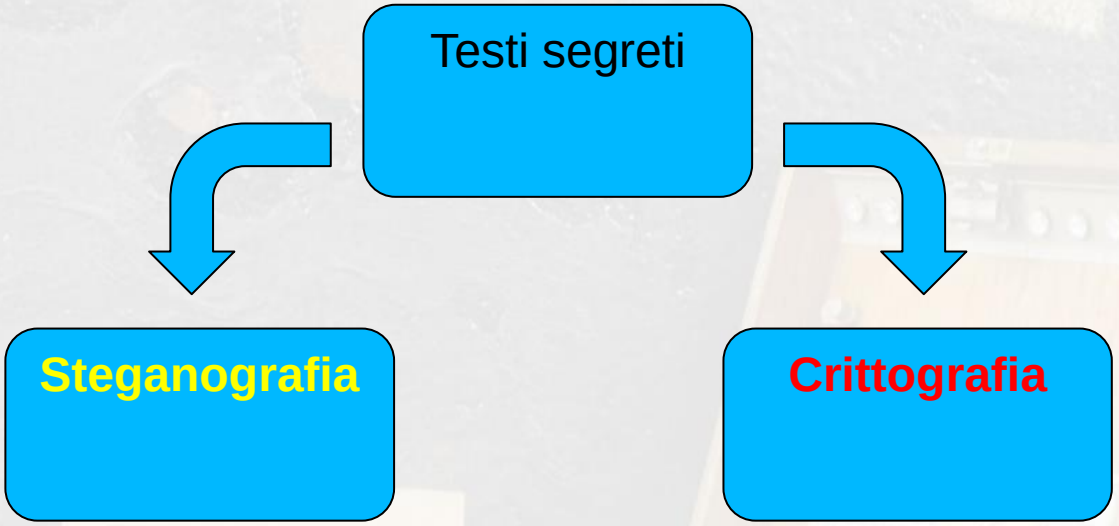
La CRITTOLOGIA

dalla Bibbia al XX secolo

Silvano Benedetti
silbened@hotmail.com

Segretezza, Integrità, Autenticazione

Information assurance



STEGANOGRAFIA

Nascondere l'esistenza di un messaggio in maniera apparentemente coerente
Funziona finchè qualcuno non ha il dubbio che se ne faccia uso

CRITTOGRAFIA

Blindare il contenuto di un messaggio affinchè sia accessibile solo al destinatario
Funziona finchè qualcuno non dispone di tecnologia superiore alla nostra

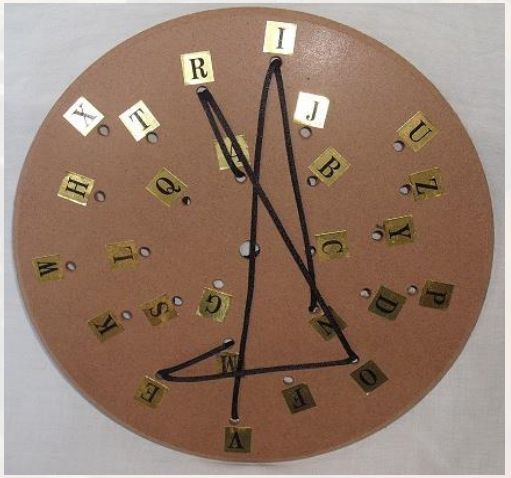
STEGANOGRAFIA

Nascondere l'esistenza di un messaggio in maniera apparentemente coerente

SULLA TESTA, TAVOLETTE CERATE, UOVO SODO, INCHIOSTRO SIMPATICO, MICROPUNTI, PALPEBRE, LSB

SCITALA LACEDEMONICA

DISCO DI ENEA



GRIGLIE DI CARDANO

CRITTOGRAFIA

Blindare il contenuto di un messaggio affinchè sia accessibile solo al destinatario

ATBASH

ABCDEFGHILMNOPQRSTUVZ
ZVUTSRQPONMLIHGFEDCBA

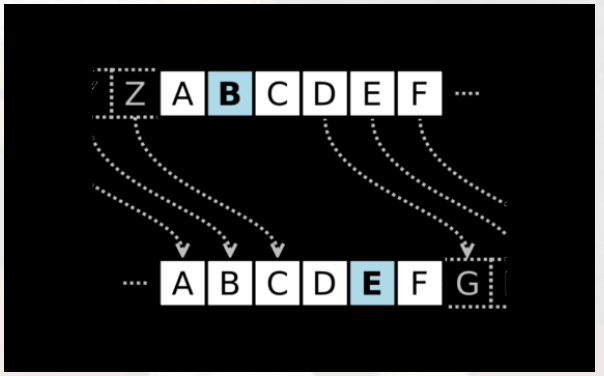
Messaggio in chiaro
SERVONO RIFORNIMENTI

Messaggio cifrato
ESFBIMI FORIFMONSMDO

SCACCHIERA DI POLIBIO

#	1	2	3	4	5
1	Α	Β	Γ	Δ	Ε
2	Ζ	Η	Θ	Ι	Κ
3	Λ	Μ	Ν	Ξ	Ο
4	Π	Ρ	Σ	Τ	Υ
5	Φ	Χ	Ψ	Ω	‡

CIFRARIO DI CESARE



Abū Yūsuf Yaʿqūb ibn Isḥāq ibn al-Ṣabbāḥ ibn ʿUmrān ibn Ismāʿīl al-Kindī

Al Kindi o Alchindus

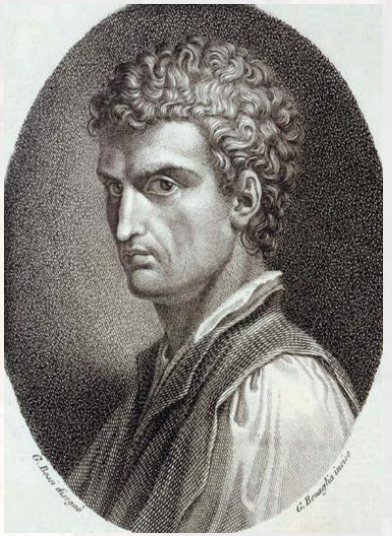
(IX secolo)

Analisi delle frequenze

Italiano	%	Inglese	%
E	11,79	E	12,31
A	11,74	T	9,59
I	11,28	A	8,05
O	9,83	O	7,94
N	6,88	N	7,19

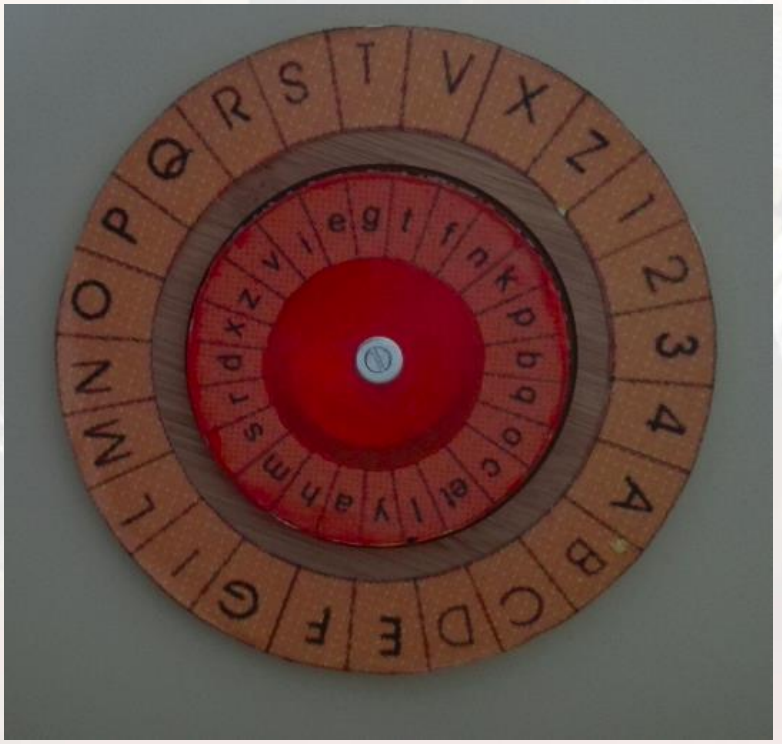
CRITTOGRAFIA

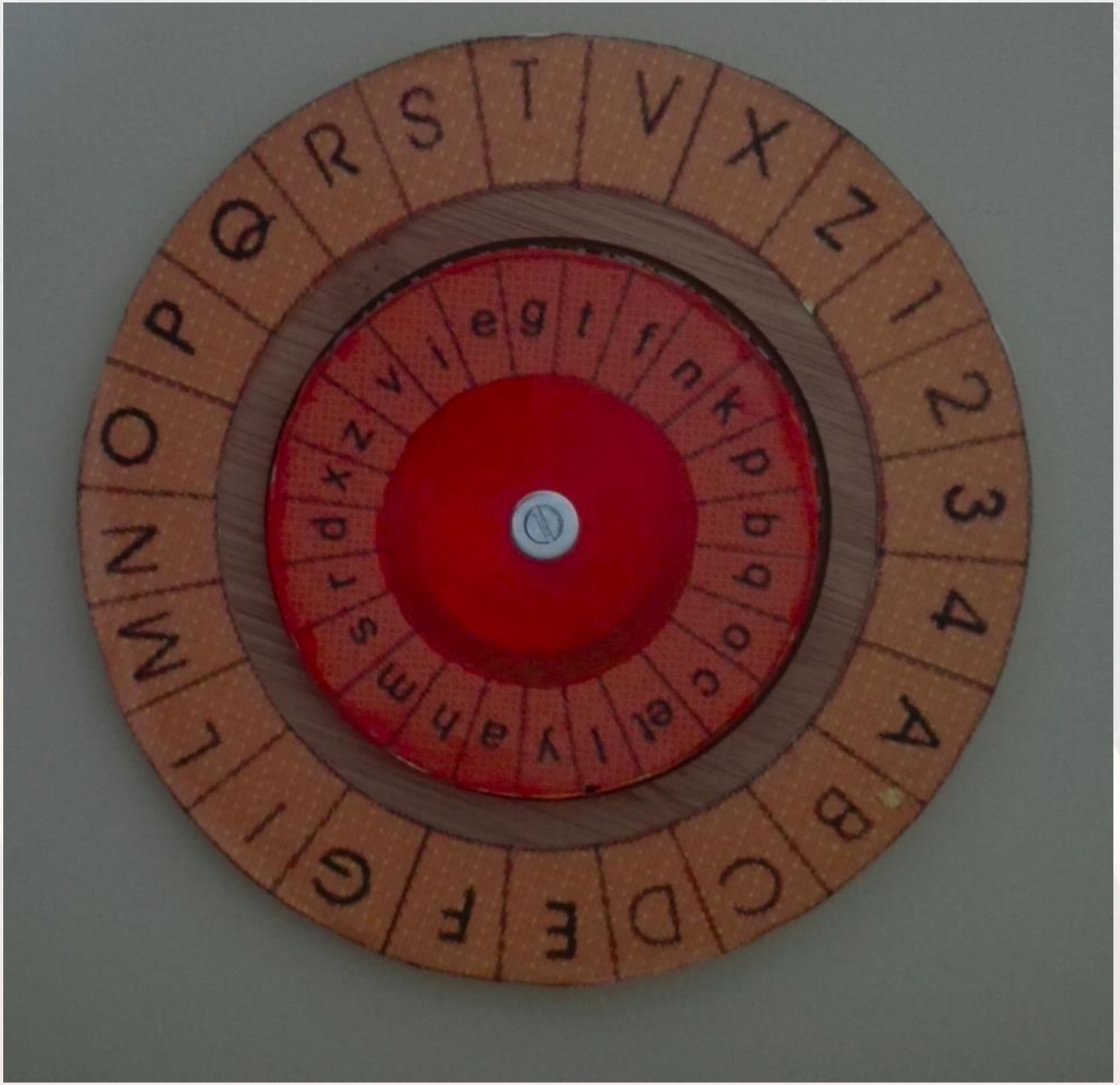
DISCO ALBERTI, CODICE VIGENERE, JEFFERSON



Leon Battista Alberti
XV secolo

Cifratura polialfabetica




A B C D E F G I L M N O P Q R S T V X Z 1 2 3 4
a b c d e f g h i k l m n o p q r s t v x z

	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
a	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
b	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	a
c	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
d	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
e	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
f	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
g	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
h	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
i	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
j	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
k	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
l	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
m	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
n	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
o	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
p	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
r	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
s	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
t	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
u	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
v	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
w	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
x	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
z	z	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

Cifrario di de’ Vigenere

XVI secolo

Disco di Jefferson 1795

MUSEO TECNICO NAVALE

CRYPTO

PAROLE (S)VELATE

(UN)COVERED WORDS

...l'ingegno umano non può architettare un codice
che l'ingegno umano non possa risolvere (E. A. Poe)

XX secolo
macchine cifranti…

ma questa è un'altra storia !!!!