Breve storia della crittografia

Settimana della Scienza

2025 - La Crittografia: segreti, enigmi e codici da decifrare

Marco Antonio Pellegrini

Università Cattolica del Sacro Cuore

22 ottobre 2025

Crittologia

La crittografia è quella disciplina che si occupa di creare e implementare codici segreti (che chiameremo crittosistemi). La crittoanalisi si occupa invece di "rompere" crittosistemi (un tentativo di rottura è detto attacco).

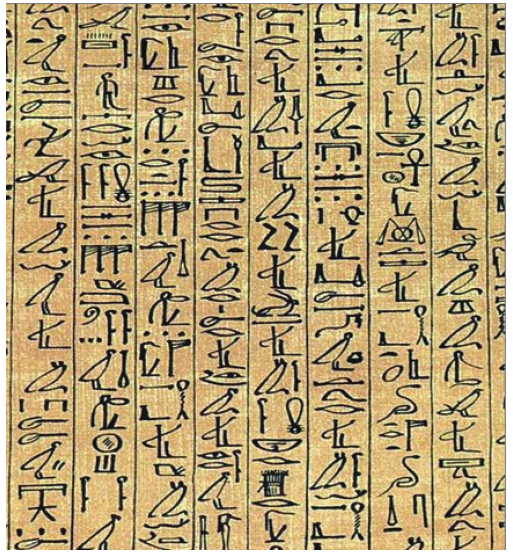
Con il termine crittologia indichiamo la disciplina più generale che comprende la crittografia e la crittoanalisi.

Un codice (o crittosistema) è un algoritmo che trasforma un testo in chiaro (*plaintext*) in un testo cifrato (*ciphertext*).

La cifratura di un messaggio trasforma il plaintext nel ciphertext, mentre la decifrazione è il processo inverso.

Egitto e Babilonia

La prima pratica della crittografia risale almeno all'antico Egitto, dove gli scribi registravano varie informazioni come geroglifici su monumenti e tombe per distinguerli dai caratteri comunemente usati all'epoca e dare loro maggiore importanza.



Questi geroglifici includevano simboli e immagini, e venivano tradotti dalla gerarchia del paese a proprio piacimento. Pertanto, i geroglifici servivano allo scopo di trascrivere qualcosa e mascherare il testo in segreto.

I Babilonesi e altri popoli, più o meno nello stesso periodo, utilizzavano tavolette cuneiformi per la loro scrittura. Una di queste tavolette conteneva la formula segreta per una smaltatura per ceramica, dove le figure che definivano gli ingredienti erano volutamente mescolate in modo che nessuno potesse rubare la ricetta segreta. Questo è il più antico esempio di crittografia sopravvissuto.

Grecia

Nel periodo tra il 400 e il 300 a.C. furono sviluppati vari sistemi di trasmissione per inviare messaggi, tra cui l'uso di segnali di fuoco per la navigazione attorno alle linee nemiche.

Polibio (II sec a.C.), storico e crittografo, perfezionò la segnalazione e la cifratura basandosi su un'idea del filosofo Democrito. Utilizzò vari segnali di torce per rappresentare le lettere dell'alfabeto greco e creò un vero e proprio sistema alfabetico basato su una griglia 5×5, chiamata 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	o
4	π	ρ	σ	τ	υ
5	ϕ	χ	ψ	ω	

Questo è il primo sistema conosciuto, di facile utilizzo, per trasformare un alfabeto in numeri.

Il Cifrario di Cesare

Il cifrario di Cesare prende il nome da Gaio Giulio Cesare, che lo utilizzava con l'intento di proteggere i suoi messaggi criptati. Grazie allo storico Svetonio, sappiamo che Cesare utilizzava in genere uno spostamento di 3 lettere per il cifrario, come nel caso della corrispondenza militare inviata alle truppe comandate da Quinto Tullio Cicerone.

Vite dei Cesari (Svetonio)

Extant et ad Ciceronem, item ad familiares, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum, id est D pro A et perinde reliquas commutet.

Quello che Cesare faceva era sostituire una lettera dell'alfabeto con la lettera che si trovava 3 posizioni successive:

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

Il Cifrario di Cesare

Il cifrario di Cesare prende il nome da Gaio Giulio Cesare, che lo utilizzava con l'intento di proteggere i suoi messaggi criptati. Grazie allo storico Svetonio, sappiamo che Cesare utilizzava in genere uno spostamento di 3 lettere per il cifrario, come nel caso della corrispondenza militare inviata alle truppe comandate da Quinto Tullio Cicerone.

Vite dei Cesari (Svetonio)

Extant et ad Ciceronem, item ad familiares, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum, id est D pro A et perinde reliquas commutet.

Quello che Cesare faceva era sostituire una lettera dell'alfabeto con la lettera che si trovava 3 posizioni successive:

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

X	Y	Z
↕	↕	↕
A	B	C

Il Cifrario di Cesare

Il Cifrario di Cesare è un (facile) esempio di cifrario permutazionale: le lettere dell'alfabeto vengono riordinate, in modo che lettere distinte vengano sostituite da lettere distinte:

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

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

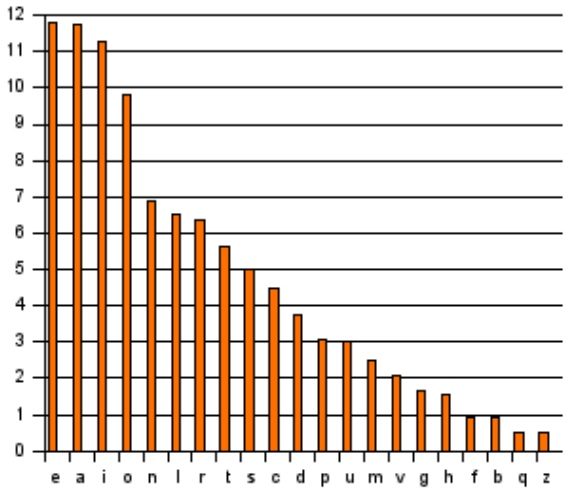
Abbiamo 403 291 461 126 605 635 584 000 000 possibilità.

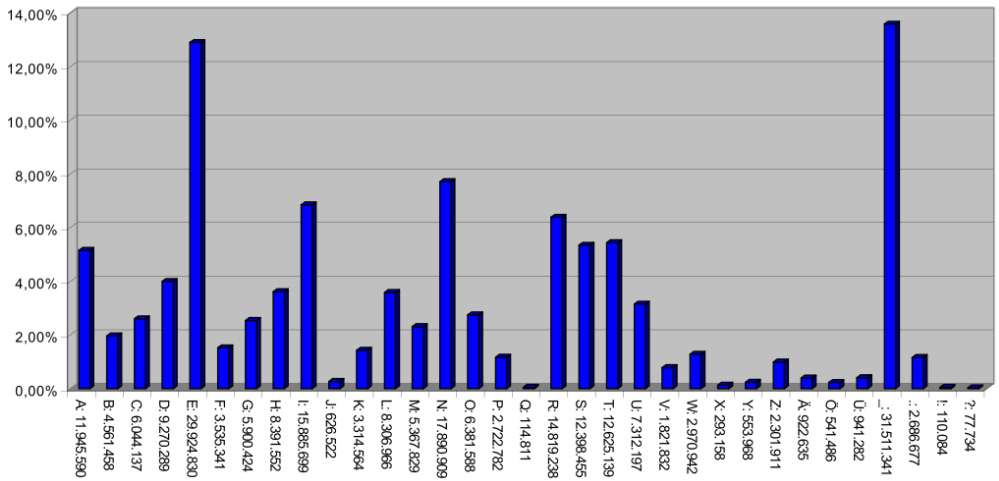
Analisi delle frequenze

I cifrari basati sulla sostituzione di una lettera con una data lettera/simbolo (in modo che a lettere uguali corrispondano lettere uguali) sono in realtà facilmente attaccabili utilizzando l'Analisi delle Frequenze.

Infatti, in ogni lingua vi sono lettere utilizzate con maggior frequenza e altre che invece lo sono molto più raramente. L'Analisi delle Frequenze utilizza proprio la frequenza delle lettere in un alfabeto come un metodo per indovinare il plaintext.

Per esempio, E e A sono le due lettere più comunemente usate in italiano, mentre E e N sono le due lettere più comunemente usate in tedesco. Pertanto, la lingua utilizzata fa la differenza.





al-Kindi

Abu Yusuf Ya'qub ibn Isḥaq al-Kindī (Alkindus per gli europei del tempo) fu un matematico arabo, vissuto tra l'801 e l'873 d.C. in quello che oggi è l'Iraq. Fu un prolifico filosofo e matematico ed era conosciuto dai suoi contemporanei come "il Secondo Maestro", il primo dei quali fu Aristotele.

Un precoce ingresso nel mondo del lavoro presso la Casa della Saggezza, il centro intellettuale dell'Età d'Oro dell'Islam, lo portò a contatto con migliaia di documenti storici che dovevano essere tradotti in arabo, avviandolo su un percorso di ricerca scientifica a cui pochi erano esposti in quel periodo.

Al-Kindi fu il primo matematico noto a sviluppare e utilizzare l'attacco tramite Analisi delle frequenze. L'intero lavoro di al-Kindi in questo campo fu pubblicato nella sua opera *Sulla decifrazione dei messaggi crittati*, uno degli oltre 290 testi pubblicati durante la sua vita.

al-Kindi

Il fulcro di questo lavoro era l'applicazione della teoria della probabilità (anticipando di quasi 800 anni Fermat e Pascal) alle lettere. Le radici dell'intuizione di al-Kindi sull'Analisi delle Frequenze risalgono allo studio del Corano.

I teologi dell'epoca cercavano di ricostruire l'ordine esatto in cui il Corano era stato assemblato contando il numero di determinate parole in ogni sura.

Dopo un esame continuo, divenne chiaro che alcune parole apparivano molto più spesso rispetto al resto e, dopo uno studio ancora più approfondito della fonetica, divenne più evidente che anche le lettere stesse apparivano a frequenze prestabilite.

al-Kindi

Nel suo trattato sulla crittoanalisi, al-Kindi scrisse:

> Un modo per risolvere un messaggio criptato, se ne conosciamo la lingua, è trovare un testo in chiaro diverso della stessa lingua abbastanza lungo da riempire circa un foglio, e poi contiamo le occorrenze di ciascuna lettera. Chiamiamo la lettera più frequente "prima", la lettera successiva più frequente "seconda", la lettera successiva più frequente "terza", e così via, fino a quando non consideriamo tutte le diverse lettere nel campione di testo in chiaro. Quindi esaminiamo il testo cifrato che vogliamo risolvere e classifichiamo anche i suoi simboli. Troviamo il simbolo più ricorrente e lo modifichiamo nella forma della "prima" lettera del campione di testo in chiaro, il simbolo successivo più comune viene modificato nella forma della "seconda" lettera, e il simbolo successivo più comune viene modificato nella forma della "terza" lettera, e così via, finché non teniamo conto di tutti i simboli del crittogramma che vogliamo risolvere.

Analisi delle frequenze

Supponiamo di aver intercettato il seguente testo cifrato, che sappiamo essere stato prodotto in italiano applicando un cifrario permutazionale:

AMQL DEOU NQL LEWU NC KUOU KZQ PULWQ E OQBBUWCUDRU JDE NMQ
KEJQRQ RUR CRJQDDUJJQ NC OURJC JMJJU E GQRC Q E WULTC E GQKURNE
NQLLU GXUDWQDQ Q NQL DCQRJDEDQ NC AMQLLC PCQR AMEGC E MR
JDEJJU E DCGJDCRWQDGC Q E XDQRNQD KUDGU Q TCWMDE NC TCMOQ
JDE MR XDUOURJUDCU E NQGJDE Q MR EOXCE KUGJCQDE NELL ELJDE XEDJQ

Analisi delle frequenze

Supponiamo di aver intercettato il seguente testo cifrato, che sappiamo essere stato prodotto in italiano applicando un cifrario permutazionale:

AMQL DEOU NQL LEWU NC KUOU KZQ PULWQ E OQBBUWCUDRU JDE NMQ KEJQRQ RUR CRJQDDUJJQ NC OURJC JMJJU E GQRC Q E WULTC E GQKURNE NQLLU GXUDWQDQ Q NQL DCQRJDEDQ NC AMQLLC PCQR AMEGC E MR JDEJJU E DCGJDCRWQDGC Q E XDQRNQD KUDGU Q TCWMDE NC TCMOQ JDE MR XDUOURJUDCU E NQGJDE Q MR EOXCE KUGJCQDE NELL ELJDE XEDJQ

Contiamo quante volte appare una data lettera:

A	B	C	D	E	F	G	H	I	J	K	L	M
3	2	21	25	26	0	9	0	0	20	6	13	10
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
12	7	2	32	16	0	3	24	0	7	5	0	1

La lettera che compare più volte è quindi la Q, seguita dalla E. Tramite l'Analisi delle Frequenze, è plausibile supporre (ovviamente si possono fare vari tentativi) che

$$Q = E, \qquad E = A$$

Analisi delle frequenze

AMEL DAOU NEL LAWU NC KUOU KZE PULWE A OEBBUWCUDRU JDA NME
KAJERE RUR CRJEDDUJJE NC OURJC JMJJU A GERC E A WULTC A GEKURNA
NELLU GXUDWEDE E NEL DCERJDADE NC AMELLC PCER AMAGC A MR JDAJJU
A DCGJDCRWEDGC E A XDERNED KUDGU E TCWMDA NC TCMOE JDA MR
XDUOURJUDCU A NEGJDA E MR AOXCA KUGJCEDA NALL ALJDA XADJE

Analisi delle frequenze

AMEL DAOU NEL LAWU NC KUOU KZE PULWE A OEBBUWCUDRU JDA NME KAJERE RUR CRJEDDUJJE NC OURJC JMJJU A GERC E A WULTC A GEKURNA NELLU GXUDWEDE E NEL DCERJDADE NC AMELLC PCER AMAGC A MR JDAJJU A DCGJDCRWEDGC E A XDERNED KUDGU E TCWMDA NC TCMOE JDA MR XDUOURJUDCU A NEGJDA E MR AOXCA KUGJCEDA NALL ALJDA XADJE

Essendo un testo in italiano, possiamo immaginare che le ultime lettere di ogni parola siano spesso delle vocali.
Avendo già utilizzato le lettere A e E, possiamo ipotizzare che U = O:

AMEL DAOO NEL LAWO NC KOOO KZE POLWE A OEBBOWCODRO JDA NME KAJERE ROR CRJEDDOJJE NC OORJC JMJJO A GERC E A WOLTC A GEKORNA NELLO GXODWEDE E NEL DCERJDADE NC AMELLC PCER AMAGC A MR JDAJJO A DCGJDCRWEDGC E A XDERNED KODGO E TCWMDA NC TCMOE JDA MR XDOOORJODCO A NEGJDA E MR AOXCA KOGJCEDA NALL ALJDA XADJE

Analisi delle frequenze

AMEL DAOU NEL LAWU NC KUOU KZE PULWE A OEBBUWCUDRU JDA NME KAJERE RUR CRJEDDUJJE NC OURJC JMJJU A GERC E A WULTC A GEKURNA NELLU GXUDWEDE E NEL DCERJDADE NC AMELLC PCER AMAGC A MR JDAJJU A DCGJDCRWEDGC E A XDERNED KUDGU E TCWMDA NC TCMOE JDA MR XDUOURJUDCU A NEGJDA E MR AOXCA KUGJCEDA NALL ALJDA XADJE

Essendo un testo in italiano, possiamo immaginare che le ultime lettere di ogni parola siano spesso delle vocali.
Avendo già utilizzato le lettere A e E, possiamo ipotizzare che U = O:

AMEL DAOO NEL LAWO NC KOOO KZE POLWE A OEBBOWCODRO JDA NME KAJERE ROR CRJEDDOJJE NC OORJC JMJJO A GERC E A WOLTC A GEKORNA NELLO GXODWEDE E NEL DCERJDADE NC AMELLC PCER AMAGC A MR JDAJJO A DCGJDCRWEDGC E A XDERNED KODGO E TCWMDA NC TCMOE JDA MR XDOOORJODCO A NEGJDA E MR AOXCA KOGJCEDA NALL ALJDA XADJE

Ora puntiamo l'attenzione sulla parola ROR: probabilmente R = N.

Analisi delle frequenze

AMEL DAOO NEL LAWO NC KOOO KZE POLWE A OEBBOWCODNO JDA NME KAJENE NON CNJEDDOJJE NC OONJC JMJJO A GENC E A WOLTC A GEKONNA NELLO GXODWEDE E NEL DCENJDADE NC AMELLC PCEN AMAGC A MN JDAJJO A DCGJDCNWEDGC E A XDENNED KODGO E TCWMDA NC TCMOE JDA MN XDOOONJODCO A NEGJDA E MN AOXCA KOGJCEDA NALL ALJDA XADJE

Analisi delle frequenze

AMEL DAOO NEL LAWO NC KOOO KZE POLWE A OEBBOWCODNO JDA NME KAJENE NON CNJEDDOJJE NC OONJC JMJJO A GENC E A WOLTC A GEKONNA NELLO GXODWEDE E NEL DCENJDADE NC AMELLC PCEN AMAGC A MN JDAJJO A DCGJDCNWEDGC E A XDENNED KODGO E TCWMDA NC TCMOE JDA MN XDOOONJODCO A NEGJDA E MN AOXCA KOGJCEDA NALL ALJDA XADJE

e così via...

QUEL RAMO DEL LAGO DI COMO CHE VOLGE A MEZZOGIORNO TRA DUE CATENE NON INTERROTTE DI MONTI TUTTO A SENI E A GOLFI A SECONDA DELLO SPORGERE E DAL RIENTRARE DI QUELLI VIEN QUASI A UN TRATTO A RISTRINGERSI E A PRENDER CORSO E FIGURA DI FIUME TRA UN PROMONTORIO A DESTRA E UN AMPIA COSTIERA DALL ALTRA PARTE.

Cerchiamo allora altre tecniche per poter comunicare in modo sicuro.

Steganografia

La steganografia è la tecnica di trasmissione di un messaggio in modo tale che ne sia sconosciuta persino l'esistenza.

Esistono due tipi di steganografia: la steganografia tecnica o fisica e quella linguistica. L'inchiostro invisibile è un esempio di steganografia tecnica, così come i libri scavati, i manici degli ombrelli e altri elementi che compaiono frequentemente nei romanzi di spionaggio.

L'uso della steganografia tecnica risale almeno al v secolo a.C. Lo storico greco Erodoto descrisse la rivolta contro il dominio persiano, che ebbe successo grazie all'uso della steganografia.

Due capi della rivolta comunicarono segretamente rasando la testa di uno schiavo e tatuandovi sopra un messaggio segreto. Dopo che i capelli dello schiavo ricrebbero, lo schiavo fu inviato ai cospiratori che lessero il messaggio rasandogli la testa.

I Greci riuscirono a rovesciare i Persiani usando le informazioni contenute nel messaggio nascosto.

Steganografia

Cinquant'anni prima, un secondo metodo steganografico fu utilizzato dai Greci contro i Persiani per respingere un'invasione di Serse e dei suoi uomini. Demarto utilizzò un dispositivo improvvisato, creato raschiando la cera da due tavolette di legno, per allertare gli Spartani. Scrisse sulle tavolette ciò che sapeva delle intenzioni dei Persiani e poi rimise a posto la copertura di cera.

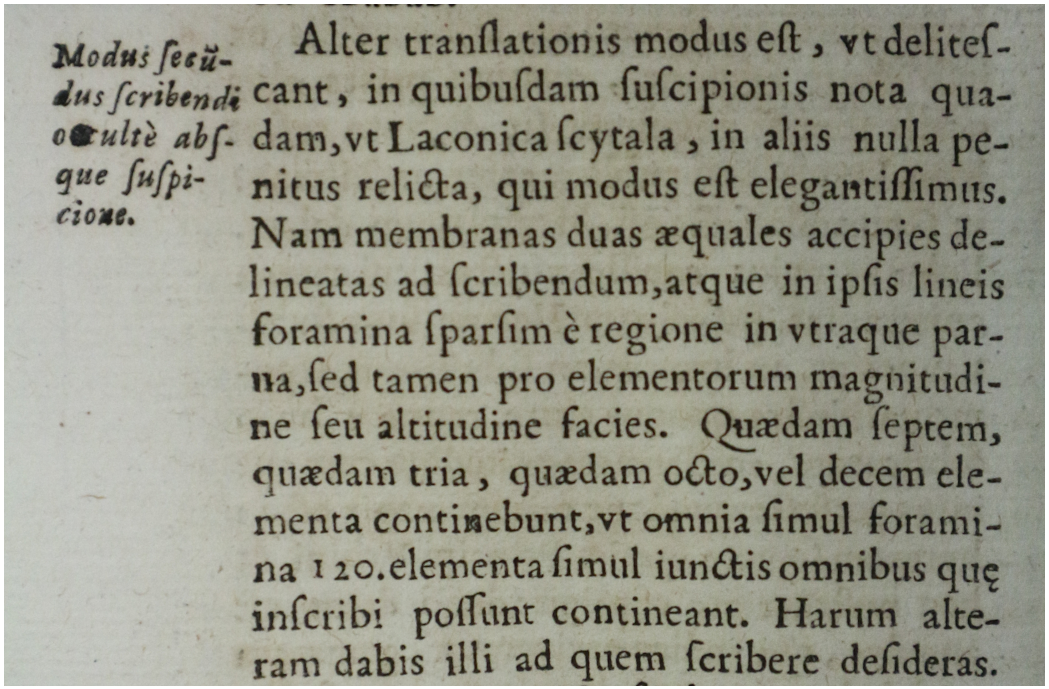
Le tavolette, apparentemente semplici, furono passate intatte agli Spartani, che a loro volta raschiarono via la cera per leggere il messaggio.

Con la steganografia abbiamo la possibilità che le persone non siano nemmeno a conoscenza dell'esistenza del messaggio.

Gerolamo Cardano

Gerolamo Cardano (1501–1576) fu un importante medico e matematico del Rinascimento, noto per la disputa con Tartaglia riguardo alle formule risolutive delle equazioni di terzo grado.

Cardano nel suo trattato *De subtilitate* tratta brevemente anche di crittografia proponendo tre cifrari, dei quali il più noto è la griglia che porta il suo nome.



Modus ſecũdus ſcribendi occultè abſque ſuſpicione.

Alter tranſlationis modus eſt, vt deliteſcant, in quibuſdam ſuſcipionis nota quadam, vt Laconica ſcytala, in aliis nulla penitus relicta, qui modus eſt elegantiſſimus. Nam membranas duas æquales accipies delineatas ad ſcribendum, atque in ipſis lineis foramina ſparſim è regione in vtraque parua, ſed tamen pro elementorum magnitudine ſeu altitudine facies. Quædam ſeptem, quædam tria, quædam octo, vel decem elementa continebunt, vt omnia ſimul foramina 120. elementa ſimul iunctis omnibus quę inſcribi poſſunt contineant. Harum alteram dabis illi ad quem ſcribere deſideras.

La Biblioteca di Scienze “Carlo Viganò”

Un lascito di più di 10 000 volumi di materia scientifica, che comprende manoscritti, incunaboli, cinquecentine e edizioni dal xvii al xix secolo, donati nel 1973 alla sede di Brescia dell’Università Cattolica del Sacro Cuore da parte dell’ingegnere Carlo Viganò, con lo scopo di renderli disponibili agli studiosi.

La griglia di Cardano

La griglia permette di nascondere un messaggio riservato all'interno di un messaggio più lungo ed avente un significato del tutto diverso. In tal modo chi intercettasse il messaggio non si renderebbe neanche conto della presenza di un messaggio nascosto. Nel linguaggio cinquecentesco si parlava di cifre non sospette.

Cardano raccomanda di usare due fogli a righe uguali, di ritagliare su uno di questi una serie di finestrelle di 5-10 posti, da distribuire a caso per un totale di 120 posti, sufficienti per un messaggio breve. Sovrapponendo il foglio così forato, la griglia, al foglio integro si scriverà il messaggio nelle finestrelle. Fatto questo si rimuove la griglia e si riempiono i posti rimasti vuoti con un messaggio fittizio in modo da mimetizzarvi il messaggio vero; Cardano dice che conviene provare, cancellare e riscrivere fino ad avere un testo plausibile.

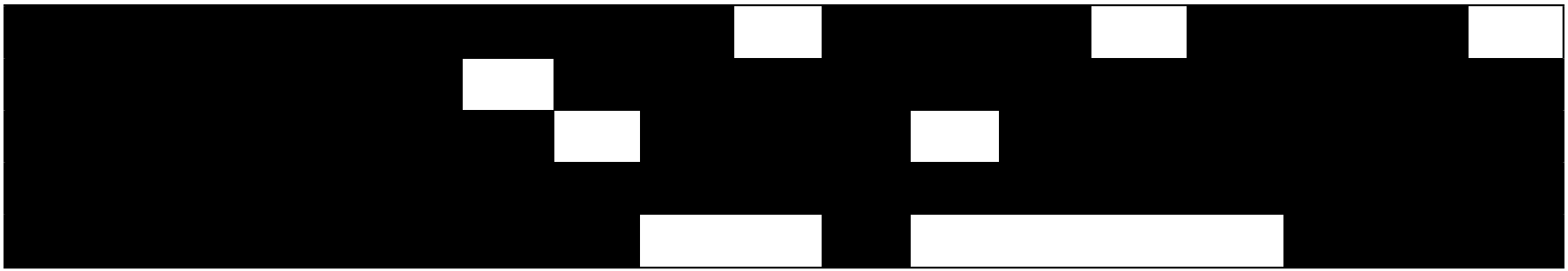
Griglia di Cardano

Il destinatario del messaggio, che deve ovviamente disporre di una copia identica della griglia, la andrà a sovrapporre al testo ricevuto e potrà facilmente leggere il messaggio segreto. Sul foglio potrà esserci un punto che indichi dove posizionare il vertice in alto a sinistra del foglio con il messaggio in modo che le finestrelle cadano nella giusta posizione.

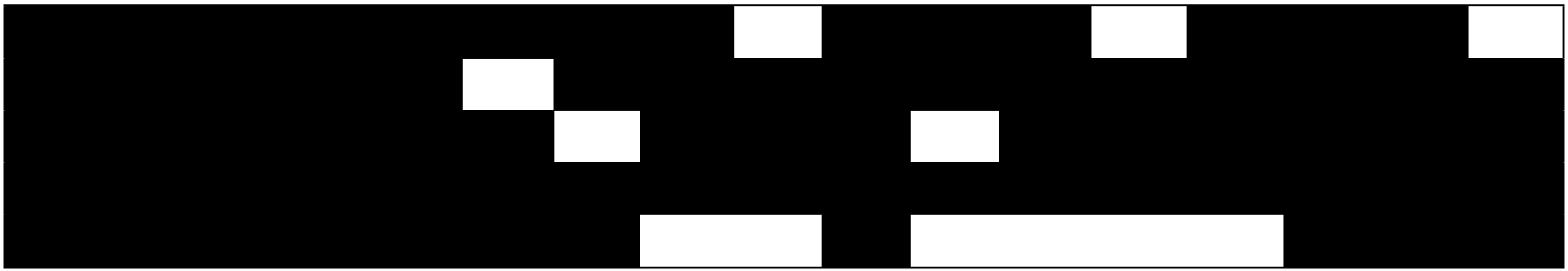
Questo metodo ha come scopo quello di mimetizzare il messaggio segreto in un messaggio chiaro e di aspetto innocuo, potenzialmente in grado di sfuggire all'attenzione di un potenziale nemico, insomma non sospetto, insospettabile.

Uno degli estimatori ed utilizzatori della griglia di Cardano era il cardinale Richelieu, che usava questo metodo sia nella sua corrispondenza privata che in quella diplomatica.

Griglia di Cardano

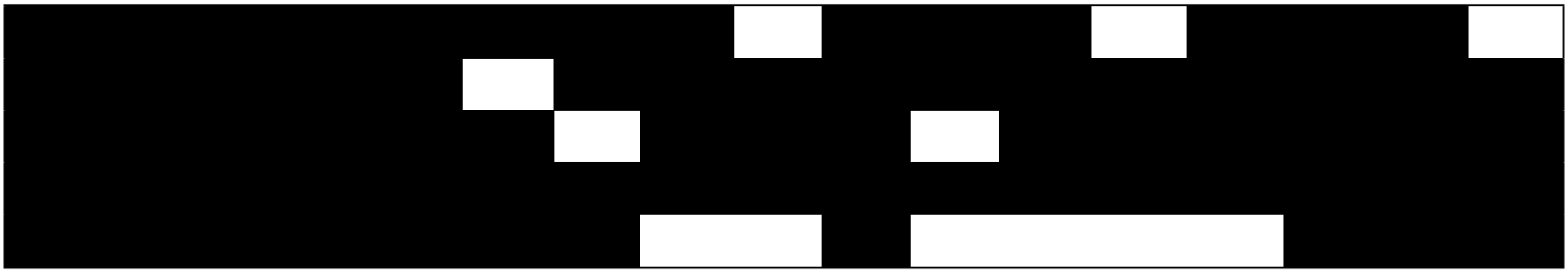


Griglia di Cardano

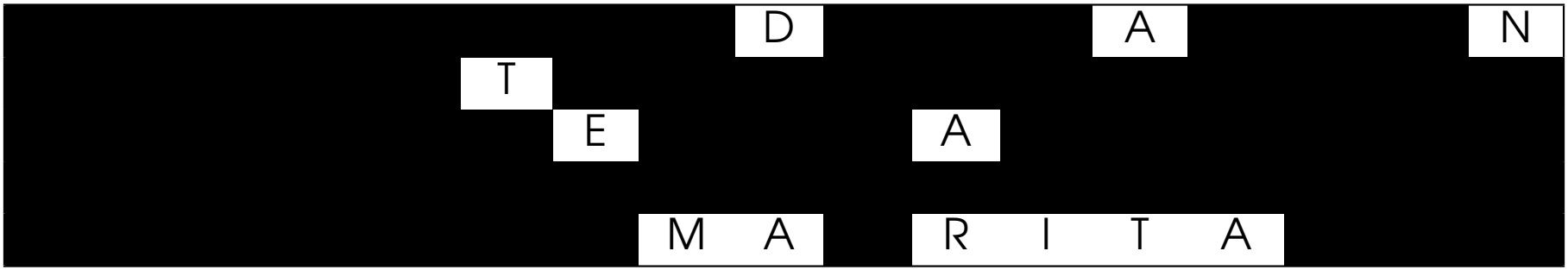


N	E	L	M	E	Z	Z	O	D	E	L	C	A	M	M	I	N
D	I	N	O	S	T	R	A	V	I	T	A	M	I	R	I	T
R	O	V	A	I	P	E	R	U	N	A	S	E	L	V	A	O
S	C	U	R	A	C	H	E	L	A	D	I	R	I	T	T	A
V	I	A	E	R	A	S	M	A	R	R	I	T	A			

Griglia di Cardano

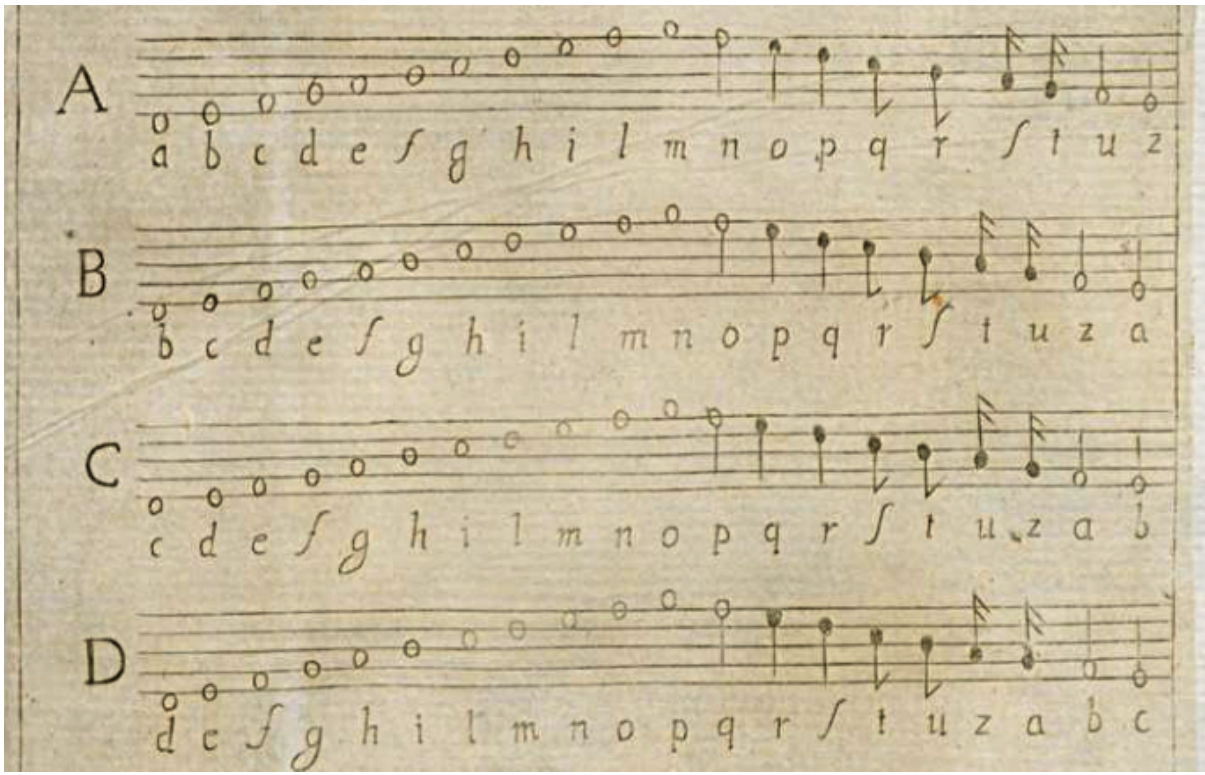


N	E	L	M	E	Z	Z	O	D	E	L	C	A	M	M	I	N
D	I	N	O	S	T	R	A	V	I	T	A	M	I	R	I	T
R	O	V	A	I	P	E	R	U	N	A	S	E	L	V	A	O
S	C	U	R	A	C	H	E	L	A	D	I	R	I	T	T	A
V	I	A	E	R	A	S	M	A	R	R	I	T	A			



Francesco Lana Terzi

Sistemi steganografici basati sulla sostituzione "lettera $\rightarrow$ nota musicale" furono proposti dal gesuita bresciano Francesco Lana Terzi (1631–1687) nella sua opera *Prodromo all'arte maestra*.

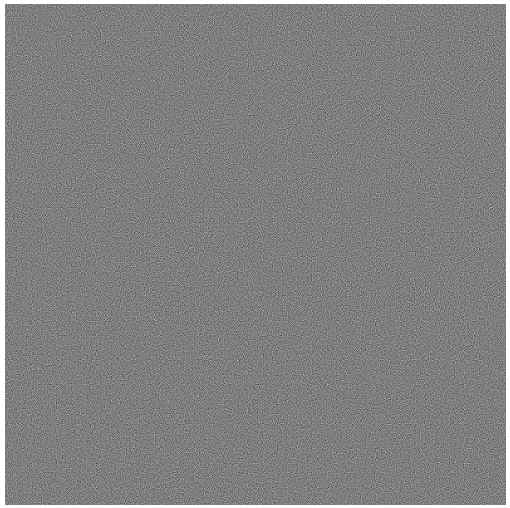


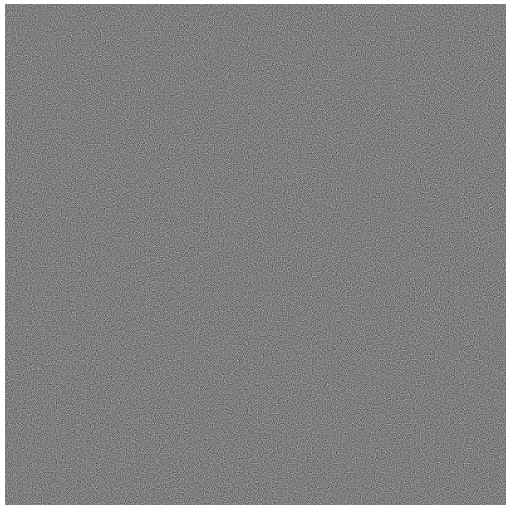
Crittografia Visuale

La steganografia viene oggi utilizzata per nascondere messaggi segreti all'interno di immagini digitali.

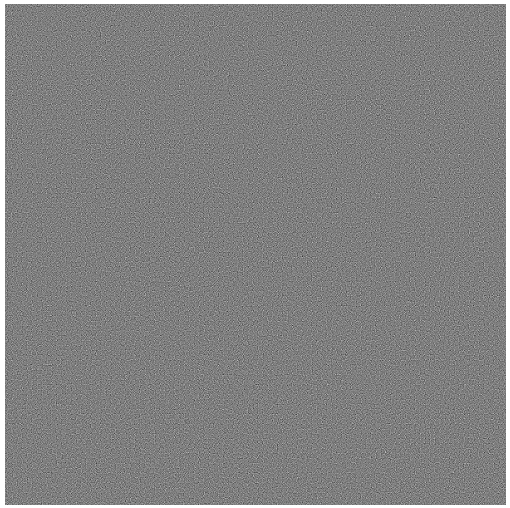
In particolare, la Crittografia Visuale permette di nascondere un messaggio segreto all'interno di varie immagini da distribuire a più persone: solo sovrapponendo un certo numero di tali immagini è possibile recuperare l'informazione.

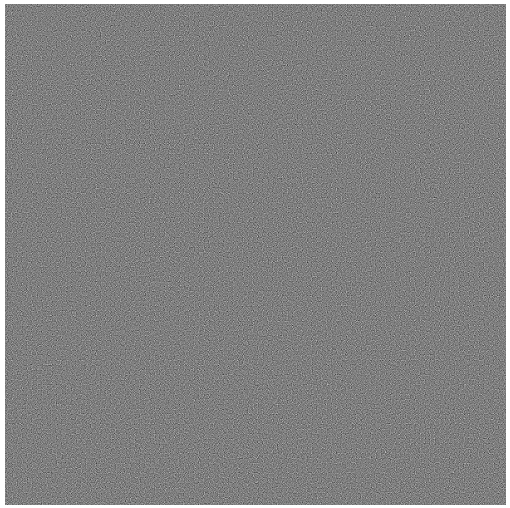
Crittografia Visuale





Crittografia Visuale





Cifrari polialfabetici

Un cifrario a sostituzione polialfabetica utlizza un numero variabile di alfabeti per sostituire le lettere del messaggio, usando un determinato ordine che costituisce la chiave, in modo da resistere all'Analisi delle Frequenze.

Disco cifrante di Leon Battista Alberti (1404–1472)

Disco cifrante di Leon Battista Alberti

Il disco cifrante di Leon Battista Alberti, descritto nel *De cifris* intorno al 1467, è il primo sistema di cifratura polialfabetica.

Si compone di due dischi concentrici, rotanti uno rispetto all'altro, contenenti un alfabeto ordinato per il testo in chiaro e un alfabeto disordinato per il testo cifrato.

Permette la sostituzione polialfabetica con periodo irregolare. Lo scorrimento degli alfabeti avviene per mezzo di lettere chiave inserite nel corpo del crittogramma.

Disco cifrante di Leon Battista Alberti

Usa come indice una lettera minuscola scelta nel cerchio interno (mobile). Stabilita la g come lettera indice e avendola giustapposta alla A maiuscola del cerchio esterno, lo sviluppo dei due alfabeti è il seguente:

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

Messaggio da trasmettere: VIVA LA MATEMATICA:

Plaintext:		V	I	V	A	2	L	A
Ciphertext:	A	h	v	h	g	a	z	g

Si inserisce la lettera chiave A nel ciphertext all'inizio e in maiuscolo.

Disco cifrante di Leon Battista Alberti

Dopo aver cifrato alcune lettere si inserisce nel cifrato un'altra lettera maiuscola (Q) ruotando il disco mobile in modo da ottenere le nuove corrispondenze:

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

La cifratura continuerà così:

Plaintext:		M	A	T	E	M	4	A	T	I	C	A
Ciphertext:	Q	b	y	n	q	b	x	y	n	f	o	y

Il risultato finale sarà quindi:

Plaintext:	`VIVA2LAMATEM4ATICA`
Ciphertext:	`AhvhgazgQbynqbxynfoy`

Cifrari polialfabetici: Giovan Battista Bellaso

Per utilizzare il disco cifrante di Alberti, bisogna indicare nello stesso corpo del ciphertext le lettere di riferimento che determinano lo scorrimento dell'alfabeto cifrante rispetto a quello in chiaro.

Il bresciano Giovan Battista Bellaso (1505-??) fu il primo a proporre di individuare la serie degli alfabeti messi in gioco per mezzo di un versetto convenuto, oltre ad insegnare vari modi per formare alfabeti cifranti mischiati allo scopo di liberare i corrispondenti dalla necessità di scambiarsi dischi o tabelle precompilate.

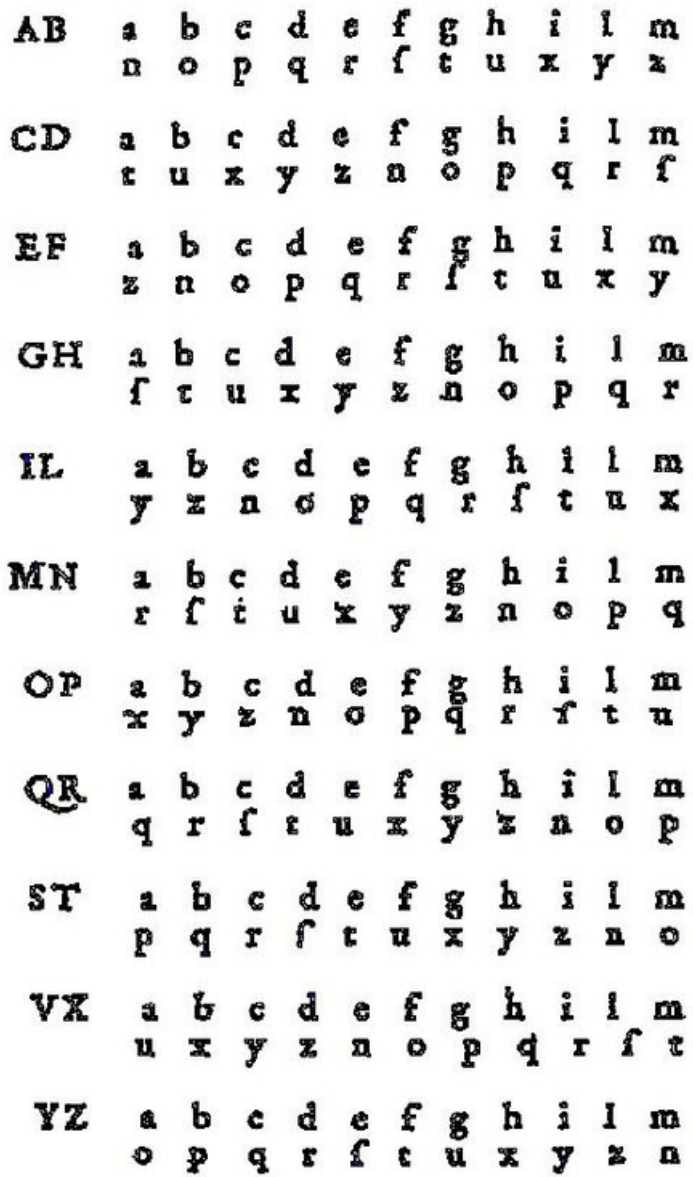
Nel 1553 venne stampato a Venezia *La cifra del Sig. Giovan Battista Belaso, gentil'huomo bresciano, nuovamente da lui medesimo ridotta à grandissima breuità & perfettione*.

In quest'opera si trova la tavola reciproca formata scorrendo la metà inferiore dell'alfabeto di un numero apparentemente irregolare di posti rispetto alla parte superiore.

Cifrari polialfabetici: Giovan Battista Bellaso

La cifratura avviene mediante l'uso di un versetto convenuto fra i due corrispondenti, chiamato contrassegno, che viene sovrapposto al testo da cifrare.

Facendo riferimento alla tavola, si sostituisce alla lettera del chiaro quella che le è sovrapposta o sottoposta nell'alfabeto identificato dalla lettera (maiuscola) del contrassegno.

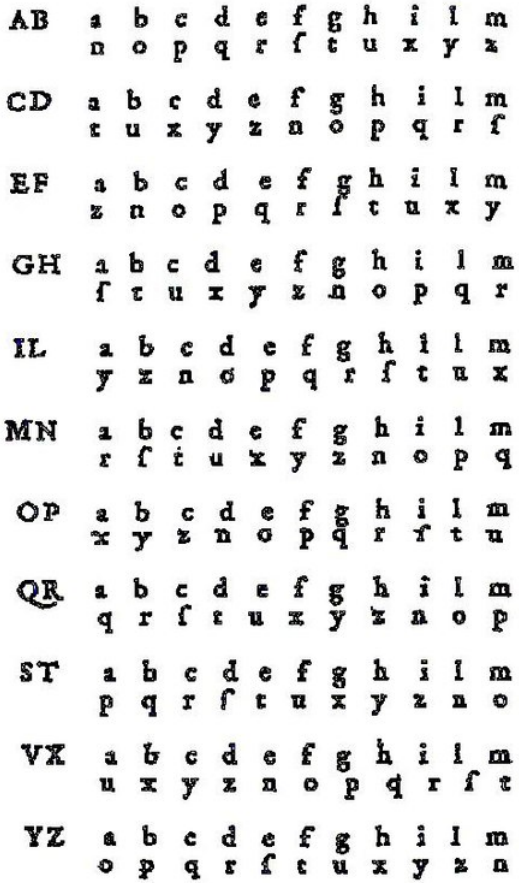


Cifrari polialfabetici: Giovan Battista Bellaso

Contrassegno:	E	N	I	G	M	A	E	N
Plaintext:	v	i	v	a	l	a	m	a
Ciphertext:	i	o	l	s	p	n	y	r
Contrassegno:	I	G	M	A	E	N	I	G
Plaintext:	t	e	m	a	t	i	c	a
Ciphertext:	i	y	q	n	h	o	n	s

Il risultato finale sarà quindi:

Plaintext:	`viva la matematica`
Ciphertext:	`iols pn yriyqnhons`



Cifrari polialfabetici: Giovan Battista Bellaso

Il secondo volumetto, *Novi et singolari modi di cifrare de l'eccellente dottore di legge Messer Giovan Battista Bellaso nobile brescian*, stampato a Brescia nel 1555, è una continuazione del primo e contiene una tavola compilata spostando metà dell'alfabeto in modo regolare.

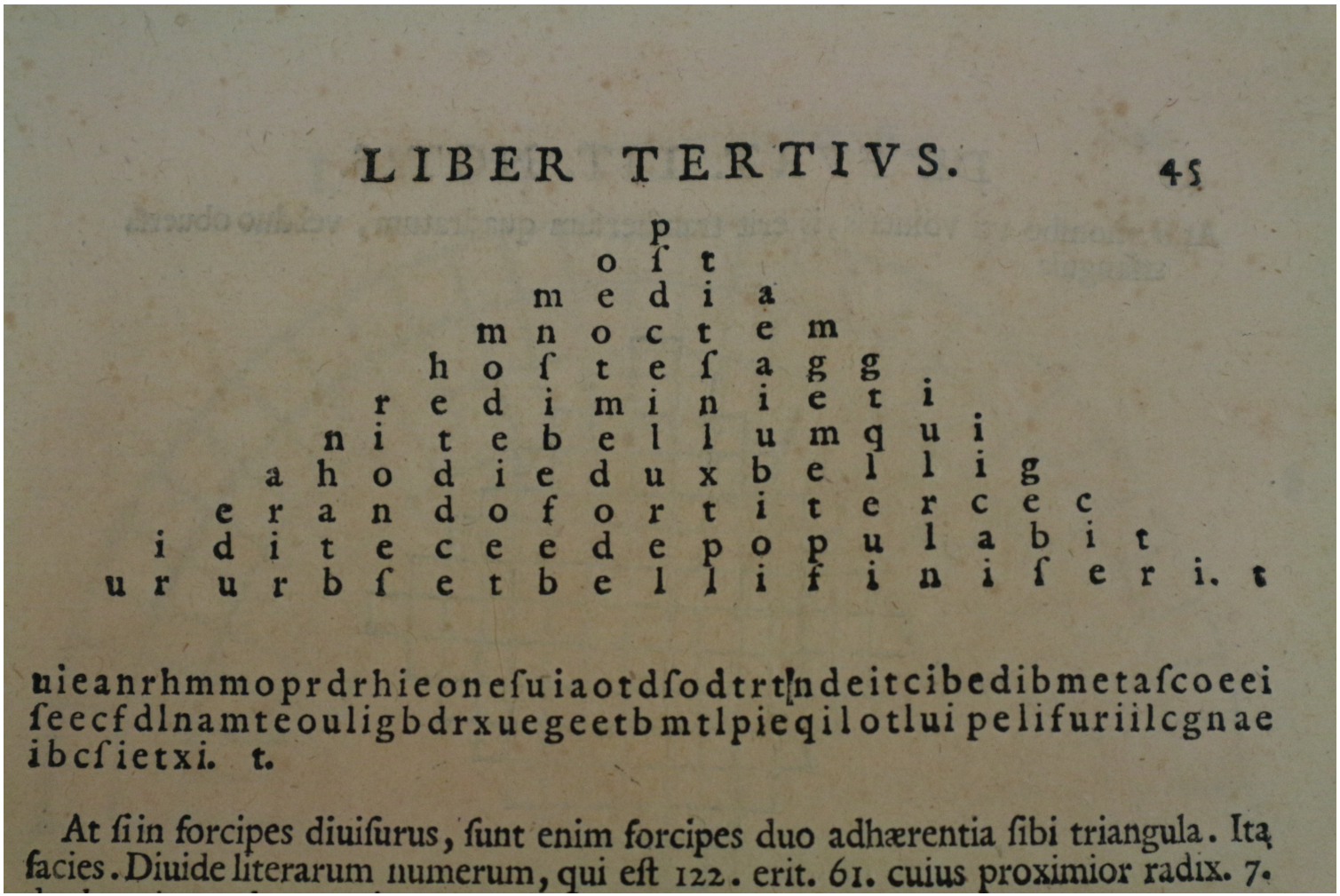
Nel 1564 venne stampato, sempre a Brescia, *Il vero modo di scrivere in Cifra con facilità, prestezza, et securezza di Misser Giovan Battista Bellaso, gentil'huomo bresciano*. Questo trattato è il riepilogo e la continuazione di entrambi i lavori precedenti. Gli alfabeti che formano queste tavole sono generati mnemonicamente per mezzo di una breve parola chiave.

Da Bellaso a Lana Terzi

Il metodo di Bellaso fu descritto anche da Lana Terzi.

Giovanni Battista Della Porta

Anche il filosofo campano Giovanni Battista Della Porta (1535–1615) si occupò di crittografia. Nel suo *De Furtivis Literarum Notis* descrive vari metodi creativi.



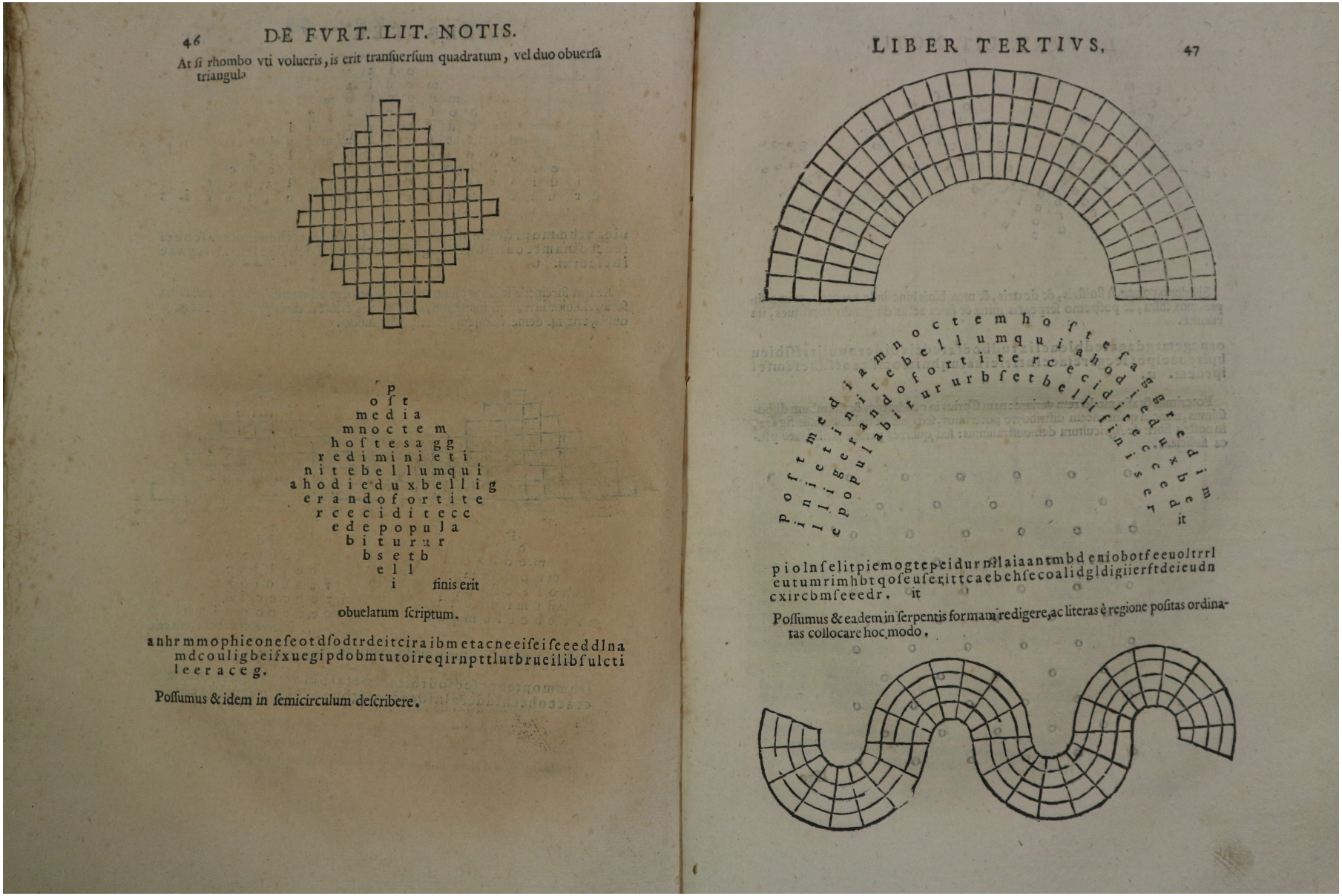
LIBER TERTIVS. 45

p
o ſ t
m e d i a
m n o c t e m
h o ſ t e ſ a g g
r e d i m i n i e t i
n i t e b e l l u m q u i
a h o d i e d u x b e l l i g
e r a n d o f o r t i t e r c e c
i d i t e c e e d e p o p u l a b i t
u r u r b ſ e t b e l l i f i n i ſ e r i. t

uieanrhmmoprdrhieoneſuiaotdſodtrtndeitcibedibmetaſcoeei
ſeecfdlnamteouligbdrxuegeetbmtlpieqilotlui pelifuriilcgnae
ibcſietxi. t.

At ſi in forcipes diuiſurus, ſunt enim forcipes duo adhærentia ſibi triangula. Ita facies. Diuide literarum numerum, qui eſt 122. erit. 61. cuius proximior radix. 7.

Giovanni Battista Della Porta



46 DE FVRT. LIT. NOTIS.

At ſi rhombo vti volueris, is erit tranſuerſum quadratum, vel duo obuerſa triangula

p
o ſ t
m e d i a
m n o c t e m
h o ſ t e s a g g
r e d i m i n i e t i
n i t e b e l l u m q u i
a h o d i e d u x b e l l i g
e r a n d o f o r t i t e
r c e c i d i t e c c
e d e p o p u l a
b i t u r u r
b s e t b
e l l
i finis erit

obuelatum ſcriptum.

anhrmmophieoneſeotdſodtrdeitciraibmetacneeiſeiſeeeddlna
mdcouligbeifxuegipdobmtutoireqirnpttlutbrueilibſulcti
leeraceg.

Poſſumus & idem in ſemicirculum deſcribere.

LIBER TERTIVS. 47

piolnſelitpiemogtepeidurmilaiaantmbd eniobotfeeuoltrrl
eutumrimhbtqoſeuſeritttcaebehſecoalidgldigiierftdeieudn
cxircbmſeeedr. it

Poſſumus & eadem in ſerpentis formam redigere, ac literas è regione poſitas ordinatas collocare hoc modo.

Giovanni Battista Della Porta

Giovanni Battista Della Porta

Il Cifrario di Vigenère

Blaise de Vigenère (1523–1596) intraprese il suo primo viaggio in Italia nel 1549, in particolare a Roma. A questo viaggio che durò dai tre ai quattro anni, ne seguirà un altro nel 1566 per altri tre anni.

Durante i suoi viaggi in Italia, Vigenère lesse libri di crittografia ed entrò in contatto con vari crittografi.

Il cifrario di Vigenère è un metodo crittografico in cui ogni lettera del testo in chiaro è codificata con un diverso cifrario di Cesare, il cui incremento è determinato dalla lettera corrispondente di un altro testo, la chiave.

Il Cifrario di Vigenère

Sfruttando l'alfabeto di 26 lettere, nel cifrario di Vigenère, la lettera A corrisponde a uno shift di 0 posizioni, la B a uno shift di 1 posizione, la C a uno shift di 2 posizioni, e così via.

Chiave:	E	N	I	G	M	A	E	N
Plaintext:	v	i	v	a	l	a	m	a
Ciphertext:	z	v	d	g	x	a	q	n
Chiave:	I	G	M	A	E	N	I	G
Plaintext:	t	e	m	a	t	i	c	a
Ciphertext:	b	k	y	a	x	v	k	g

Il risultato finale sarà quindi:

Plaintext:	`viva la matematica`
Ciphertext:	`zvdg xa qnbkyaxvkg`

Il Cifrario di Vigenère

Il celebre cifrario di Vigenère prende chiara ispirazione da quello di Bellaso. Si noti, tuttavia, che a differenza del moderno cifrario di Vigenère, il cifrario di Bellaso non prevedeva 26 "shift" diversi (diversi cifrari di Cesare) per ogni lettera, ma solo 13 shift per ogni coppia di lettere.

Nel XIX secolo, l'invenzione di questo cifrario, essenzialmente progettato da Bellaso, fu erroneamente attribuita a Vigenère.

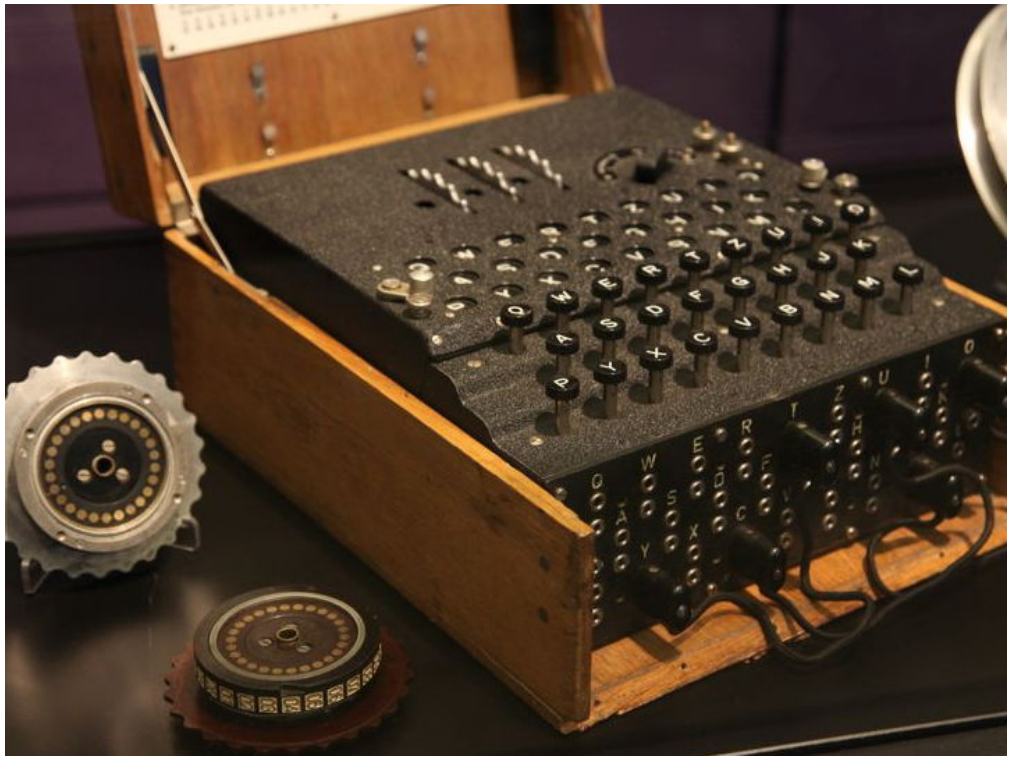
Il cifrario di Vigenère si guadagnò la reputazione di essere eccezionalmente robusto. Il noto autore e matematico Charles Lutwidge Dodgson (Lewis Carroll) definì il cifrario di Vigenère inviolabile nel suo articolo del 1868 *The Alphabet Cipher* su una rivista per bambini. Nel 1917, la rivista SCIENTIFIC AMERICAN descrisse il cifrario di Vigenère come "impossibile da tradurre".

In realtà, già nel 1863, Friedrich Kasiski aveva pubblicato un metodo generale per decifrare messaggi generati utilizzando il cifrario di Vigenère.

Enigma

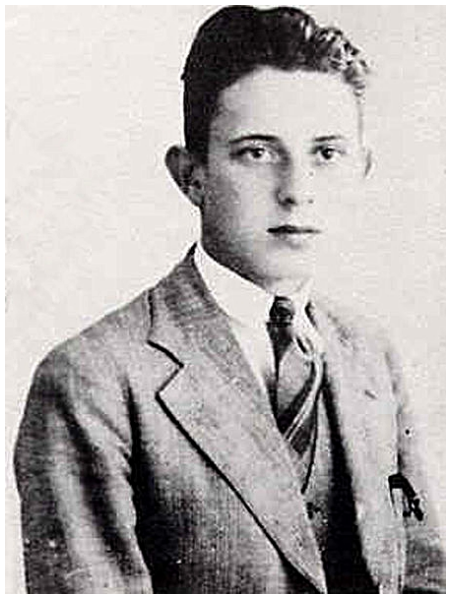
I metodi crittografici visti sfruttano solo competenze linguistiche. La necessità di coinvolgere anche i Matematici per realizzare o rompere crittosistemi emerse con piena forza negli anni Trenta del xx secolo, quando l'esercito tedesco iniziò ad utilizzare le macchine Enigma.

Una macchina Enigma permette di rendere automatico e molto facile l'utilizzo di un sistema crittografico polialfabetico estremamente sicuro.



Enigma

I polacchi, temendo un'invasione da parte dei tedeschi, cercarono di capire come poter decifrare un messaggio realizzato utilizzando Enigma. A tale scopo furono assunti nel 1932 tre matematici, oggi considerati eroi nazionali: Marian Rejewski (1905–1980), Jerzy Rozycki (1909–1942) e Henryk Zygalski (1908–1978).


Crittografia matematica

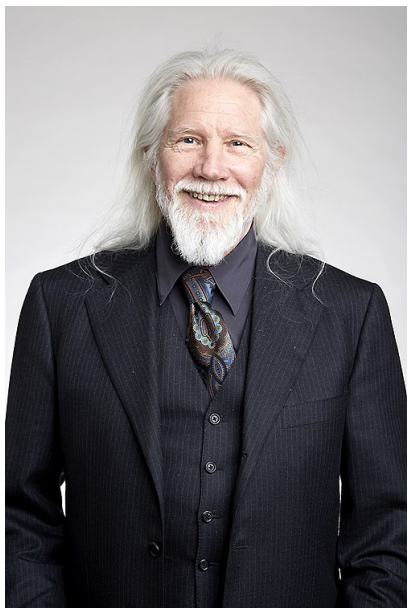
L'avvento dell'Informatica moderna e la digitalizzazione di molti processi ha spinto a cercare nella Matematica soluzioni sempre più sicure. In particolare, discipline come la Teoria dei Numeri, l'Algebra e la Geometria sono in grado di fornire quelle basi teoriche necessarie per la creazione di crittosistemi.

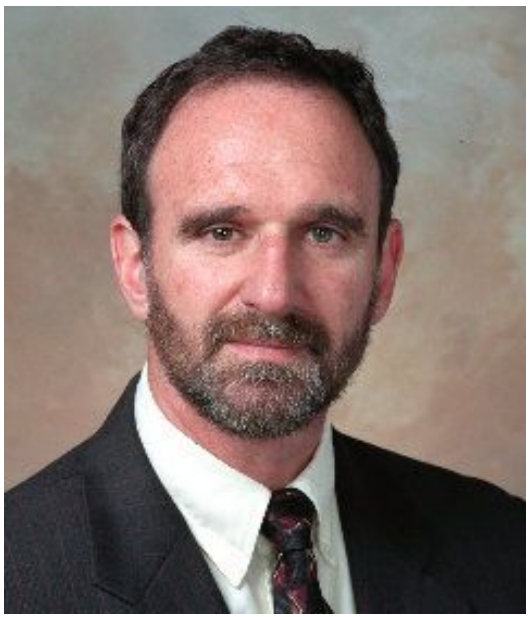
Una vera rivoluzione avvenne negli anni Settanta con l'introduzione di sistemi crittografici a chiave pubblica.

Diffie-Hellman

Lo scambio di chiavi Diffie-Hellman è un protocollo crittografico, ideato nel 1976 da Whitfield Diffie (1944–) e Martin Hellman (1945–), che consente a due persone (computer) di stabilire una chiave condivisa e segreta utilizzando un canale di comunicazione insicuro (pubblico) senza la necessità che le due parti si siano scambiate informazioni o si siano incontrate in precedenza. La chiave ottenuta mediante questo protocollo può essere successivamente impiegata per cifrare le comunicazioni successive tramite uno schema di crittografia simmetrica.

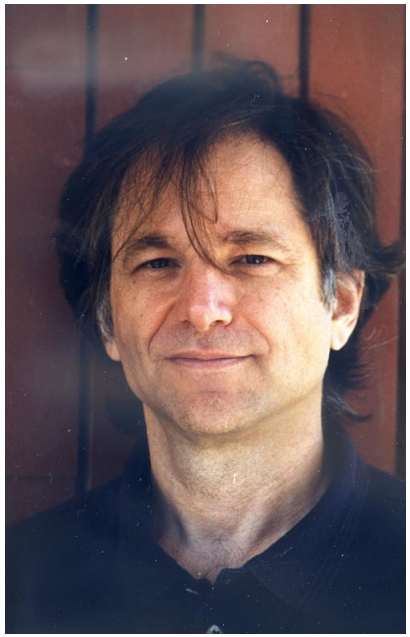
Esso sfrutta l'Aritmetica modulare e il logaritmo discreto.





RSA

In crittografia la sigla RSA indica un algoritmo di crittografia asimmetrica, inventato nel 1977 da Ronald Rivest (1947–), Adi Shamir (1952–) e Leonard Adleman (1945–) utilizzabile per cifrare o firmare informazioni.



RSA

L'algoritmo RSA si basa sulla difficoltà di fattorizzare un numero molto grande in prodotto di numeri primi. Quindi, anche se qualcuno ha accesso all'informazione cifrata e alla chiave pubblica, è molto difficile per loro scoprire la chiave privata che è necessaria per decodificare il messaggio. Questa caratteristica rende l'algoritmo RSA molto sicuro e per questo viene utilizzato per proteggere molte comunicazioni online, come per esempio i pagamenti online o le comunicazioni via e-mail.

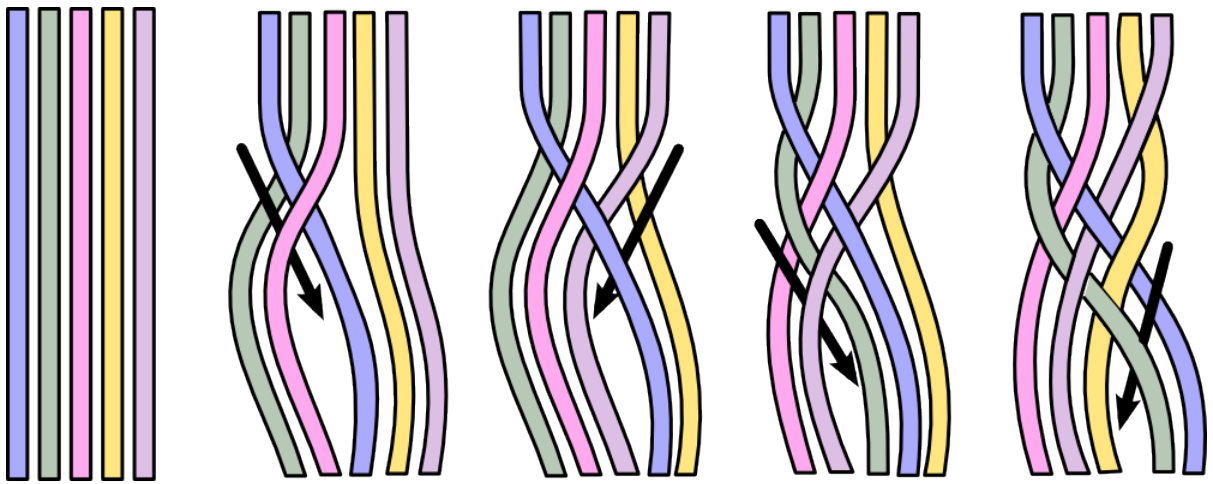
Il sistema RSA sfrutta il Teorema di Eulero e si basa sull'esistenza di due chiavi distinte, che vengono usate per cifrare e decifrare. La questione fondamentale è che, nonostante le due chiavi siano fra loro dipendenti, non è possibile risalire dall'una all'altra, in modo che se anche si è a conoscenza di una delle due chiavi, non si possa risalire all'altra, garantendo in questo modo l'integrità della crittografia.

Crittografia post-quantistica

La possibile futura diffusione di calcolatori quantistici viene percepita come una seria minaccia per la sicurezza di metodi come lo scambio Diffie-Hellman e l'algoritmo RSA.

Lo statunitense NIST (National Institute of Standards and Technology) sta già vagliando sistemi crittografici che dovrebbero resistere anche all'attacco tramite l'utilizzo di Computer Quantistici.

Questi metodi sfruttano concetti algebrici come i gruppi infiniti o geometrici come i codici.

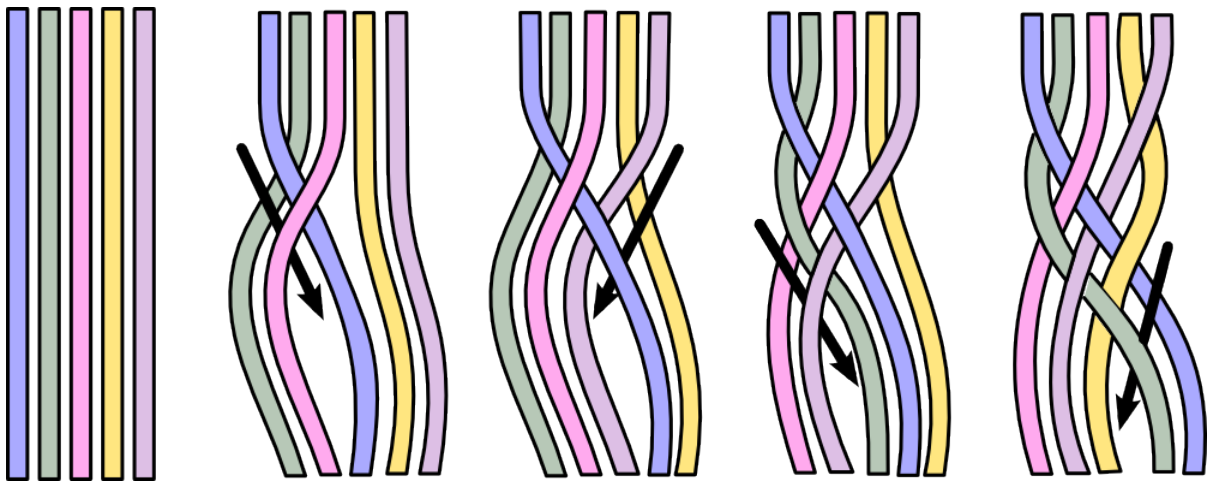


Crittografia post-quantistica

La possibile futura diffusione di calcolatori quantistici viene percepita come una seria minaccia per la sicurezza di metodi come lo scambio Diffie-Hellman e l'algoritmo RSA.

Lo statunitense NIST (National Institute of Standards and Technology) sta già vagliando sistemi crittografici che dovrebbero resistere anche all'attacco tramite l'utilizzo di Computer Quantistici.

Questi metodi sfruttano concetti algebrici come i gruppi infiniti o geometrici come i codici.



Grazie per l'attenzione!

Fonti

- Simon Singh, Codici & Segreti, Rizzoli, 1999.
- Margaret Cozzens, Steven J. Miller, The Mathematics of Encryption, American Mathematical Society, 2013.
- Wikipedia.
- Immagini di opere custodite nella Biblioteca di Storia delle Scienze "Carlo Viganò", Università Cattolica del Sacro Cuore.
- Immagini prese da Internet.