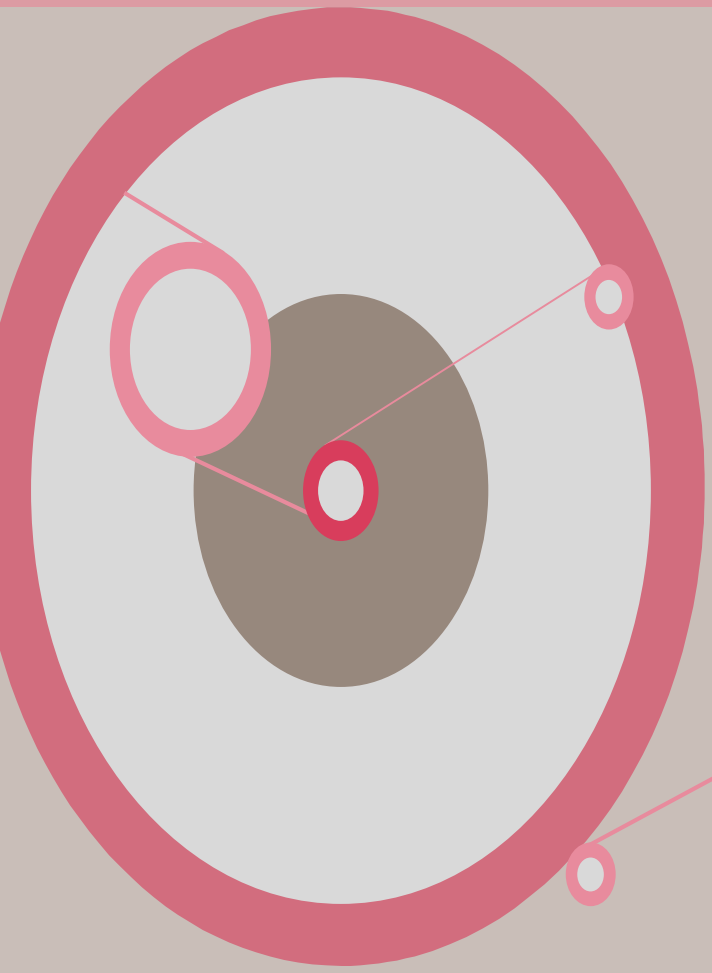
La segretezza nella Storia



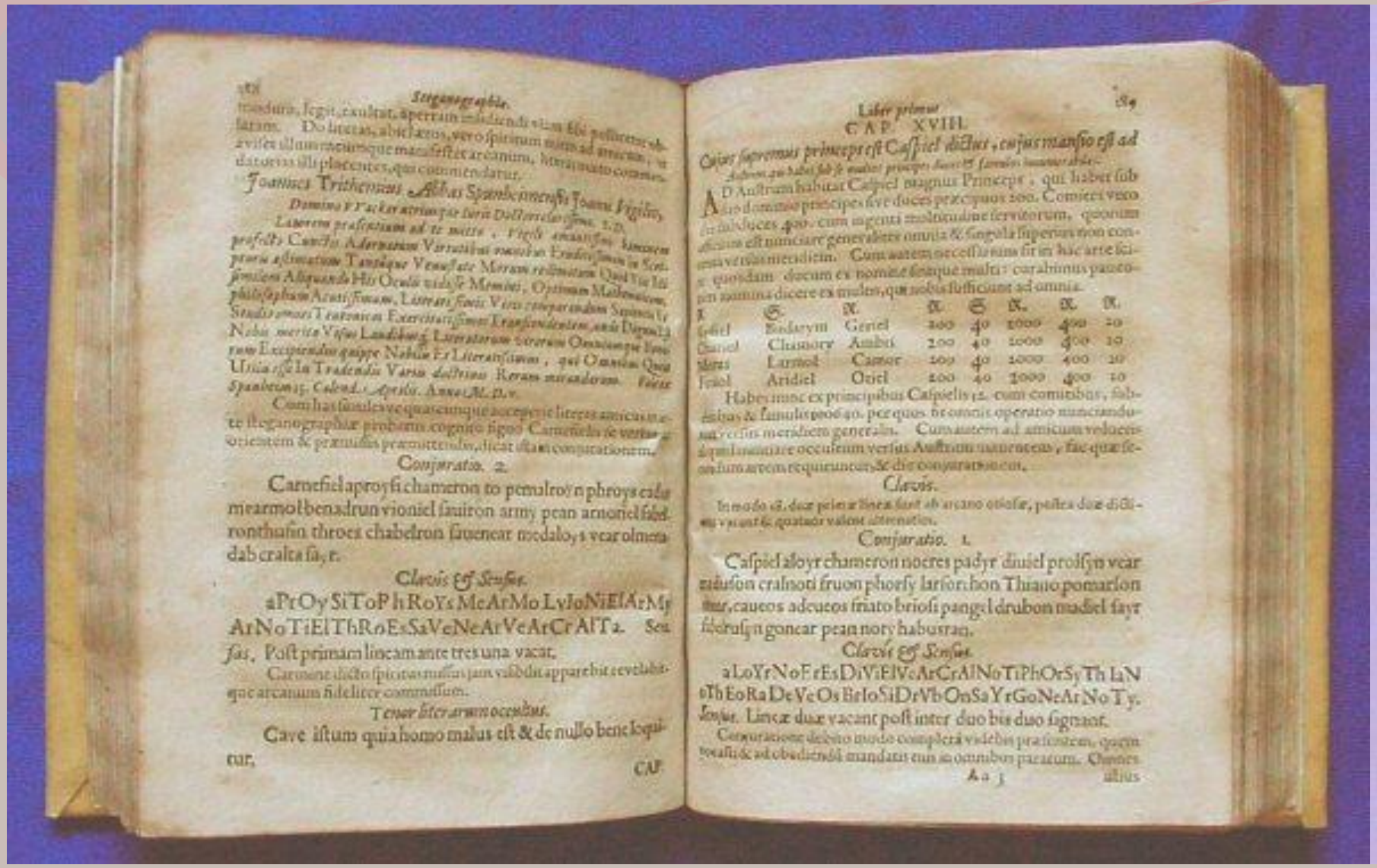
Mondo virtuale

- L'attuale società che scambia una enorme quantità di informazioni ad una velocità sorprendente
- La necessità di rendere inaccessibili le informazioni è diventata una problematica talmente complessa e talmente grande ma anche così *critica* da renderla
- *una tra le più importanti del mondo moderno.*

Da sempre

- In molti credono si tratti di una moderna tecnica di sicurezza informatica, ma in realtà i primi sistemi di *crittografia* risalgono a circa 3.000 anni fa
- Crittografia è una parola d'origine greca composta da κρυπτός (kryptós) che significa "nascosto", e γραφία (graphía) che significa "scrittura".

Steganografia



Steganographiæ.

mandura, legit, exultat, aperiam mihi dicendi vim sibi polliceretur ob-
latrans. Do literas, abi latros, vero spiritum mittit ad arcanum, si
evitet illum nacunque manifestet arcanum, literas mutato commen-
datorias illi placentes, quo commendatur.

Joannes Trithemius Abbas Spanheimensis Joanni Virgilio,

Domino Vracker artium per Iuris Doctori clarissimo, S.D.

Laborem præsentium ad te mitto, Virgili amantissime, tuumque
profectu Cupidissime Admirandum Virtutibus meritisque Eruditissimum in Scri-
pturis æstimatione Tantaque Venustate Morum redimitum. Quid Vir lu-
minibus Aliquando His Oculis vidisse Memini, Optimum Mathematicum,
philosophum Acutissimum, Literati sinceri Virum comparandum Summis Vi-
Studiis omori Tentatum Exercitatissimum Eruditissimum, unde Dignum
Nobis meritis Vestris Laudibus Literatorum virorum Omnium que Ve-
rum Excipiendo quippe Nobilem Et Literatissimum, qui Omnibus Quæ
Utilia sunt In Tradendis Variis doctrinis Rerum mirandarum. Valete
Spanheimi 15. Calend. Aprilis. Anno M. D. V.

Cum has simules vel quascunque acceperit literas amicus ar-
te steganographiæ probatus cognito signo Carneficha se versus
orientem & præmissis præmittendis, dicat illam conjurationem.

Conjuratio. 2.

Carneficha proysi chameron to pemalroyn phroys esdra
mearmolbenadrun vioniel fauiron army pean armoniel fabd-
ronthusin throes chabedron sruenear medaloys vear olmeta
dab cralta sa, e.

Clavis & Sensus.

aPrOy SiToP hRoYs MeArMo LyIoNiElArMy
ArNoTiElThRoEsSaVeNeArVeArCrAlTa. Sen-
sus. Post primam lineam ante tres una vacat.

Carmine dicto spiritus malus jam vehdum apparebit cervelabi-
que arcanum fidelitter commissum.

Tenor literarum occultus.

Cave istum quia homo malus est & de nullo bene loqui-
tur.

CAP.

Liber primus 89

CAP. XVIII.

Quis supremus princeps est Caspiel dictus, cujus mansio est ad
Austrum, ac habet sub se multos principes duces & famulos innumerabiles.

AD Austrum habitat Caspiel magnus Princeps, qui habet sub
se duos principes sive duces præcipuos 200. Comites vero
ducibus 400. cum ingenti multitudine servitorum, quorum
officium est nunciare generaliter omnia & singula superius non con-
tenta versus meridiem. Cum autem necessarius sit in hac arte scie-
quosdam ducum ex nomine seorsque multi: caralminus pauco-
pen nomina dicere ex multis, qui nobis sufficiunt ad omnia.

I	G.	R.	R	S	R.	R.	R.
Gabriel	Badarym	Geniel	200	40	2000	400	20
Chamiel	Chamory	Ambri	200	40	2000	400	20
Sabrac	Larmoel	Camor	200	40	2000	400	20
Israel	Aridiel	Oriel	200	40	2000	400	20

Habet hunc ex principibus Caspielis 12. cum comitibus, sub-
ditis & famulis 2400. per quos de omni operatio nunciandu-
versus meridiem generalis. Cum autem ad amicum vel
quod nunciare occultum versus Austrum nunciem, hæc quæ se-
cum sum autem requirunter, & dic conjurationem.

Clavis.

In modo 18. duæ primæ lineæ sunt ab arcano otiosæ, postea duæ dicti-
us vocant & quatuor valent alternatim.

Conjuratio. 1.

Caspiel aloyr chameron nocres padyr diuiel prolsyn vear
ziausun cralnori fruon phorsy larsor: hon Thiano pomarlon
mur, caueos adeueos sriato briosi pangel drubon madiel sayr
fidebrusyn goncar pean noty habustran.

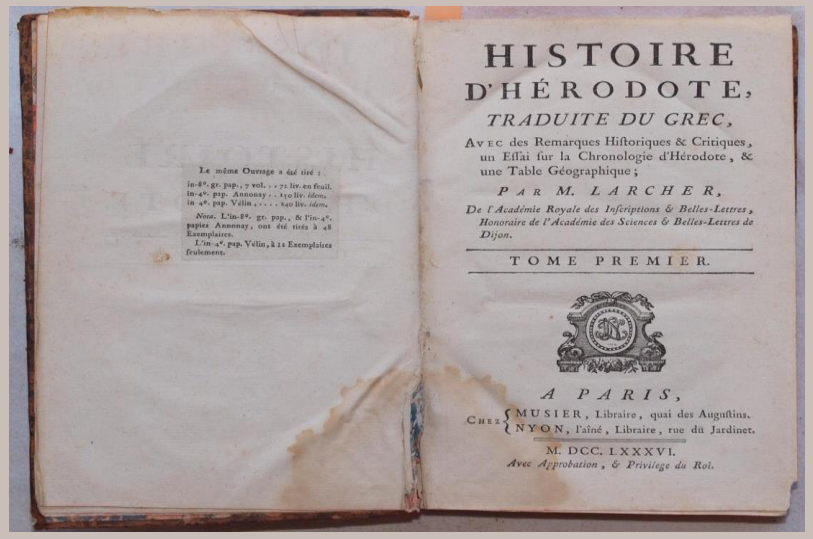
Clavis & Sensus.

aLoYrNoErEsDiViElVeArCrAlNoTiPhOrSyThLaN
sThEoRaDeVeOsBrIoSiDrVbOnSaYrGoNeArNoTy.
Sensus. Lineæ duæ vacant post inter duo bis duo signantur.

Conjuratione dicto modo completa videbis præsentem, quem
vocasti & ad obediendū mandatis eius in omnibus paratum. Omnes

Steganografia

- Nelle “Storie” di Erodoto
  - Se ne trova già testimonianza



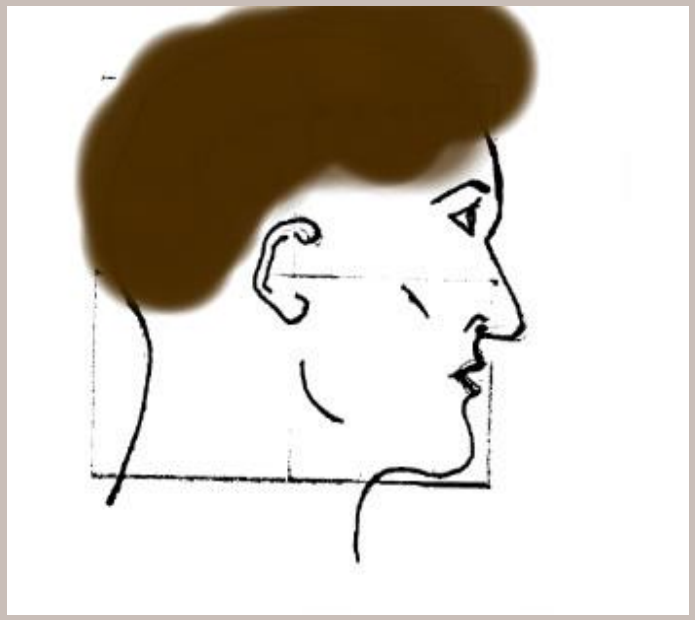
Le même Ouvrage a été tiré :
in-8°. gr. pap., 7 vol. . . 72 liv. en feuil.
in-4°. pap. Annonay . . 240 liv. idem.
in-4°. pap. Vélin . . . . . 240 liv. idem.

Nota. L'in-8°. gr. pap., & l'in-4°. papier Annonay, ont été tirés à 48 Exemplaires.
L'in-4°. pap. Vélin, à 12 Exemplaires seulement.

HISTOIRE
D'HÉRODOTE,
TRADUITE DU GREC,
Avec des Remarques Historiques & Critiques, un Essai sur la Chronologie d'Hérodote, & une Table Géographique ;
PAR M. LARCHER,
De l'Académie Royale des Inscriptions & Belles-Lettres, Honoraire de l'Académie des Sciences & Belles-Lettres de Dijon.
TOME PREMIER.
A PARIS,
Chez { MUSIER, Libraire, quai des Augustins.
NYON, l'aîné, Libraire, rue du Jardinet.
M. DCC. LXXXVI.
Avec Approbation, & Privilege du Roi.

Testa segnata

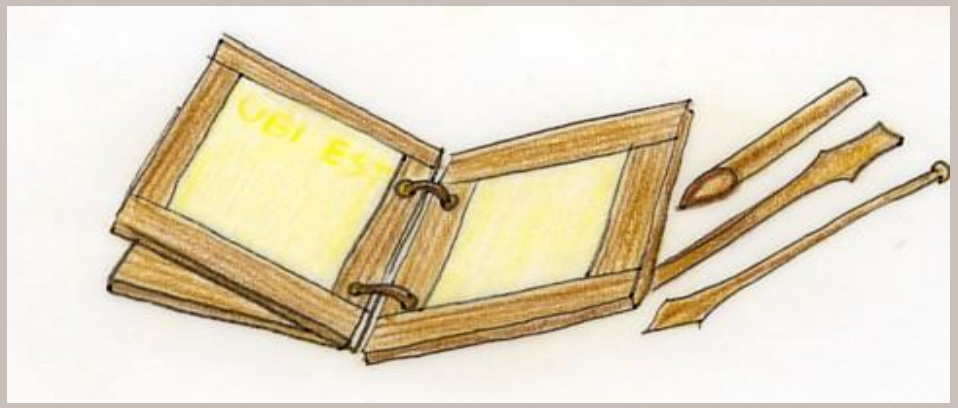
Istieo manda a Aristagora a Mileto il messaggero dalla testa segnata



- il messaggio è sulla testa rasata
- Il messo viene inviato una volta cresciuti i capelli
- Il messaggio sarà visibile rasando i capelli.

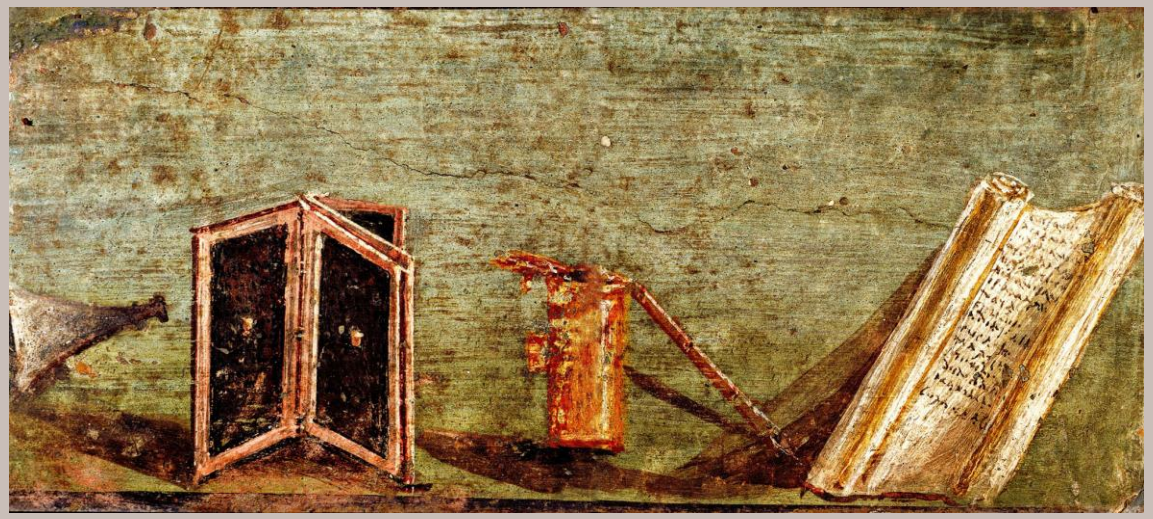
I Persiani!!

- I Lacedemoni vengono avvisati della decisione di Serse di attaccare la Grecia col sistema della doppia tavoletta
  - Il messaggio è inciso sul legno che poi verrà ricoperto con la cera
  - Una tavoletta apparentemente vuota rivela il messaggio sciogliendo la cera.



Inchiostro che scompare..

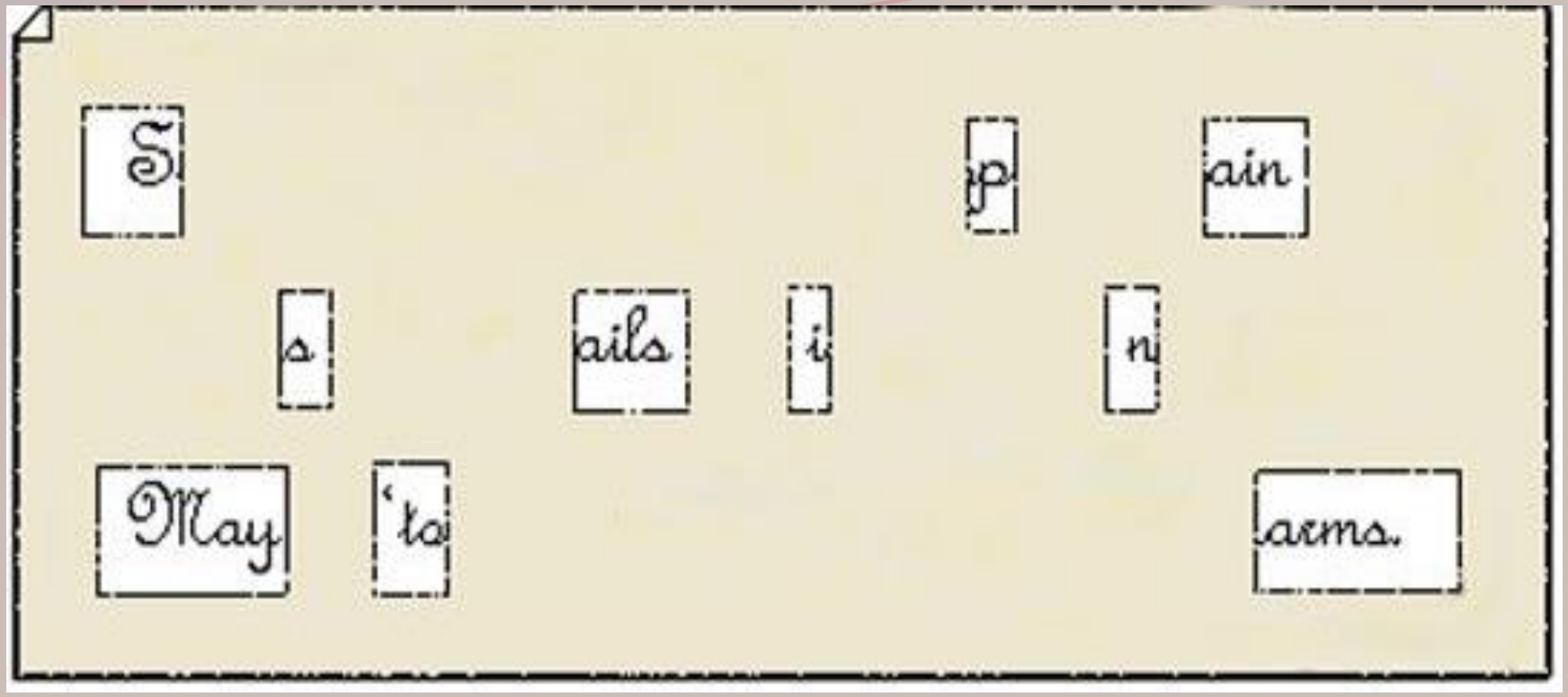
- Plinio il Vecchio nel I secolo d.c.
  - Ci parla di messaggi scritti con una sorta di inchiostro simpatico
  - realizzato con particolari piante, scompare asciugandosi
  - il messaggio si rileva al calore.



L’uovo ..?

- Gianbattista della porta XVI secolo
  - il messaggio è scritto sul guscio di un uovo sodo
  - l’inchiostro a base di aceto viene assorbito dal guscio
  - si rivela sbucciando l’uovo
- La segretezza è perduta al momento dell'intercettazione .

Griglie di Cardano (XVI secolo):



Thritemius

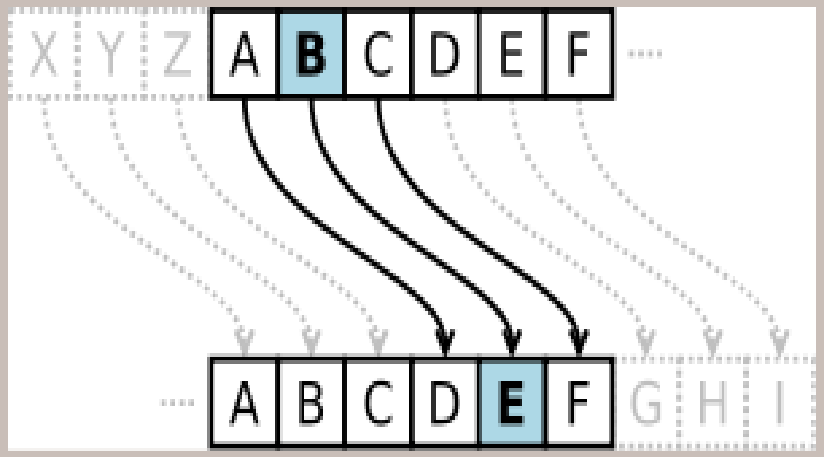
- Johannes Trithemius (1462 –1516)
- "Steganografia" : propone 40 sistemi per nascondere i messaggi.

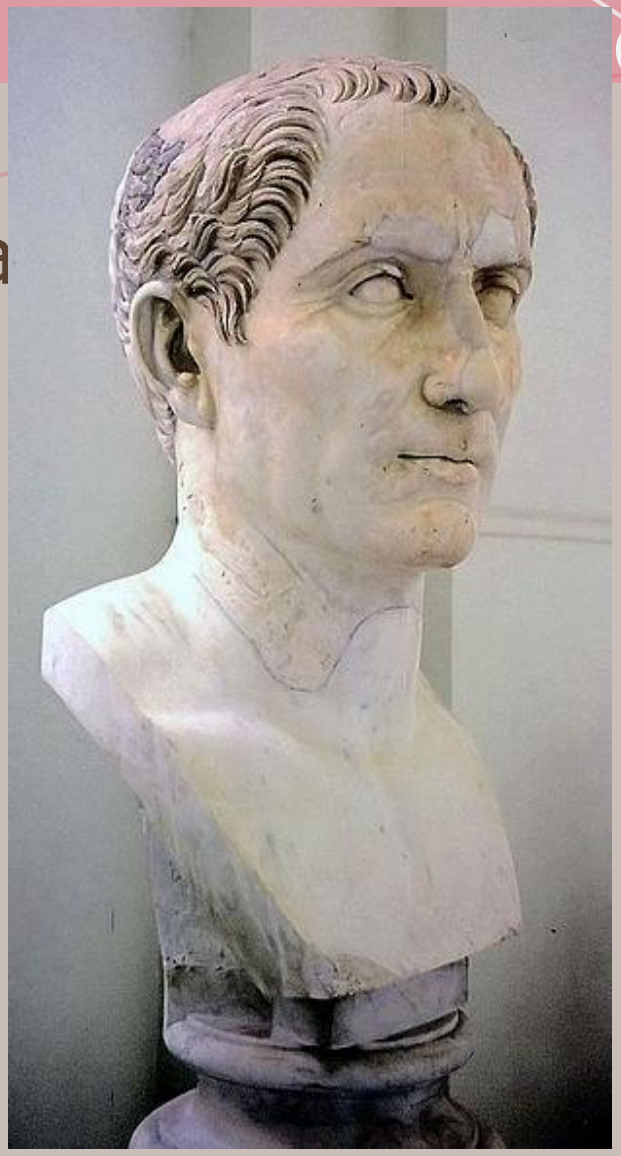
Nelle ore notturne feroci illusioni di antichi riti tramandati in dimenticate isole ci assalgono, ivi ora..

Non fidatevi di Caio.

Crittografia

- Trasformazione + segretezza
- Codice Giulio Cesare.





crittoanalisi

- dal greco kryptós, "nascosto", e analýein, "scomporre", o crittanalisi
- si intende lo studio dei metodi per ottenere il significato di informazioni cifrate senza avere accesso all'informazione segreta che è di solito richiesta per effettuare l'operazione
- Tipicamente si tratta di trovare una chiave segreta.

crittologia

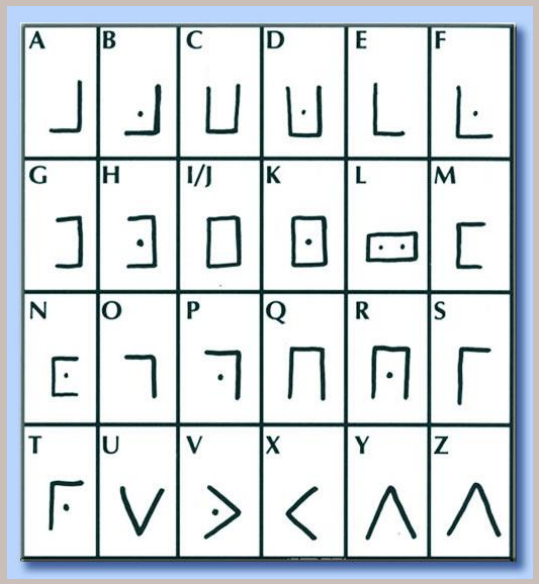
- La crittoanalisi è la "controparte" della crittografia
- assieme formano la crittologia, la scienza delle scritture nascoste.

Crittoanalisi

- Furono probabilmente motivi religiosi inerenti all'analisi testuale del Corano che portarono all'invenzione della tecnica **dell'analisi delle frequenze** per violare i cifrari a sostituzione monoalfabetica da parte di Al-Kindi intorno al IX secolo.
- Tecnica + importante fino alla II guerra mondiale

Sostituzione

- Cifrari a sostituzione mono alfabetica
  - Ogni lettera viene sostituita con un’altra
  - Elevato numero di chiavi possibili
  - I simboli conservano l'identità
  - E’ facilmente decifrabile con l’analisi delle frequenze



Alfabeto dei RosaCroce

Congiura di Babington

- Maria Stuarda ne fu coinvolta nel 1586
- Veniva usato un corriere
- Birraio
  - nascondeva i messaggi nello zipolo delle botti
- 35 simboli x lettere e frasi
- 4 nulle e un simbolo per le doppie.

Trasposizione

- Cifrari a trasposizione
- Le lettere del messaggio in chiaro cambiano posizione nel messaggio cifrato
- Sono semplici da decifrare perché le lettere sono visibili

Trasposizione

- La **scitala lacedemonica**,
  - usata in Grecia fin dal 400 a.C., non era altro che un bastone (idealmente un cilindro), attorno al quale veniva avvolto a spirale una striscia di tessuto sul quale veniva scritto il messaggio
  - Una volta srotolato il tessuto, solo con un bastone dallo stesso diametro sarebbe stato possibile leggere correttamente il messaggio.

Leon Battista Alberti

- Per rendere più difficile l'applicazione dell'analisi delle frequenze, già nel 1460, elaborò un nuovo sistema di criptazione
- aggiungendo un secondo alfabeto
- Per criptare il messaggio si proponeva di alternare i due alfabeti cifrati.

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
Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M
M	N	B	V	C	X	Z	T	K	J	H	G	F	D	S	A	P	O	I	U	Y	L	R	E	W	Q

- Ad esempio se la parola è “CAPRA” verrà codificata in “EMHOQ”
- Il vantaggio di questo metodo, rispetto ai precedenti è il fatto che uno stesso carattere del messaggio in chiaro può essere cifrato in due modi diversi, come possiamo vedere nell’esempio precedente, dove la A è codificata in Q ed M.

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
Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M
M	N	B	V	C	X	Z	T	K	J	H	G	F	D	S	A	P	O	I	U	Y	L	R	E	W	Q

- Questo portava così un po' di confusione al crittanalista che volesse applicare il metodo delle frequenze
- L'analisi delle frequenze perdeva così buona parte della sua utilità
- L'idea di Alberti però è stata attribuita ad altri due teorici delle stessa epoca, il tedesco Johannes Trithemius ed il francese Blais De Vigenère.

Alberti

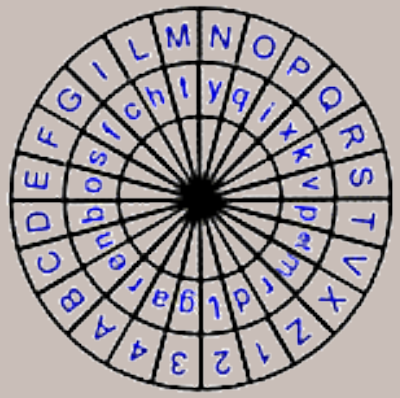
- I dischi di Alberti
- Sono una sorta di cifratori portatili costituiti da un telaio circolare fisso, in cui è inciso l'alfabeto convenzionale, dove, in modo concentrico viene applicato all'interno un disco rotante con l'alfabeto cifrato .

Esempio

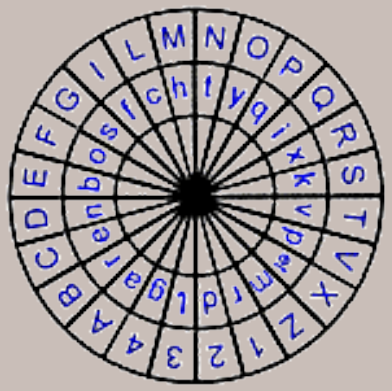
LEON BATTISTA ALBERTI

T hoqy O drqqnyqr H acrbxvf

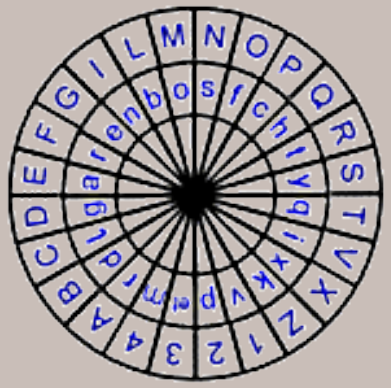
M=T



M=H



M=O



Oggi

- Oggi la **crittografia** è diventata indispensabile in campo informatico
- Con sistemi sempre più avanzati di hackering e di phishing, le società di sicurezza informatica devono utilizzare sistemi crittografici sempre più complessi
- In particolare, la crittografia trova applicazione in ambito Internet, dove la protezione dei dati personali è divenuta ormai "affare di stato".

Nell'epoca dei computer

- Lavorare con cifre binarie invece di lettere
- Si possono ripetere le elaborazioni molte volte
- La velocità di esecuzione è molto maggiore
- Le vecchie tecniche sono superate.