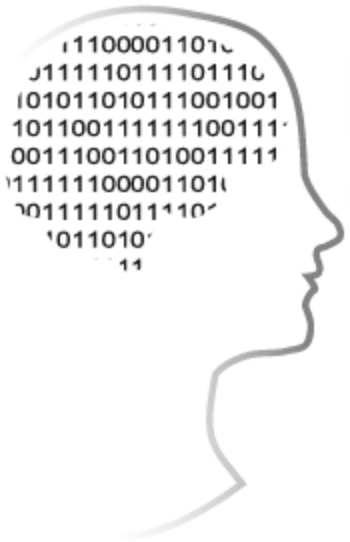
Lección 1: Historia de la criptografía y su desarrollo en Europa



intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Arturo Ribagorda Garnacho
arturo@inf.uc3m.es

Universidad Carlos III de Madrid
Catedrático de Universidad

Grecia clásica. Desarrollo del cifrado

- Homero. La Ilíada.
  - Título VI.
- Heródoto. Los Nueve Libros de la Historia.
  - Título V. Histeio.
  - Título VII. Demarato.

Tablilla encerada

Tablilla encerada (Mural. Pompeya)

Criptografía: método César

- […] Para los negocios secretos utilizaba una manera de cifra que hacía el sentido ininteligible, estando ordenadas las letras de manera que no podía formarse ninguna palabra; para descifrarlas tiene que cambiarse el orden de las letras, tomando la cuarta por la primera, esto es “d” por “a”, y así las demás […]

Suetonio (69 - 140). Doce Césares.

Métodos de cifrado

- Sustitución.
- Permutación (Transposición).
- Producto (Supercifrado o Recifrado).

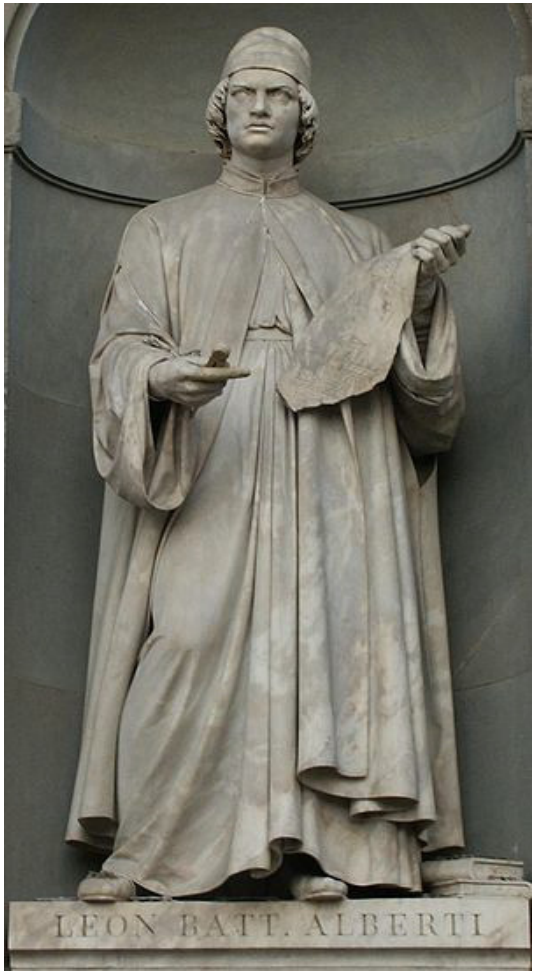
Frecuencia de las letras (%) en español

e	a	o	l	s	n	d	r	u	i
16,78	11,96	8,69	8,37	7,88	7,01	6,87	4,94	4,80	4,15

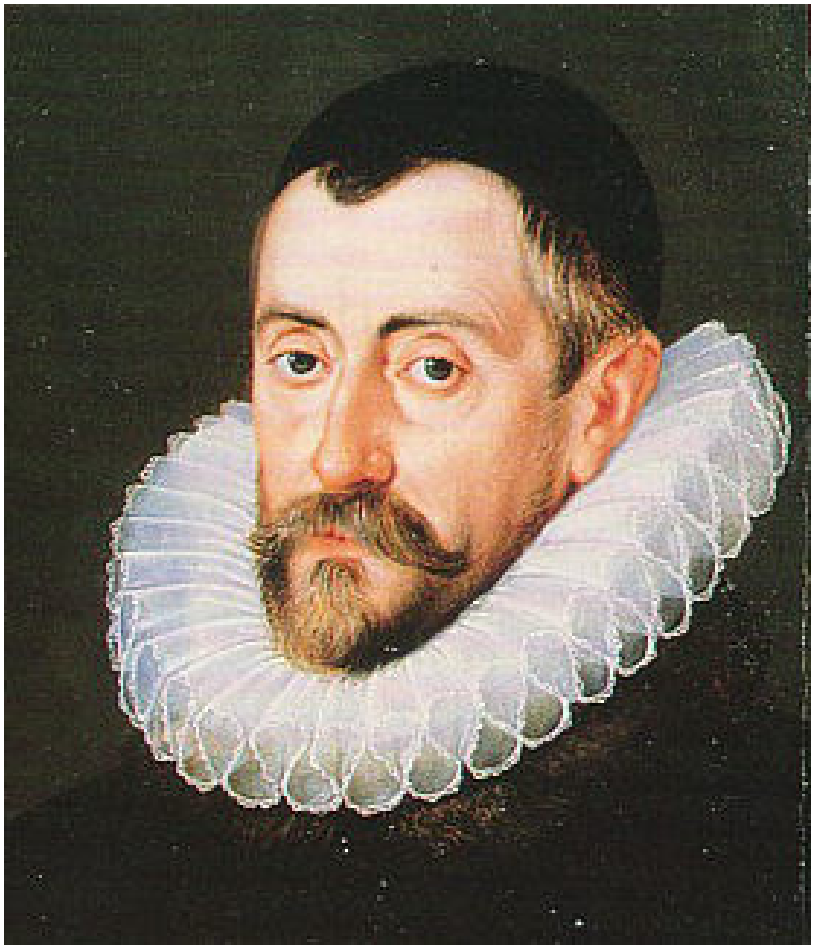
t	c	p	m	y	q	b	h	g	f
3,31	2,92	2,77	2,12	1,54	1,53	0,92	0,89	0,73	0,52

v	j	ñ	z	x	k	w
4,80	4,15	3,31	2,92	0,06	0,00	0,00

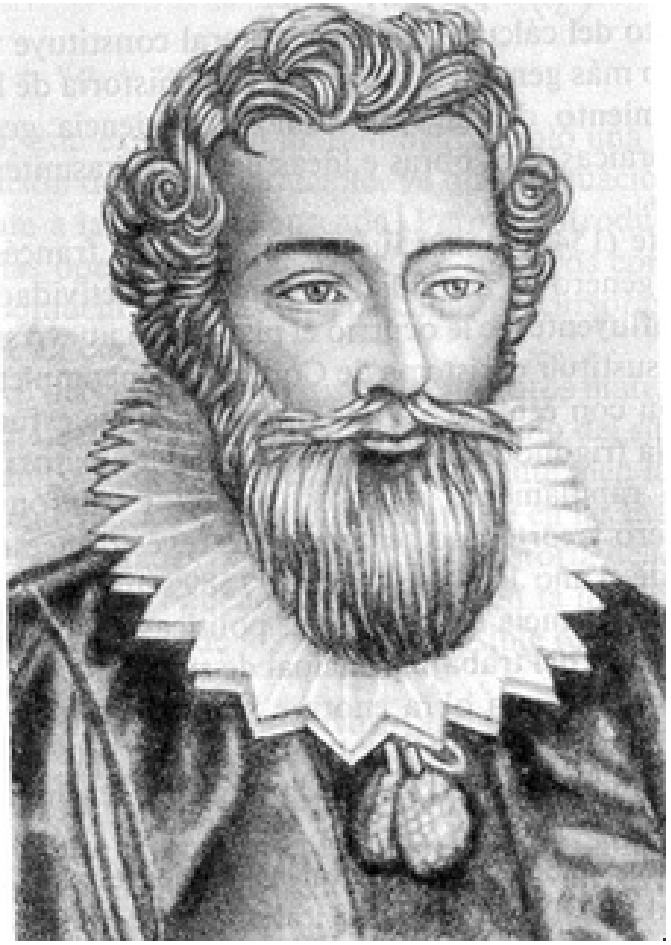
Leone Battista Alberti.
Galleria degli Ufficci (Florencia)



Francis Walsinghan (1530 - 1590)



François Viète (1540 – 1603)



Felipe II. Tipos de cifra (1)

- Las cosas que se ofrecieren en secreto las habéis de escribir en cifra y para ello se os ha dado la general que yo tengo con todos mis ministros y otra particular para cuando se ofreciere negocio de tanto secreto que convenga servir por ella y no por la general.
- Instrucción de Felipe II a Diego Guzmán de Silva, Embajador en Venecia.

Los Espías de Felipe II. Carnicer. C., Marcos, J. La Esfera de los Libros, 2005.

Felipe II. Tipos de cifra (2)

- Algunas veces ofrécense negocios tan graves e importantes y de tanto secreto que no será bueno escribirlas en cifra general, se os envía para este caso una particular en la cual no podéis escribir a los demás ministros, sino sólo a mí.
- Carta de Felipe II al Duque de Medina Sidonia. 19 de junio de 1581.

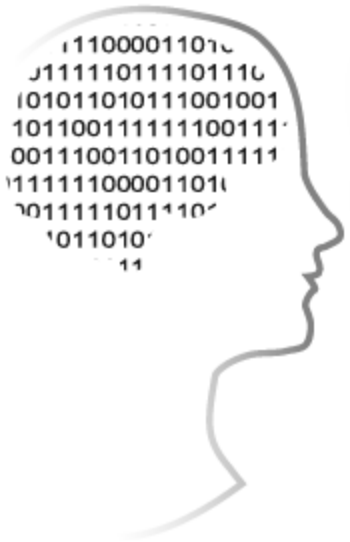
Los Espías de Felipe II. Carnicer. C., Marcos, J. La Esfera de los Libros, 2005.

España. Felipe II: tipos de cifra

- General
  - Mensajes entre Secretarios de Estado y de la Guerra, Virreyes, Embajadores, Gobernadores Generales, …
- Particular
  - Rey o Secretarios de Estado o de la Guerra con particulares.

Criptografía: etapas

- Precientífica (“artística”): Antigüedad - 1949
- Científica (Shannon): 1949 - 1976
- Asimétrica (Diffie-Hellman): 1976 - Actualidad



intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Contacto: info@intypedia.com