INTRODUZIONE ALLE SCRITTURE SEGRETE

LA STEGANOGRAFIA

Deriva dal GRECO

steganos (coperto) grafia (scrittura)

È una tecnica che mira a nascondere il fatto stesso che vi sia stato un passaggio di informazione

Erodoto racconta la storia di un nobile persiano che fece
tagliare a zero i capelli
di uno schiavo fidato al fine di poter
tatuare un messaggio sul suo cranio

Una volta che i capelli furono ricresciuti, inviò lo schiavo alla sua destinazione, con la sola istruzione di tagliarseli nuovamente.

Nell’antica Cina

si dipingeva il messaggio su

striscioline di seta finissima

che venivano appallottolate e coperte di cera

Le palline erano poi consegnate dal messaggero

al destinatario del messaggio

Nel XVI secolo lo scienziato italiano

Della Porta

spiegò come comunicare tramite un

uovo sodo

preparando un particolare inchiostro con cui scrivere

sul guscio

L’inchiostro penetra nel guscio, che è poroso, senza lasciar tracce, e tinge l’albume solidificato. Quindi il messaggio potrà essere letto

sbucciando l’uovo

Facciamo qualche prova per vedere se riuscite a interpretare un messaggio nascosto in un altro

IL SEGUENTE INNO A ROMA RAPPRESENTA UN NUMERO IRRAZIONALE MOLTO FAMOSO. DI CHE NUMERO SI TRATTA?

Ave o Roma o Madre gagliarda di latine

virtù che tanto luminoso splendore prodiga

spargesti con la tua saggezza

IL SEGUENTE TESTO CONTIENE UN CONSIGLIO E NASCONDE IL NOME DI UNA CITTÀ. DI CHE CITTÀ SI TRATTA?

Coricati a letto! Ti aspetterebbero notti insonni sdraiato sull'enorme tappetto: troppi acari!

OGGETTI NASCOSTI NELLE IMMAGINI

Considera la copia del
dipinto “Gli ambasciatori”.
di Holbein il Giovane.

La strana figura in basso
è un esempio di **ANAMORFOSI**,
una tecnica che distorce un oggetto rendendolo
riconoscibile soltanto da una certa posizione visuale
o utilizzando uno strumento ottico.

Riesci a capire cosa rappresenta la figura distorta? Consiglio: ti conviene guardare il dipinto tenendolo all’altezza del tuo naso, il modo che soltanto l’occhio sinistro possa vedere la figura.

Abbiamo visto alcuni esempi di steganografia e abbiamo brevemente citato un altro tipo di comunicazione segreta, basata su parole usate per intenderne altre o per intendere altro.

Noi non ci occuperemo più di steganografia, concentrando l'attenzione su un altro modo per nascondere l'informazione: si tratta della

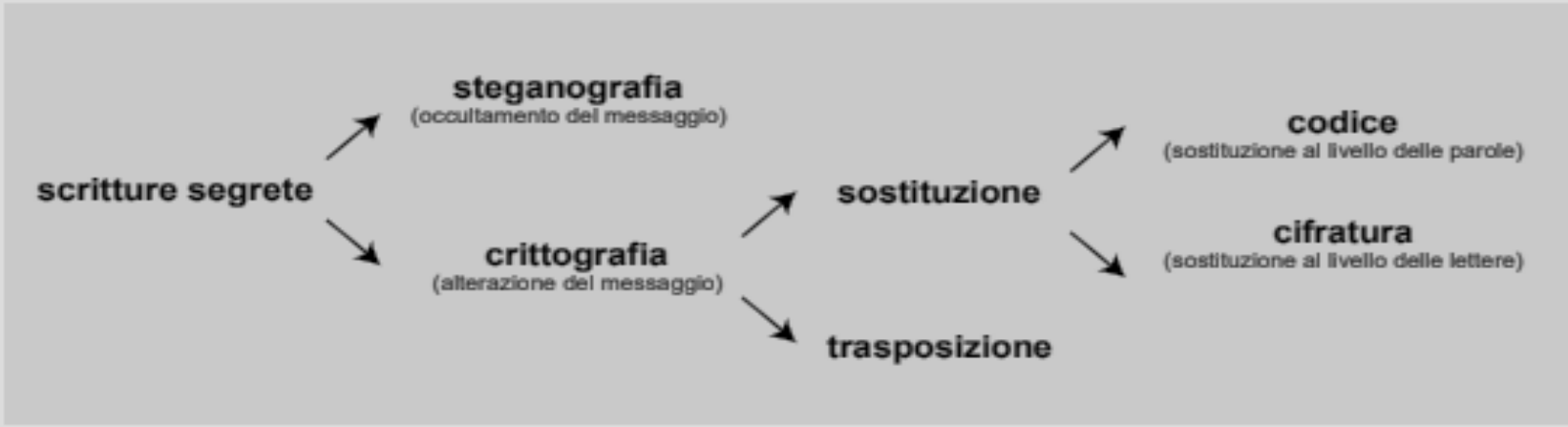
CRITTOGRAFIA

che non nasconde l'esistenza del messaggio

ma nasconde il suo significato.

Possiamo riassumere in questo schema

Scritture segrete (secondo la classificazione di S. Singh)



tratto da SIMON SINGH, "Codici e Segreti", Rizzoli, 1999

Scritture segrete (secondo la classificazione di L. Sacco)

scritture ***invisibili*** (ottenute con inchistri simpatici o procedimenti simili)
scritture ***dissimulate*** (contenute in testi apparentemente innocui)
scritture ***convenzionali*** (nelle quali alcune parole hanno un significato deciso a priori)
scritture ***cifrate*** (incomprensibili senza speciali trasformazioni)

tratto da SACCO gen. LUIGI, "Il manuale di Crittografia", Youcanprint Self-Publishing, 2014

Come vedremo, il messaggio cifrato si accompagna spesso ad una chiave.

Vedremo più in là il significato del termine e soprattutto la sua centralità concettuale.

Con la locuzione "**codice segreto**" si intende lo stesso che "cifrario

Mentre le operazioni che richiedono l'utilizzo di tale codice sono dette **cifratura**.

Una **cifratura**

nella ***CRITTOGRAFIA***

è un **ALGORITMO**

utilizzato per **ESEGUIRE OPERAZIONI**

o una serie di passaggi ben definiti

che possono essere seguiti come una **PROCEDURA**,

volte (le operazioni) a **RENDERE *OSCURO***

ossia **SEMANTICAMENTE NON LEGGIBILE**

un testo di un messaggio in chiaro (*plain text*)

o, al contrario,

al ripristino in chiaro di un messaggio precedentemente cifrato.

SEMANTICAMENTE SIGNIFICA DAL PUNTO DI VISTA SEMANTICO

Semantico significa significativo
ovvero che ha un significato

LA SEMANTICA È QUELLA PARTE DELLA LINGUISTICA CHE STUDIA IL SIGNIFICATO DELLE PAROLE

INCISO

La parola "cifra" deriva dal termine arabo صفرṣifr, che significa *vuoto*

che gli Arabi usavano per indicare il numero "0" Dopo l'introduzione in Europa dei numeri arabi, si diffuse l'uso di definire come "cifra" qualunque numero, non solo lo zero.

Si può forse ritenere che i cifrari furono definiti così perché comprensibili solo a coloro che sapevano come ricostruire il testo in chiaro, un po' come la numerazione araba che era ben diversa da quella romana e quindi nota solo a chi l'aveva studiata

CIFRARIO DI CESARE

I PIÙ SEMPLICI CIFRARI, E ANCHE I PIÙ ANTICHI, SONO I CIFRARI COSIDDETTI A SOSTITUZIONE

ESSI CONSISTONO NELLA SOSTITUZIONE DI CIASCUNA DELLE 21 LETTERE CHE COSTITUISCONO L'ALFABETO CON UN'ALTRA LETTERA DELLO STESSO ALFABETO.

IN TERMINI MATEMATICI SI TRATTA DUNQUE DI OPERARE UNA PERMUTAZIONE DELL'ALFABETO
DOVE PER PERMUTAZIONE S'INTENDE UNA FUNZIONE CHE TRASFORMA L'ALFABETO IN SE STESSO
FACENDO CORRISPONDERE A OGNI LETTERA UN'ALTRA LETTERA (IN GENERALE DIVERSA) E VICEVERSA.

Numeriamo le lettere 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

Decidiamo che la nostra chiave sia 5
Scrivi quale posto occuperanno le singole lettere dopo lo spostamento e completa la tabella

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Cifrare il seguente messaggio

"Nel mezzo del cammin di nostra vita"

Decritta il seguente messaggio
"HTIPHP L ALNZLBP"

Con chiave 15 cifrare il seguente messaggio
"DICHIARARE LA PACE TRA I POPOLI"

Decritta il seguente messaggio

DR AOVLLR V ZCFCNR

ANALISI DELLE FREQUENZE

I cifrari per sostituzione non sono molto sicuri se si dispone di un messaggio cifrato abbastanza lungo, infatti si può fare l'analisi delle frequenze e individuare le lettere più frequenti confrontandoli con quelli della lingua del messaggio in chiaro.

Tavola delle frequenze della lingua italiana:

%	Lettera	%	Lettera	%	Lettera
11,79	*e*	*5,63*	t	2,10	v
11,74	*a*	*4,98*	s	1,65	g
11,28	*i*	*4,50*	c	1,54	h
9,83	*o*	*3,73*	d	0,95	f
6,88	n	*3,05*	p	0,92	b
6,51	l	*3,02*	u	0,51	q
6,38	r	*2,52*	m	0,49	z

Tavola delle frequenze lingua italiana

Hai intercettato il seguente messaggio cifrato

T	H		I	N	U		Z	B	N	C	D	V		D	E	D	D	R		R		C	V	P	U	R

H	U	U	V		R	U	F	H	C	V		S	H		T	R	H		C	D	H	U	G	H	

Riporta nella tabella il numero di volte in cui ciascuna lettera compare nel messaggio cifrato:

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

LE CONGRUENZE E IL CIFRARIO DI CESARE

Ma la matematica dov'è?

Riprendiamo il primo esempio in cui la chiave è 5

La A in posizione 0 va in posizione 0+5=5

La B in posizione 1 va in posizione 1+5= 6

….

La S in posizione 16 va in posizione 16+5 =21 ma le posizioni possibili sono solo da 0 a 20 quindi andrà al posto della A, cioè in posizione 0

La T in posizione 17 va in posizione 17+5=22, andrà al posto della B cioè in pos izione 1

La U _____

La V _____

La Z _____

In matematica questo tipo di calcoli rientrano nell'aritmetica modulare o aritmetica dell'orologio.

Il primo ad ideare questa aritmetica fu Gauss