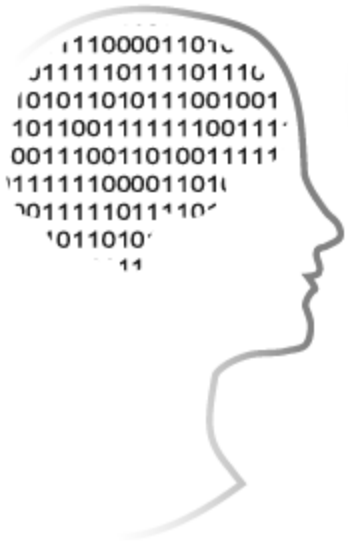
Lesson 1: History of Cryptography and its Early Stages in Europe



intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Arturo Ribagorda Garnacho
arturo@inf.uc3m.es

Carlos III University of Madrid
University Professor

Ancient Greece – Cipher development

- Homer- The Iliad
  - Book VI
- Herodotus - The Histories
  - Book V - Histiaeus
  - Book VII - Demaratus

Wax Tablet

Wax Tablet (Wall-painting in Pompeii)

Cryptography – Caesar method

- […] If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others. […]

Suetonius (69 – 140)
The Twelve Caesars

Cipher Methods

- Substitution
- Permutation (Transposition)
- Product ciphers

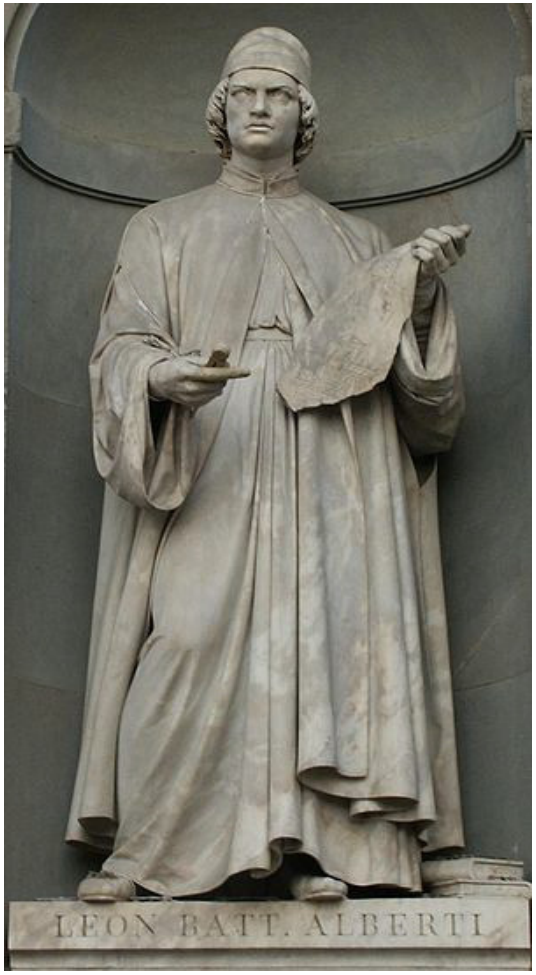
Frequency of the letters (%) in Spanish

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

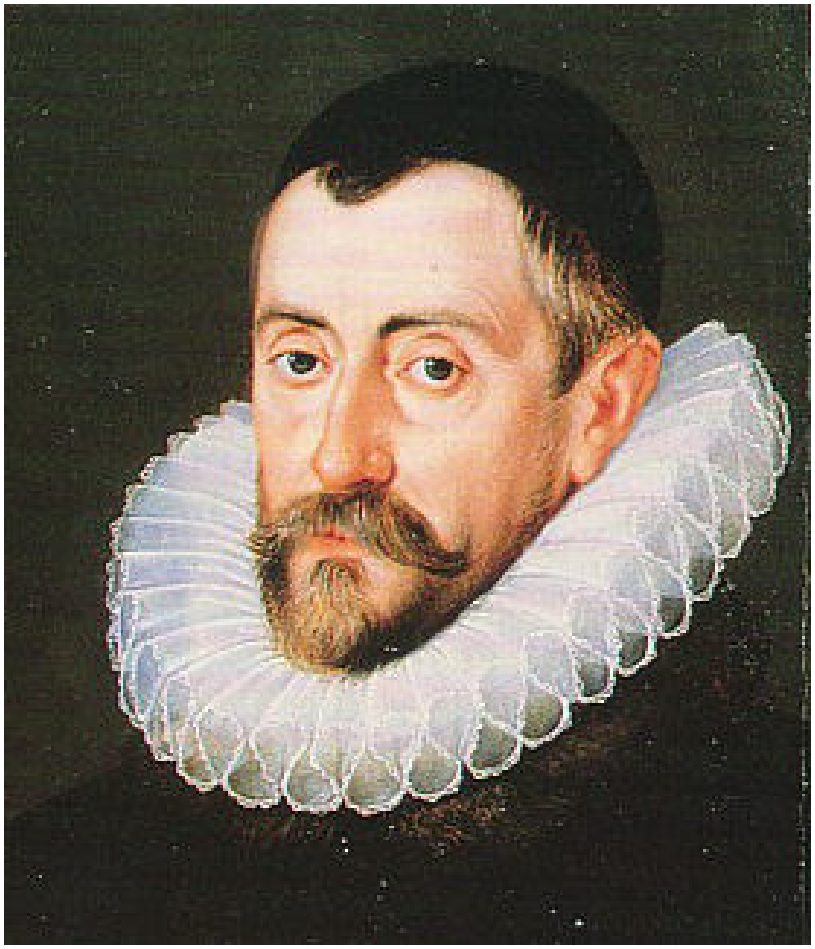
t	c	p	m	y	q	b	h	g	f
3,31	2,92	2,77	2,12	1,54	1,53	0,92	0,89	0,73	0,52

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

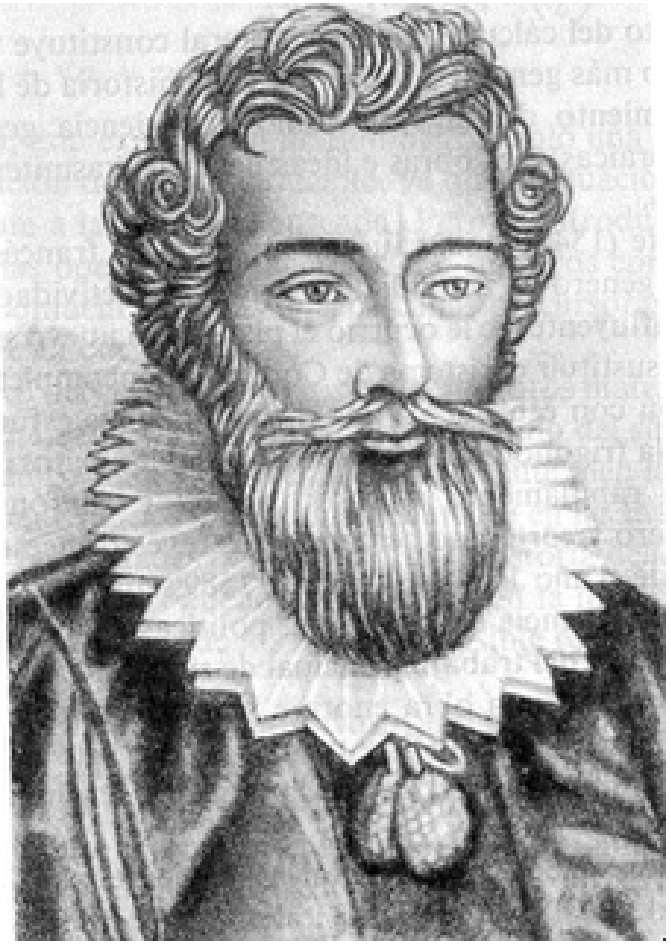
Leone Battista Alberti
Uffizi Gallery (Florence)



Francis Walsingham (1530 - 1590)



François Viète (1540 – 1603)



Philip II – Types of Cipher (1)

- "Whatever is to be kept secret should be written in ciphertext for which you use the general one that I use with all my ministers, and the personal one is used for when the business is so secret that it suits better than the general one."
- Instruction given by Philip II to Diego Guzmán de Silva, Ambassador in Venice.

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

Philip II – Types of Ciphers (2)

- "Sometimes, the business you are undertaking may be so serious, important and of such secrecy, that it would not be advisable to write it in general cipher, so for this purpose you are sent a personal cipher which will not be useful with the other ministers, only with me."
- Letter from Philip II to the Duke of Medina Sidonia, 19th of June, 1581.

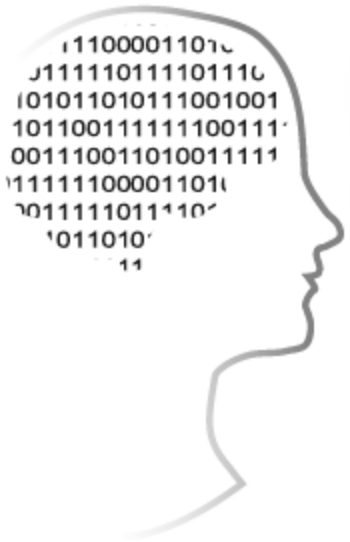
Los Espías de Felipe II. Carnicer. C., Marcos, J. La Esfera de los Libros, 2005.

Spain – Philip II – Types of Cipher

- General
  - Messages between Secretaries of Sate and War, Viceroys, Ambassadors, General Governors...
- Personal
  - King or Secretaries of Sate and War with other people

Cryptography - Stages

- Pre-scientific (“artistic”) – Ancient Times to 1949
- Scientific (Shannon) – 1949 to 1976
- Asymmetric (Diffie-Hellman) – 1976 to Present



intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Contact: info@intypedia.com