Associazione De Cifris
Università degli Studi di Trento – Dipartimento Matematica

SCRIVERE PER NASCONDERE, LEGGERE PER SCOPRIRE
La crittografia e lo spionaggio a Roma: un'analisi storica

Marco Moraglio

PRIMA DI ROMA

ISRAELE

I primi Israeliti fecero ampio uso di spie e codici crittografici:

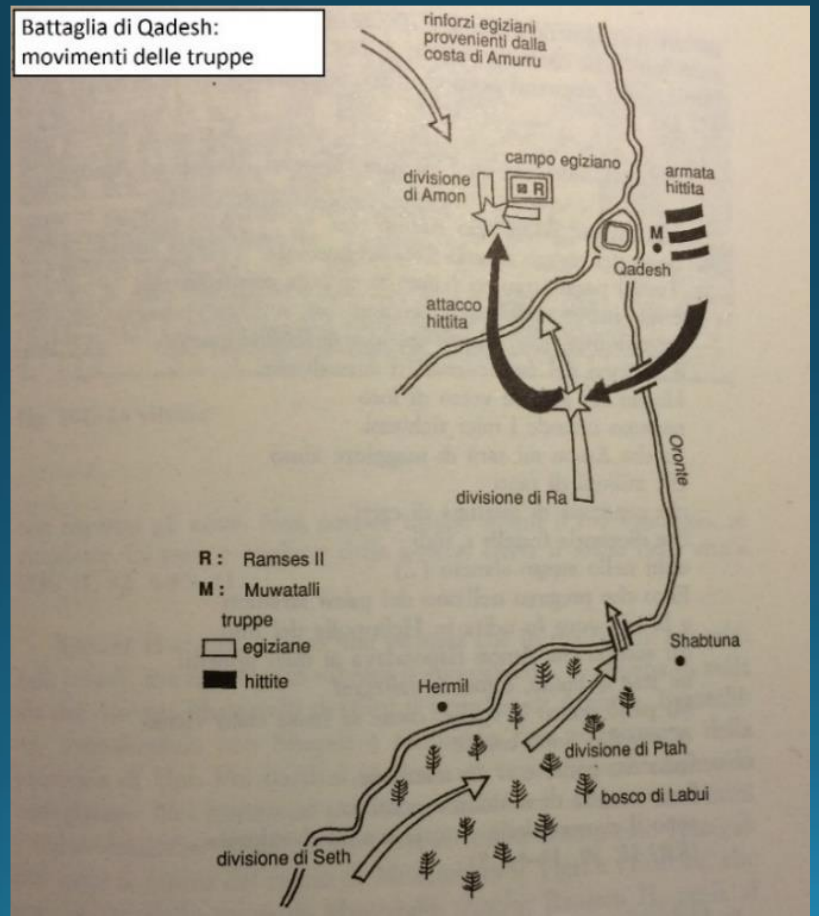
- Giuditta → Assassinio di Oloferne
- CODICE ATBASH → Il primo codice monoalfabetico mai utilizzato, nella Bibbia è utilizzato per celare il nome della città di Babele

alfabeto chiaro	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
alfabeto cifrato	ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

ANTICO EGITTO

Esistevano tre sezioni diverse dei servizi segreti egizi: la prima ricercava informazioni di carattere economico, la seconda era riservata alla protezione fisica del faraone (ed era denominata Occhi e orecchie del re) e, la terza, ricercava notizie politiche e geografiche

Il lavoro di spionaggio in Egitto può essere ben rappresentato dalla battaglia di Qadesh (aprile 1274 a.C.)



LA STEGANOGRAFIA IN ERODOTO

La steganografia cerca di occultare direttamente l'intero messaggio anziché solo il testo dello stesso; la fonte principale a cui si deve fare riferimento per studiare alcuni esempi è sicuramente Erodoto con il suo capolavoro, le Storie:

- Messaggio nel ventre della lepre
- Schiavo tatuato
- Doppia tavoletta

LA CRITTOGRAFIA IN GRECIA

Plutarco → Lisandro → **SCITALA** →

Enea Tattico tra il 390 e il 360 a.C. scrive un trattato sull'arte militare, a noi giunto solo in parte. Il XXXI capitolo, intitolato *Sui messaggi segreti* Enea riporta un elenco di 15 metodi per trasmettere segretamente un messaggio. Di questi, solo due sono esempi di crittografia mentre gli altri tredici sono esempi di steganografia. Analizziamo i due metodi crittografici:

1) Prevedeva l'utilizzo di «puntini» da inserire nella parola al posto delle vocali → era di facile decrittazione

2) Disco di Enea →

LO SPIONAGGIO A ROMA

Roma inizialmente NON utilizza un sistema di *intelligence* → Perché?

↓

MOS MAIORUM e BELLUM IUSTUM

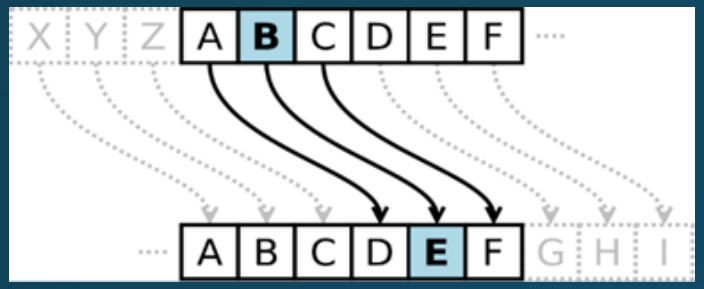
Con la Seconda Guerra Punica però cambia tutto → Cartagine da sempre faceva ampio uso di spie e trovò in Annibale il perfetto comandante che riuscì a sfruttare pienamente le potenzialità delle sue strutture di *intelligence*

Di fronte al pericolo della sconfitta la mentalità romana fu costretta a modificarsi e Scipione fu il primo a comprendere la necessità di reperire informazione ed usare stratagemmi → Invio dell'ambasceria presso Siface composta da diplomatici e centurioni che, tuttavia erano travestiti da schiavi e avevano il compito di aggirarsi nell'accampamento con lo scopo di analizzare l'esercito e studiare il posizionamento delle torrette d'avvistamento pericolose.

Conseguenza della guerra annibalica fu la paura: Roma iniziò a considerare preoccupante qualsiasi movimento si verificasse all'orizzonte e questo sentimento spinse ad un utilizzo sempre più massiccio di spie.

LA CRITTOGRAFIA A ROMA

Cifrario di **GIULIO CESARE** → Cifrario a sostituzione monoalfabetica con chiave 3



Cifrario di **AUGUSTO** → Cifrario a sostituzione monoalfabetica con chiave 1

Secondo Robert Graves, ad Augusto sarebbe ascrivibile un altro cifrario, molto più complesso che sarebbe stato poi risolto dall'imperatore Claudio. Quasi sicuramente si tratta di un'invenzione dello scrittore (non ci sono altre fonti che ne parlano) ma il metodo è interessante e vale la pena studiarlo: si tratta ancora di un cifrario a sostituzione ma, la distanza tra la lettera di partenza e quella cifrata non è fissa. Come chiave infatti viene utilizzato un testo e quindi per ogni lettera cambia la corrispondenza.

TABELLA CORRISPONDENZA LETTERE - NUMERI

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

TESTO IN CHIARO

D	E	C	I	F	R	A	L	O	S	E	C	I	R	I	E	S	C	I

TESTO CHIAVE

N	E	L	M	E	Z	Z	O	D	E	L	C	A	M	M	I	N	D	I

VALORE DELLA CHIAVE

14	5	12	13	5	26	26	15	4	5	12	3	1	13	13	9	14	4	9

Il testo cifrato si ottiene aggiungendo al valore della chiave il valore del testo in chiaro:

VALORE DELLA CHIAVE	*VALORE TESTO CHIARO*	*RISULTATO*	*TESTO CIFRATO*
N → 14	**D → 4**	**18 (14+4)**	**R**
E → 5	**E → 5**	**10 (5+5)**	**J**
L → 12	**C → 3**	**15 (12+3)**	**O**
M →13	**I → 9**	**22 (13+9)**	**V**
E → 5	**F → 6**	**11 (5+6)**	**K**

Il destinatario del messaggio riceverà così un testo apparentemente privo di senso (RJOVK…) e, per scoprire il testo in chiaro dovrà svolgere l'operazione inversa sottraendo al valore del testo cifrato, il valore della chiave

I SERVIZI DI "INTELLIGENCE" A ROMA

- **FRUMENTARII** → Origine incerta, non sappiamo il modo in cui iniziarono a essere utilizzati come spie, erano agenti sempre in movimento, furono usati per spiare i primi cristiani. Con Traiano furono riorganizzati mentre fu Diocleziano a scioglierli.

- **STATIONARII** → Sono diffusi soprattutto nell'apparato burocratico romano, abbiamo documenti che testimoniano la loro presenza dal I-II al VII-VIII secolo d.C.

- **SPECULATORES** → Inizialmente erano delle semplici vedette (in latino *speculator* = *osservatore*). Divennero poi probabilmente gli *exploratores.*

- **BENEFICIARII** → Molti dubbi sulle loro reali funzioni. Sono impiegati di sicuro per spiare e punire cristiani e malfattori. Sono attestati dal I secolo a.C. al VI d.C.

- **AGENTES IN REBUS** → Furono formati probabilmente tra il 284 e il 319 d.C. Erano spie imperiali e per assumere tale carica dovevano superare una serie requisiti. Il loro compito principale era quello di sorvegliare il *cursus publicus.*

L’ENIGMA DEL SATOR

L'ENIGMA DEL SATOR

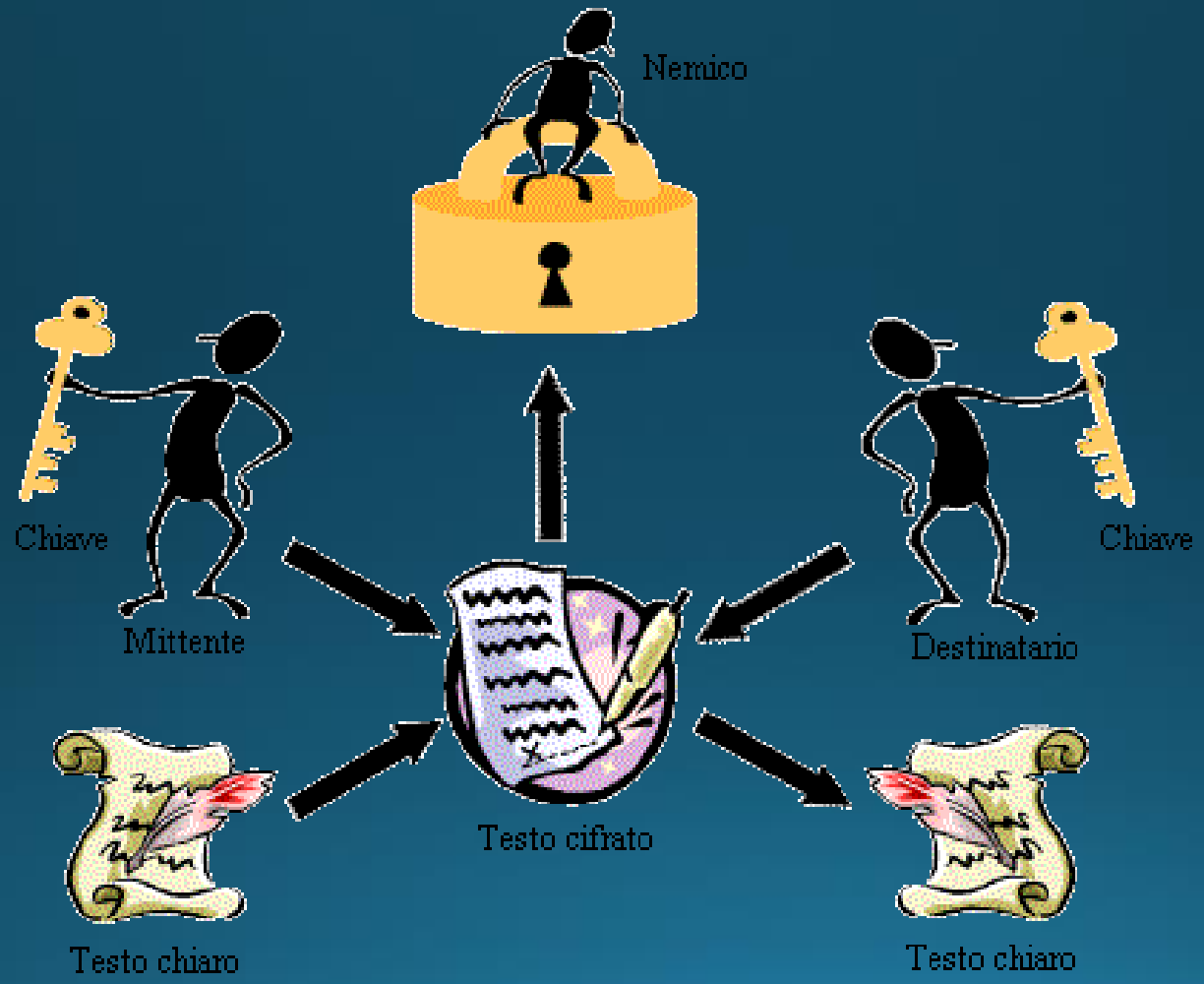
R	O	T	A	S
O	P	E	R	A
T	E	N	E	T
A	R	E	P	O
S	A	T	O	R

S	A	T	O	R
A	R	E	P	O
T	E	N	E	T
O	P	E	R	A
R	O	T	A	S

Gli studiosi Agrell e Grosser, indipendentemente l'uno dall'altro, riuscirono a risolvere il rompicapo individuando un doppio *pater noster* trascritto in forma di croce con ai lati due A e due O che simboleggiano l'alfa e l'omega.

Secondo il giornalista Messori, il Quadrato rappresenta una *summa* di elementi evangelici

GRAZIE PER L'ATTENZIONE



PER APPROFONDIRE…

Crittografia e crittoanalisi. Dietro le righe della storia tra sviluppi tecnico-scientifici e conflitti

Aracne Editrice

CONTATTI

Sito internet: www.marcomoraglio.com

Mail: info@marcomoraglio.com

Instagram: MarcoMoraglio

Facebook: MarcoMoraglioGuida