Dall'arte alla matematica:

anamorfosi

steganografia

crittografia

Giorgio Mainini, SMASI

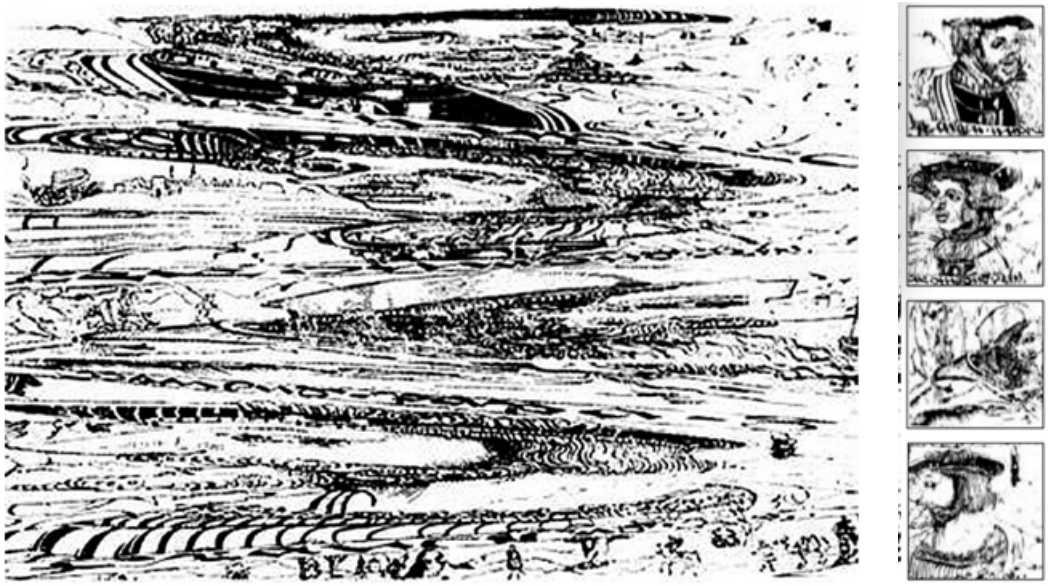
Anamorfosi

L'**anamorfòsi**, da ανά (*anà* = in su, indietro) e μορφή (*morfé* = forma), è la raffigurazione di un oggetto secondo una prospettiva diversa da quella centrale, in modo che risulti quasi invisibile. L'oggetto ridiventa visibile se l'osservatore si colloca in un ben preciso punto (o usa un appropriato strumento).

Qualche bella immagine per cominciare

Leonardo da Vinci [1]

Erhard Schön [2]



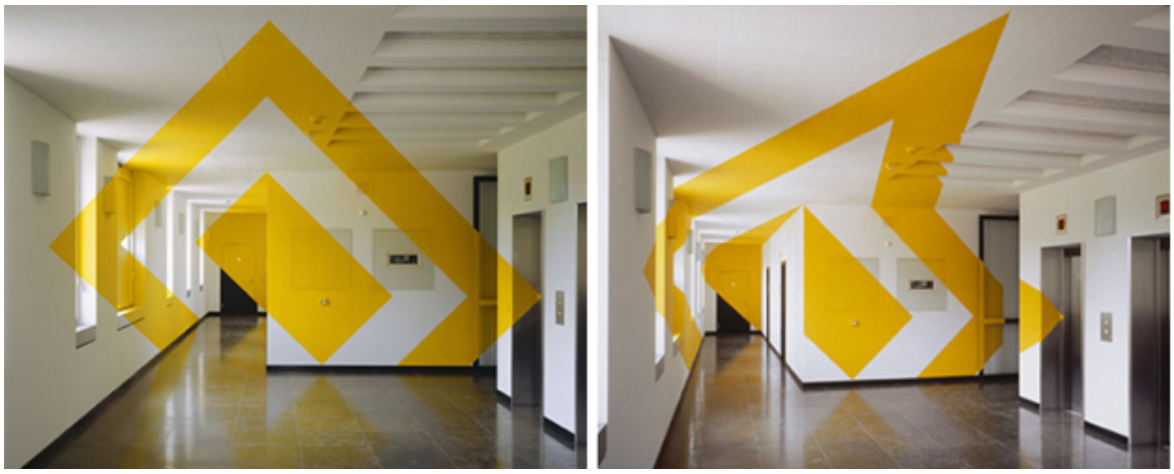
[1] Anchiano, 1452 – Amboise, 1519

[2] Norimberga, ca. 1491– Norimberga, 1542

Hans Holbein il Giovane [3]

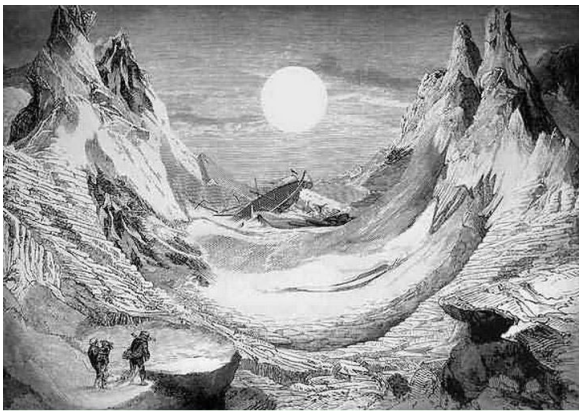
[3] Augusta, 1497/'98 – Londra, 1543

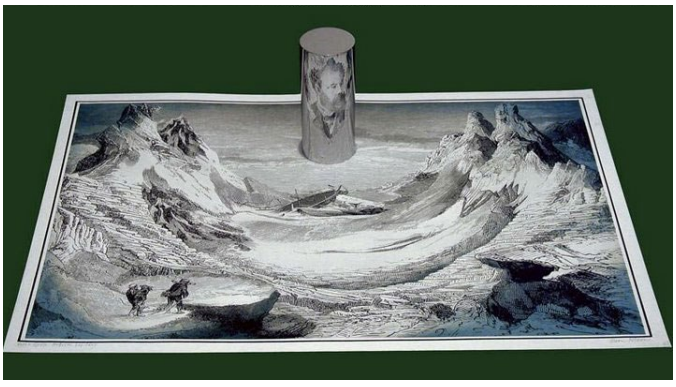
Felice Varini [4]



Street Art
Gruppo Boa Mistura

Istvan Orosz [5]





Vedi anche Leon Keer, Edgar Müller, Julian Beever, Kurt Wenner

[4] Locarno, 1952 – vivente
[5] Kecskemét, 1951 - vivente

Anamorfosi quotidiane


BUS




30

30

Steganografia

La **steganografia** è una tecnica che si prefigge di ***nascondere*** la comunicazione tra due interlocutori; infatti il termine è composto appunto dalle parole greche στεγανός (*steganòs* = coperto) e γραφία (*grafia* = scrittura).
Di solito i messaggi steganografici sono contenuti in documenti di qualsiasi tipo, **documenti digitali compresi** (messaggi, musiche, immagini, filmati, …)

Erodoto [6]

scrive ne "Le Storie" che durante le guerre dei Greci contro i Persiani di Serse, ca. 500 – 480 a.C., fu usato questo metodo: da una tavoletta ricoperta di cera si grattava via la cera, si scriveva sul legno e si ricopriva di nuovo di cera, mostrando così una tavoletta vergine.
Si narra anche di Istieo, tiranno di Mileto, il quale rasò la testa di uno schiavo, tatuò il messaggio sul cuoio capelluto, aspettò che i capelli ricrescessero e mandò lo schiavo ad Aristagora, suo figlio adottivo.
Certo che non doveva essere un messaggio urgente…

Gerolamo Cardano [7]

propone il metodo utilizzato nell'esempio che segue:

> 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 del 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; e il ponte, che ivi congiunge le due rive, par che renda ancor più sensibile all'occhio questa trasformazione, e segni il punto in cui il lago cessa, e l'Adda rincomincia, per ripigliar poi nome di lago dove le rive, allontanandosi di nuovo, lascian l'acqua distendersi e rallentarsi in nuovi golfi e in nuovi seni. La costiera, formata dal deposito di tre grossi torrenti, scende appoggiata a due monti contigui, l'uno detto di san Martino, l'altro, con voce lombarda, il *Resegone*, dai molti suoi cocuzzoli in fila, che in vero lo fanno somigliare a una sega: talché non è chi, al primo vederlo, purché sia di fronte, come per esempio di su le mura di Milano che guardano a settentrione, non lo discerna tosto, a un tal contrassegno, in quella lunga e vasta giogaia, dagli altri monti di nome più oscuro e di forma più comune.

[6] Alicarnasso, 484 a.C. – Thurii, dopo il 430 a.C.
[7] Pavia, 1501 – Roma, 1576. *De subtilitate*, 1554)

Se si copre il testo con un cartoncino forato nei punti giusti, ecco che appare il messaggio nascosto:

l a
s p
i a e

A
l d
o
M
o
n
t i
n
i

Oppure, con un cartoncino forato in altri punti:

v
e r
r
a e
l e

t
t
o
b e
r

g o g
l i
o

Immagini nascoste

Si vedano:

la freccia tra E e x (= FedEx è veloce),

quella tra a e z (= amazon ha tutto, dall'a alla z),

i profili di un muso di gorilla a sinistra e di una leonessa a destra.

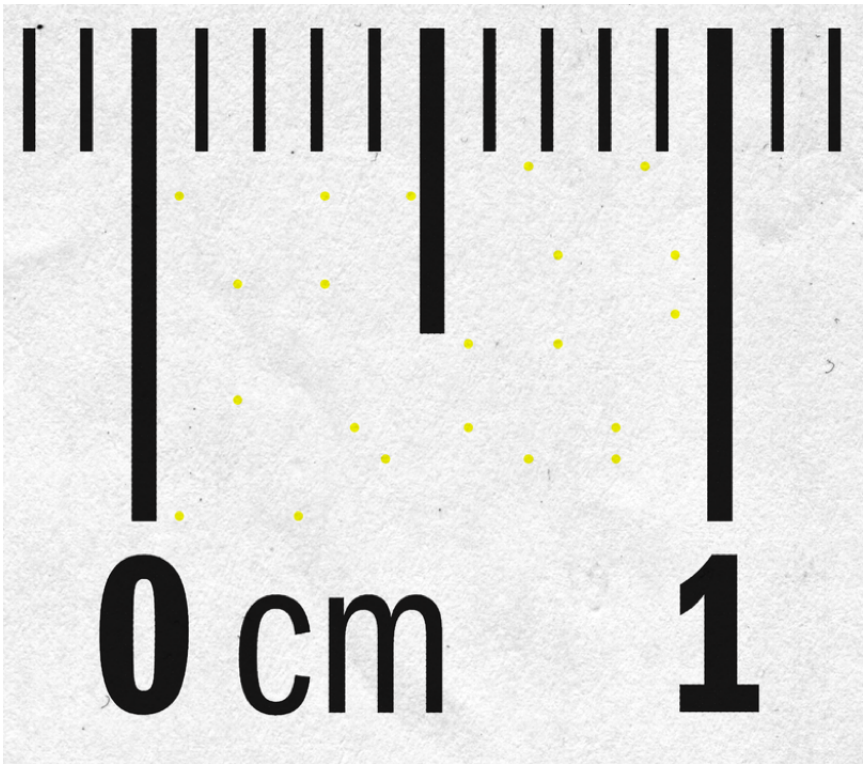
Un esempio di "steganofonia"

https://www.youtube.com/watch?v=VvckOPQhaGM

All' "Ebbene?" di Scarpia, Tosca non risponde, ma l'orchestra suona con forza due note. Ai melomani il piacere della scoperta.

I "punti gialli" delle stampanti laser

Alcune stampanti laser a colori di diversi produttori stampano minuscoli puntini gialli su ogni pagina. I puntini sono appena visibili e contengono informazioni come il numero di serie della stampante, la data e l'ora della stampa.



Altri "trucchi"

Anche inchiostri simpatici (succo di limone o di cipolla, latte, …), microfotografie nascoste, lavori a maglia con fili con nodi (alfabeto Morse) o con punti irregolari, … fanno pure parte delle tecniche steganografiche.

Crittografia

La **crittografia**, da κρυπτός (*kryptós*= nascosto) e γραφία (*grafía* = scrittura) è stata l'arte, ora branca della matematica, di **alterare** un messaggio in modo che solo chi è autorizzato possa leggerlo nella forma chiara.

Principio di Kerckhoffs [8]: la sicurezza di un sistema crittografico è basata esclusivamente sulla segretezza della chiave. In pratica si presuppone noto a priori l'algoritmo di cifratura e di decifrazione.

Atbash

Usata nel "Libro di Geremia". La parola deriva da quattro lettere ebraiche: א (alef), ת (tau), ב (beth) e ש (shin), nell'ordine la prima, l'ultima, la seconda e la penultima dell'alfabeto. In sostanza, si cifra il messaggio scambiando ogni lettera di posto ***n*** con quella che sta al posto ***23-n***, poiché l'alfabeto è di 22 lettere.
In italiano si scambierebbe la lettera di posto ***n*** con quella di posto ***22-n***:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
z	v	u	t	s	r	q	p	o	n	m	l	i	h	g	f	e	d	c	b	a

Esempio:
CRITTOGRAFIA diventa ufoddiqfzroz

Cifrario di Cesare [9]

Il metodo consiste nel sostituire ogni lettera con quella che la segue di tre posti nell'alfabeto, immaginato scritto su un anello.
In italiano si avrebbe la seguente sostituzione:

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z	a	b	c

Esempio:
CRITTOGRAFIA diventa funzzrludind

Osservazione: la debolezza dei metodi di questo tipo sta nella frequenza delle lettere, abbastanza caratteristica di ogni lingua. Si veda
https://it.wikipedia.org/wiki/Analisi_delle_frequenze

Si legga per esempio "Lo scarabeo d'oro" di Edgar Allan Poe, o qui
http://keespopinga.blogspot.ch/2012/07/crittografia-e-trigonometria-nello.html

[8] Auguste Kerckhoffs, Nuth, 1835 – Parigi, 1903
[9] Roma, 100/102 a.C. – Roma, 15 marzo 44 a.C.

Cifrario di Leon Battista Alberti [10]

Il suo metodo consiste nell'uso di due anelli concentrici simili a questi:

Sull'anello esterno c'è l'alfabeto ordinato in lettere maiuscole per il testo in chiaro, su quello interno un alfabeto disordinato in lettere minuscole. Si noti che sul cerchio esterno appaiono anche le cifre 1, 2, 3 e 4 che sono "nulle", cioè che si dovranno omettere durante la decifrazione. Nel corso della cifratura si potranno mettere lettere maiuscole che indicheranno come spostare l'anello interno. Per decifrare occorre avere una copia degli anelli e sapere qual è la corrispondenza iniziale fra i due alfabeti (nella figura sopra alla ***A*** corrisponde la ***g***).

Il metodo è piuttosto complicato, difficile da spiegare in poche parole: gli interessati vedano il sito
https://it.wikipedia.org/wiki/Disco_cifrante

[10] Genova, 1404 – Roma, 1472. *De Cifris*, ca. 1467

Cifrario di Vigenère [11]

Si tratta di un perfezionamento del cifrario di Cesare: invece di spostare ogni lettera sempre dello stesso numero di posti (tre, nel caso di Cesare), la lettera viene spostata di un numero variabile stabilito da una parola chiave, detta verme.
Con l'alfabeto inglese di 26 lettere, se il verme fosse CHIAVE, e si ponesse A=1, B=2, …, si dovrebbe spostare la prima lettera del testo in chiaro di 3 posti (C = 3), la seconda di 8 (H = 8), la terza di 9 (I = 9) e così via. Dopo la E si ricomincia con la C, fin che si raggiunge la fine del testo.
A differenza dei metodi visti fin qui, il cifrario di Vigenère lavora con numeri e non con lettere.
L'operazione di cifratura può quindi essere matematizzata nel seguente modo (alfabeto italiano di 21 lettere numerate da 0 a 20).

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z

Chiaro	S	M	A	S	I	C	H
Verme	C	H	I	A	V	E	C
	16+2	10+7	0+8	16+0	8+19	2+4	7+2
	18	17	8	16	27 (-21) 6	6	9
Cifrato	U	T	I	S	G	G	L

Vedi Tavola Vigenère, in appendice.

Il metodo di decifrazione del cifrario di Vigenère fu scoperto da Charles Babbage [12] verso il 1854 ma non fu pubblicato per motivi di sicurezza dello Stato. Nel 1863 il colonnello prussiano Friedrich Kasiski [13] pubblicò il suo metodo, che era lo stesso di Babbage.

Il "cifrario perfetto" – cifrario di Vernam [14]

Si immagini di usare, nel cifrario di Vigenère, come verme una successione casuale di lettere lunga come il testo in chiaro e che tale successione venga utilizzata una sola volta (occorre quindi creare blocco monouso, *one time pad*, OTP). Claude Shannon [15] nel 1949 dimostrò l'inviolabilità di tale sistema nell'articolo *Communication Theory of Secrecy Systems* del 1949. È ovvio che l'OTP è tutt'altro che pratico, eppure pare (pare…) che sia stato utilizzato per cifrare i messaggi sul "telefono rosso" che metteva in comunicazione i capi di Stato di USA e URSS ai tempi della guerra fredda.

[11] Saint-Pourçain-sur-Sioule, 1523 – Parigi, 1596. *Traité des chiffres où secrètes manières d'escrire*, 1586
[12] Londra, 1791 – Londra, 1871
[13] Schlochau, 1805 – Neustettin, 1881. *Die Geheimschriften und die Dechiffrir-Kunst. Mit besonderer Berücksichtigung der deutschen und der französischen Sprache*, 1863
[14] Gilbert Sandford Vernam, Brooklyn,1890 – Hackensack, 1960
[15] Claude Elwood Shannon, Petoskey, 1916 – Medford, 2001

Un grave problema

Un grave problema che affligge tutti i metodi visti fin qui consiste nel fatto che il cifratore e il decifratore devono entrambi conoscere la **stessa** chiave (**crittografia simmetrica**).
Fin che i cifratori sono pochi, la distribuzione delle chiavi, diverse per ognuna di loro, non pone problemi seri, ma quando il loro numero cresce la faccenda si fa pesante.
Nasce quindi il bisogno di trovare metodi di **crittografia asimmetrica** che consentano di cifrare con **algoritmi irreversibili** (funzioni *one way*).
Un algoritmo è irreversibile se a partire dai dati fa trovare facilmente il risultato ma che, dato il risultato, richiede una grande quantità di tentativi, e quindi di tempo, per risalire ai dati iniziali (mi scuseranno i puristi [16]).

L'idea base è questa:

> io **ti dico** quale algoritmo e quale chiave utilizzare per cifrare il messaggio che mi vuoi spedire,
> ma **non ti dico** quale algoritmo e quale chiave usare per decifrarlo.

Per il cifratore la situazione è curiosa: pur avendo a disposizione sia il testo in chiaro sia quello cifrato, non può ricostruire il primo a partire dal secondo.
In altre parole: se non fa una copia del testo in chiaro non può ricordare che messaggio ha spedito!

Primo esempio di algoritmo irreversibile

Dati i due numeri primi, è facile trovare il loro prodotto. Con un po' (tanta) pazienza e attenzione anche uno scolaro di III elementare sa eseguire questo calcolo:
11'551 x 113'327 = 1'309'040'177
Adesso si provi a trovare due numeri primi il cui prodotto è
1'335'327'673 [17].

Un possibile metodo crittografico asimmetrico potrebbe basarsi su questa difficoltà: per cifrare bisogna conoscere il numero 1'309'040'177, ma per decifrare occorre conoscere i due numeri 11'551 e 113'327.
Il primo numero costituisce la **chiave pubblica**, gli altri due la **chiave privata**.

In realtà scomporre in fattori primi un numero come 1'309'040'177 è oggi un semplice gargarismo per computer [18] ma, se il numero fosse di qualche centinaia di

---

[16] **Definizione**: Una funzione f si dice *one way* se per ogni x il calcolo computazionale di **y=f(x)** è semplice, mentre il calcolo di $\mathbf{x=f^{-1}(y)}$ è computazionalmente difficile (richiede una quantità enorme di tempo).

[17] = 31817 x 41969

[18] il sito http://factordb.com/ lo ha scomposto in 0,01 secondi, sul mio vecchio Mac. Si faccia qualche prova.

cifre, anche i supercomputer potrebbero impiegare milioni o miliardi di anni per scomporlo.
Si veda
https://it.wikipedia.org/wiki/RSA

Secondo esempio di algoritmo irreversibile

Contando i giorni della settimana lunedì = 1, martedì = 2, mercoledì = 3, …, domenica = 7, si potrebbe codificare l'affermazione "4 giorni dopo il venerdì viene il martedì" con "4 + 5 = 2".
Allo stesso modo, numerando i mesi gennaio = 1, febbraio = 2, …, dicembre = 12, si potrebbe dire, invece che "5 mesi dopo novembre viene aprile", "5 + 11 = 4".
Si dice normalmente che "4 ore dopo le 11 sono le 3", o "4 + 11 = 3".
Si noti che

nel caso dei giorni:	4 + 5 = 9	e	9 : 7 = 1	resto 2
nel caso dei mesi:	5 + 11 = 16	e	16 : 12 = 1	resto 4
nel caso delle ore:	4 + 11 = 15	e	15 : 12 = 1	resto 3

In tutti e tre i casi si calcola con quella che vien detta **addizione modulare**: nel primo il modulo è 7, negli altri due è 12. Si scrive

nel primo caso:	4 + 5 = 2 mod 7
nel secondo:	5 + 11 = 4 mod 12
nel terzo:	4 + 11 = 3 mod 12

Si può generalizzare, così:

6 + 7 = 3 mod 5	perché 6 + 7 = 13	e	13 : 5 = 2	resto 3
6 x 6 = 0 mod 4	perché 6 x 6 = 36	e	36 : 4 = 9	resto 0
7 x 8 = 1 mod 11	perché 7 x 8 = 56	e	56 : 11 = 5	resto 1
5^3 = 8 mod 13	perché 5^3 = 5 x 5 x 5 = 125	e	125 : 13 = 9	resto 8

Come si vede, l'aritmetica modulare permette di trovare facilmente le somme, i prodotti e le potenze di due numeri: basta sommare / moltiplicare / elevare a potenza, eseguire una divisione intera e trovare il resto.
È però difficile, nel caso dell'elevazione a potenza, "tornare indietro":
Quale numero devo mettere al posto di x perché sia
$3^x = 13 \bmod 17$? [19]
In realtà le soluzioni sono infinite e si cerca la più piccola.
Nell'esempio bastano pochi tentativi per trovarla ma se, invece di 3, 13 e 17, si usano numeri grandi (e primi) il numero di tentativi diventa subito enorme.
In generale: non è difficile calcolare $\mathbf{S = n^x \bmod m}$ conoscendo **n** e **x** dato **m**, ma è difficile trovare **x** conoscendo **S** e **n**, dato **m**.

[19] x = 4 perché $3^4 = 81$ e 81 : 17 = 4 resto 13

Su questa difficoltà si basa il

Cifrario di ElGamal [20]

Si procede così:
- si sceglie un numero primo **p**,
- si sceglie un numero α (che deve sottostare a una certa condizione),
- si sceglie un numero casuale **a**,
- si calcola α^a **mod p**.

La chiave pubblica è data dalla terna ordinata (**p**, α, α^a **mod p**), la chiave privata è **a**. Come si vede, **a** è all'esponente e, come scritto sopra, ricavare un esponente è un problema difficile.

Per approfondire si vedano per esempio
http://alessiorolleri.wikidot.com/crypto-elgamal
https://it.wikipedia.org/wiki/Logaritmo_discreto

I duri possono consultare
https://it.wikipedia.org/wiki/Crittografia_ellittica
https://it.wikipedia.org/wiki/Digital_Signature_Algorithm
https://it.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm

Il futuro è già cominciato

Lo stato più avanzato della crittografia è la cosiddetta **crittografia quantistica**.
Mi sono informato qua e là, per cominciare qui
https://it.wikipedia.org/wiki/Crittografia_quantistica
ma le mie competenze in fisica quantistica sono decisamente insufficienti, per non dire nulle.

[20] Taher ElGamal, Il Cairo, 1955

Appendice

Tavola di Vigenère

Vigenère, per facilitare (secondo lui) la procedura di cifratura e di decifrazione, propone di preparare una tabella come quella che segue.

Per cifrare la prima lettera di SMASICH con la prima lettera del verme CHIAVE si cerca la colonna intestata S e la si interseca con la riga intestata C: alla loro intersezione si trova la U, come visto con il calcolo.
Nel caso "complicato" della cifratura di I con V si procede allo stesso modo e si trova la G, proprio come previsto con il calcolo.

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

Volendo si può cambiare l'ordine in cui gli alfabeti spostati si susseguono, ma ciò non rende più difficile il compito del crittoanalista, cioè di colui che vuole decifrare pur non essendo il destinatario del messaggio.