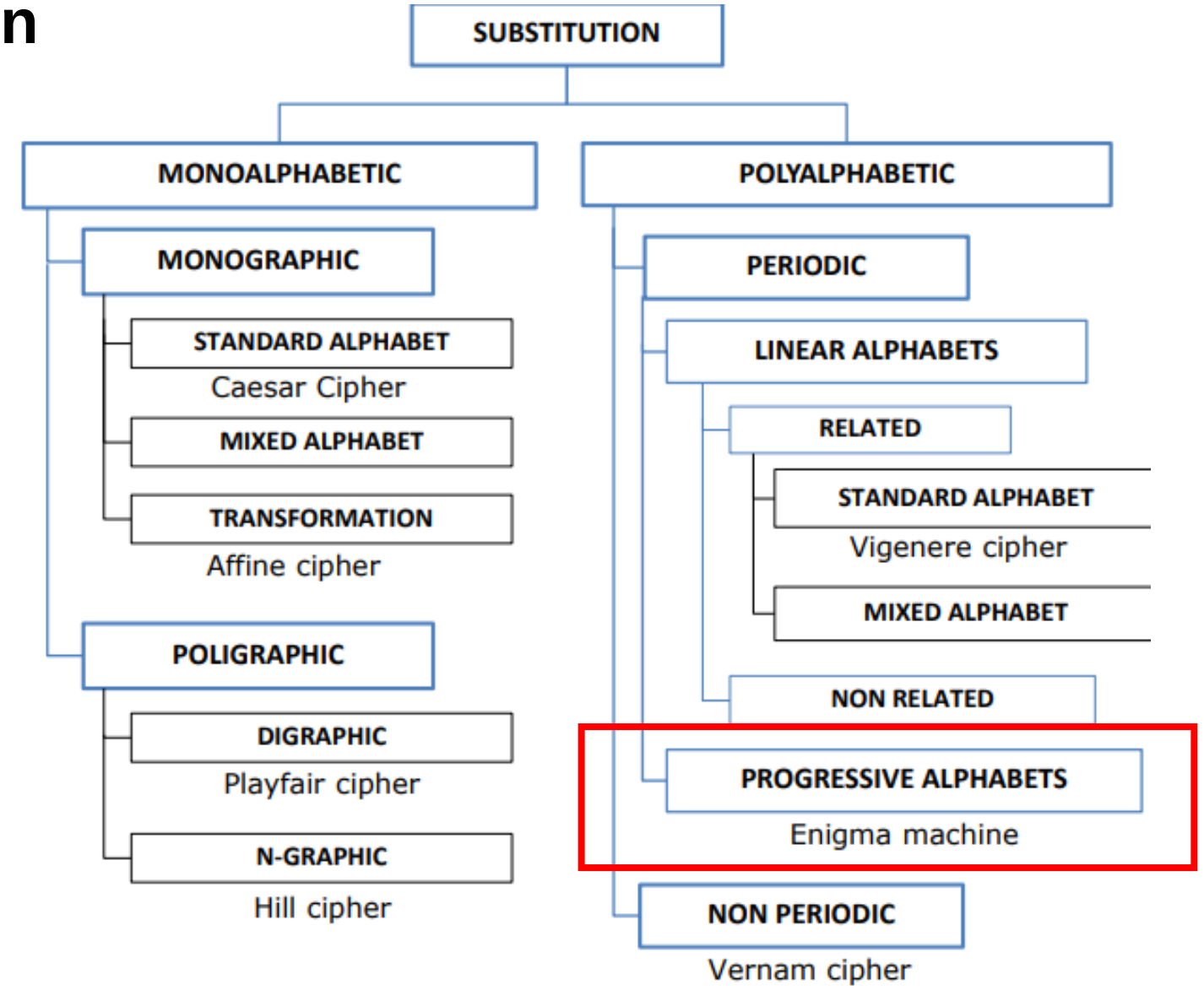
Vigenere

Ejemplo

Texto plano	***M***	***E***	*N*	*S*	*A*	*J*	*E*	*U*	*N*	*O*
Clave	***C***	***L***	*A*	*V*	*E*	*C*	*L*	*A*	*V*	*E*
Texto cifrado	***O***	***P***	*?*	*?*	*?*	*?*	*?*	*?*	*?*	*?*

Criptografía Clásica

- **Clasificación**

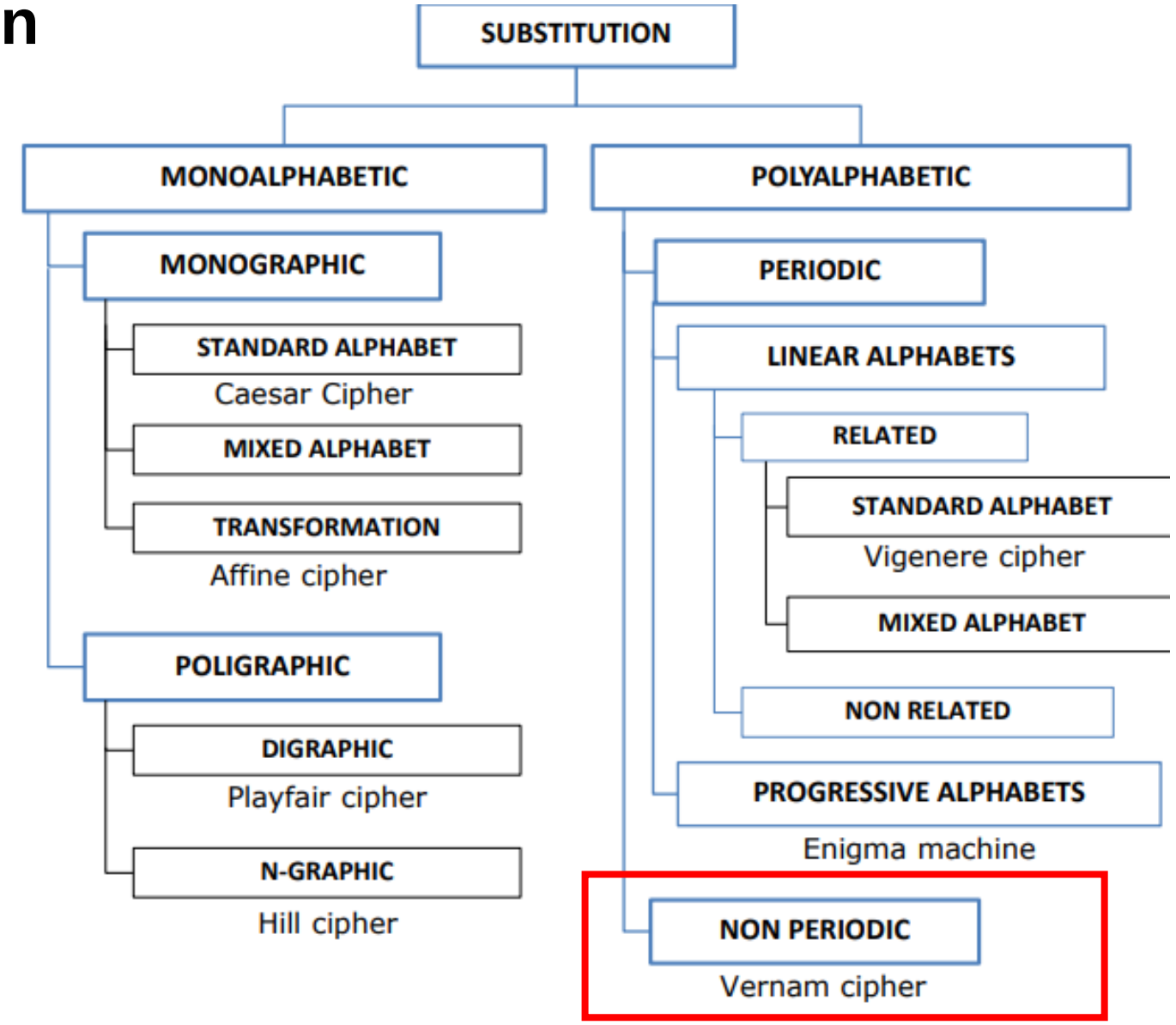


Máquina Enigma

Ejemplo de Sustitución Polialfabética Progresiva

Criptografía Clásica

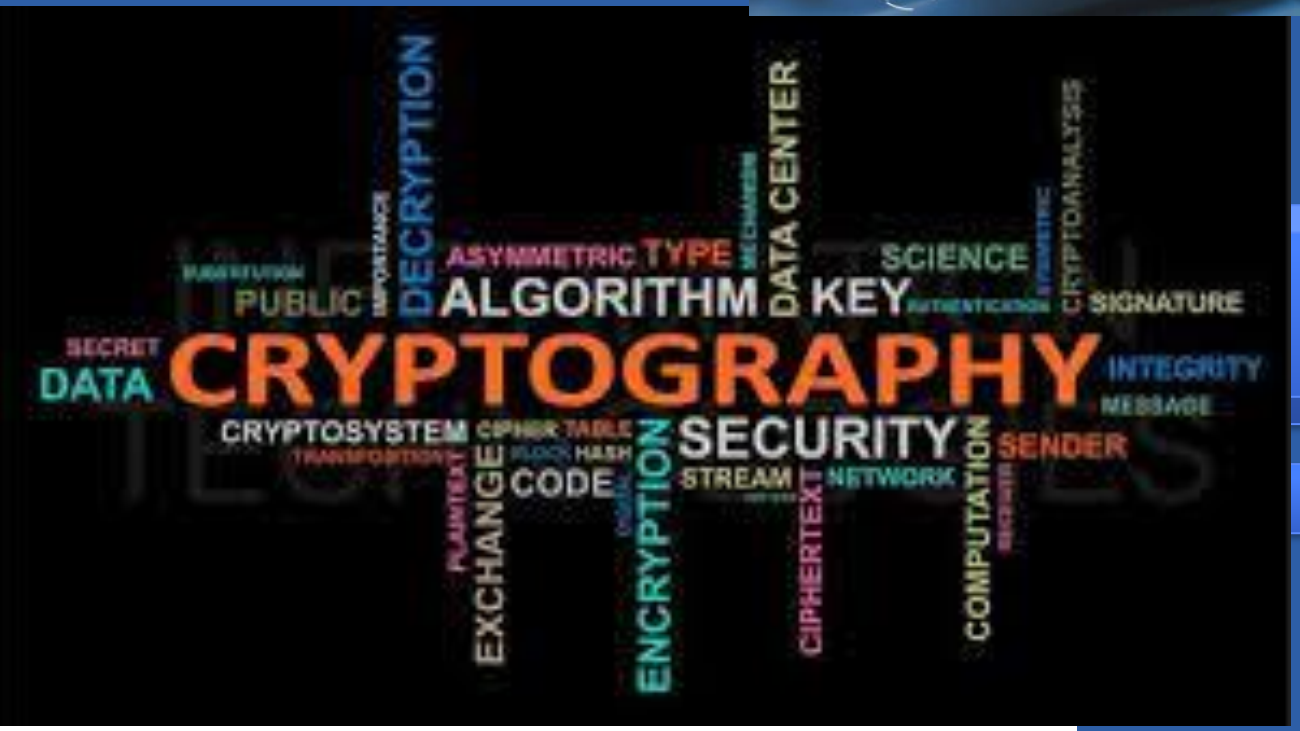
- **Clasificación**

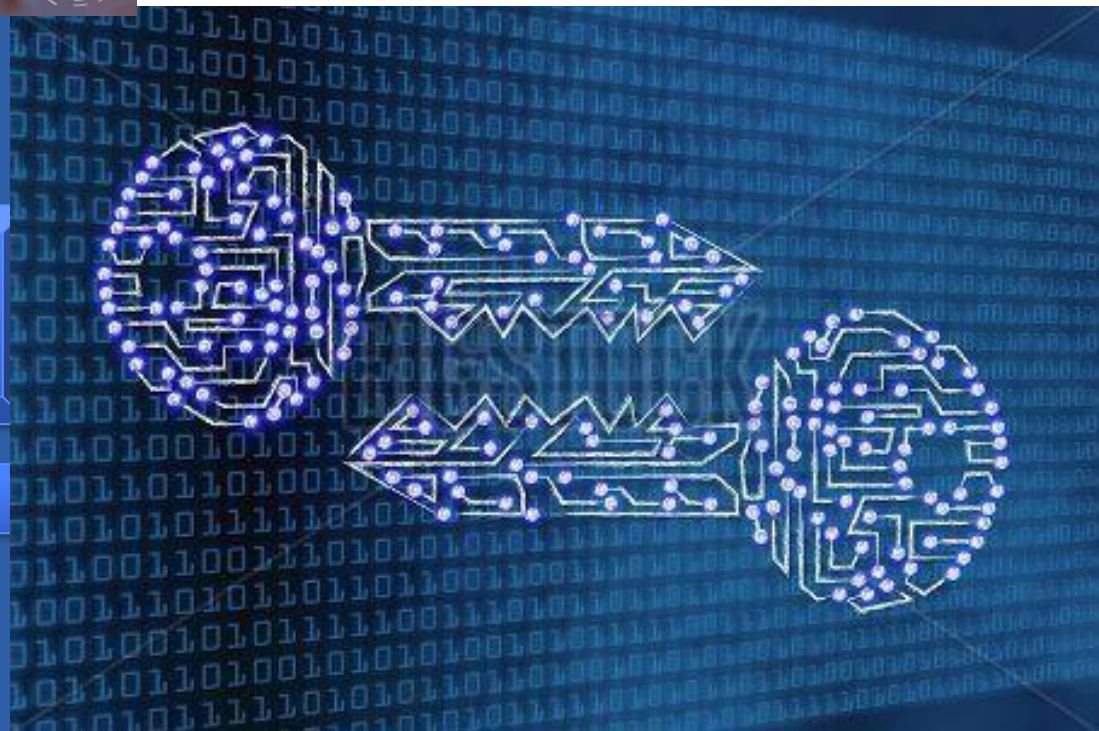


Criptografía

Universidad Francisco de Vitoria
UFV Madrid

Tema 1.3
Criptoanálisis





Criptografía Clásica

- **Criptoanálisis**

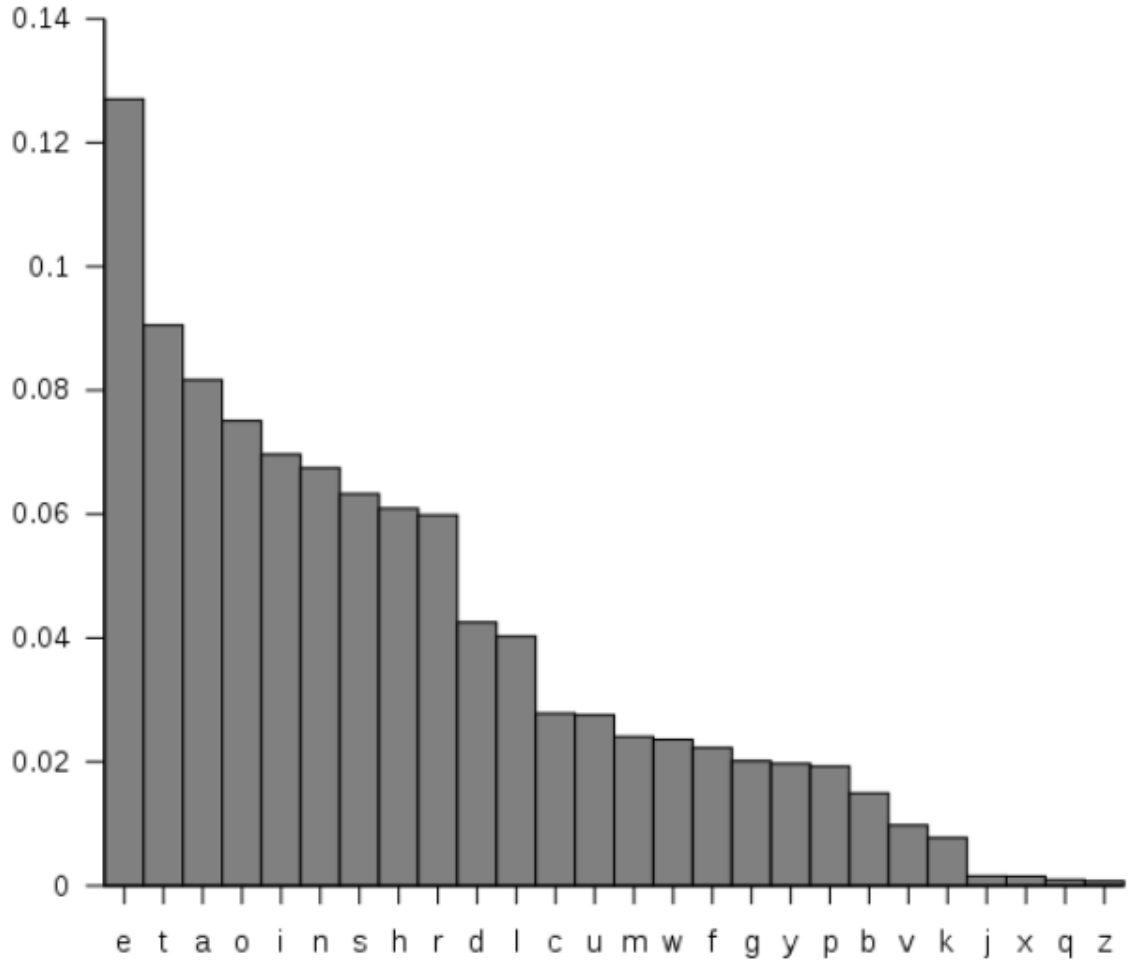
  - ámbito de la **criptología** que se ocupa de las técnicas para romper códigos cifrados y criptosistemas, en particular de obtener métodos más eficientes que una búsqueda por fuerza bruta.

  - Busca acceder a la información (texto plano), incluso si la clave de cifrado / descifrado no es conocida.

- **Criptoanálisis. Herramientas / Técnicas útiles:**

  - **<u>Análisis de frecuencia</u>**

    - *Ejemplo: idioma inglés*



- **Criptoanálisis. Herramientas / Técnicas útiles:**

  - **Patrones de repetición idiomáticos**

    - *Ejemplo: idioma inglés*

Common pairs	TH, EA, OF, TO, IN, IT, IS, BE, AS, AT, SO, WE, HE, BY, OR, ON, DO, IF, ME, MY, UP
Common repeated letters	SS, EE, TT, FF, LL, MM and OO
Common triplets	THE, EST, FOR, AND, HIS, ENT or THA

- **Criptoanálisis. Herramientas / Técnicas útiles:**

  - **Método KASISKY**

    - Para cifradores de sustitución polialfabéticos

    - Pasos:
      - Estimar la longitud de la clave (buscando cadenas repetidas)
      - Obtención de sub-criptogramas
      - Análisis de frecuencia para cada sub-criptograma

Criptografía Clásica

- **Criptoanálisis. Herramientas / Técnicas útiles:**

  - **<u>Método KASISKY</u>.** ***Ejemplo:***

```
OOEXQGHXINMFRTRIFSSMZRWLYOWTTWTJIWMOBEDAXHVHSFTRIQKMENXZ
PNQWMCVEJTWJTOHTJXWYIFPSVIWEMNUVWHMCXZTCLFSCVNDLWTENUHSY
KVCTGMGYXSYELVAVLTZRVHRUHAGICKIVAHORLWSUNLGZECLSSSWJLSKO
GWVDXHDECLBBMYWXHFAOVUVHLWCSYEVVWCJGGQFFVEOAZTQHLONXGAHO
GDTERUEQDIDLLWCMLGZJLOEJTVLZKZAWRIFISUEWWLIXKWNISKLQZHKH
WHLIEIKZORSOLSUCHAZAIQACIEPIKIELPWHWEUQSKELCDDSKZRYVNDLW
TMNKLWSIFMFVHAPAZLNSRVTEDEMYOTDLQUEIIMEWEBJWRXSYEVLTRVGJ
KHYISCYCPWTTOEWANHDPWHWEPIKKODLKIEYRPDKAIWSGINZKZASDSKTI
TZPDPSOILWIERRVUIQLLHFRZKZADKCKLLEEHJLAWWVDWHFALOEOQW
```

Método KASISKY. *Ejemplo:*

```
OOEXQGHXINMFRTRIFSSMZRWLYOWTTWTJIWMOBEDAXHVHSFTRIQKMENXZ
PNQWMCVEJTWJTOHTJXWYIFPSVIWEMNUVWHMCXZTCLFSCVNDLWTENUHSY
KVCTGMGYXSYELVAVLTZRVHRUHAGICKIVAHORLWSUNLGZECLSSSWJLSKO
GWVDXHDECLBBMYWXHFAOVUVHLWCSYEVVWCJGGQFFVEOAZTQHLONXGAHO
GDTERUEQDIDLLWCMLGZJLOEJTVLZKZAWRIFISUEWWLIXKWNISKLQZHKH
WHLIEIKZORSOLSUCHAZAIQACIEPIKIELPWHWEUQSKELCDDSKZRYVNDLW
TMNKLWSIFMFVHAPAZLNSRVTEDEMYOTDLQUEIIMEWEBJWRXSYEVLTRVGJ
KHYISCYCPWTTOEWANHDPWHWEPIKKODLKIEYRPDKAIWSGINZKZASDSKTI
TZPDPSOILWIERRVUIQLLHFRZKZADKCKLLEEHJLAWWVDWHFALOEOQW
```

Pasos:

1. Cadenas repetidas → SYE, ZKZA
2. Determinar la **distancia** entre repeticiones
3. Hipótesis: la **longitud de la clave** es el **divisor** de las distancias más repetido

$196-122 = 2 \cdot 37$
$383-196 = 11 \cdot 17$
$383-122 = 9 \cdot 29$
$439-252 = 11 \cdot 17$
$472-439 = 3 \cdot 11$
$472-252 = 22 \cdot 5 \cdot 11$

Método KASISKY. *Ejemplo:*

Pasos:

4. Dividir en fragmentos de la longitud (estimada) de la clave

```
1   OOEXQGHXINM FRTRIFSSMZR WLYOWTTWTJI WMOBEDAXHVH
2   SFTRIQKMENX ZPNQWMCVEJT WJTOHTJXWYI FPSVIWEMNUV
3   WHMCXZTCLFS CVNDLWTENUH SYKVCTGMGYX SYELVAVLTZR
4   VHRUHAGICKI VAHORLWSUNL GZECLSSSWJL SKOGWVDXHDE
5   CLBBMYWXHFA OVUVHLWCSYE VVWCJGGQFFV EOAZTQHLONX
6   GAHOGDTERUE QDIDLLWCMLG ZJLOEJTVLZK ZAWRIFISUEW
7   WLIXKWNISKL QZHKHWHLIEI KZORSOLSUCH AZAIQACIEPI
8   KIELPWHWEUQ SKELCDDSKZR YVNDLWTMNKL WSIFMFVHAPA
9   ZLNSRVTEDEM YOTDLQUEIIM EWEBJWRXSYE VLTRVGJKHYI
10  SCYCPWTTOEW ANHDPWHWEPI KKODLKIEYRP DKAIWSGINZK
11  ZASDSKTITZP DPSOILWIERR VUIQLLHFRZK ZADKCKLLEEH
12  JLAWWVDWHFA LOEOQW
```

5. Extraer sub-pictogramas (letras del mismo color)
6. Análisis de frecuencias para cada sub-pictograma

Criptografía

Universidad Francisco de Vitoria
UFV Madrid

Tema 2
Criptografía Clásica