RATIO MATH. 1.
(1990), 15 - 37

Il Problema della Protezione dell'Informazione, I: Cenni Storici e Metodi Statistici per la Decrittazione di Sistemi di Cifratura Classici

Emilio Ambrisi (*) e Franco Eugeni (**)

(*) Mathesis - via Vicenza 23 - Roma

(**) Dipartimento di Scienze e Storia dell'Architettura - Università di Pescara

1.- INTRODUZIONE: UN PO' DI STORIA

Una visione storica del problema è sempre di grande utilità per la comprensione dello stesso. In questa introduzione intendo dare una breve, spero efficace, panoramica sulla Crittologia.

La Crittologia può essere divisa in tre grandi branche:

- la **crittografia** o arte delle scritture segrete. In questo ambito il problema è nascondere un messaggio con dei procedimenti noti solo al mittente e al destinatario al fine di impedire che un personaggio estraneo alla comunicazione possa, senza esserne autorizzato, comprendere il messaggio.

I procedimenti per "cifrare" e "decifrare" i messaggi sono il segreto del codice.

- **l'autenticazione** è un ulteriore procedimento mediante il quale il ricevente ha una garanzia che il messaggio sia esattamente quello spedito proprio dal mittente, e che il testo sia autentico. Metodi di autenticazione più sofisticati sono i procedimenti di firma numerica, mediante essi il mittente non può disconoscere di aver inviato quel messaggio; inoltre il destinatario è in

grado di provare ad un terzo l'identità del mittente.

- la **crittoanalisi** è la metodologia di ricerca che mira alla ricostruzione, parziale e/o totale, dei sistemi di cifratura usati senza essere in possesso nè della loro architettura, nè delle norme d'impiego, nè delle chiavi usate. Le condizioni di lavoro precedentemente indicate sono le più difficili che si possono presentare.

L'uso delle scritture segrete è antichissimo. Erodoto (VII, 139) ci narra che un tale Demarato riuscì a informare i Lacedemoni del progetto di Serse di invadere la Grecia facendo pervenire loro un messaggio inciso su di una tavoletta, che era stata ricoperta con cera. Aulo Gellio (*Noct. att.*, XVII, 9) parla di un sistema simile, usato dai Cartaginesi, e descrive la *scytala* lacedemonica, della quale parla anche Plutarco. I caratteri venivano tracciati sopra una stretta striscia di pelle arrotolata attorno ad un bastone. Essi potevano essere letti solo da chi possedeva un bastone dello stesso diametro. Svetonio (*Caes.*, LVI) parla di un alfabeto convenzionale usato da Giulio Cesare, consistente nella sostituzione di ogni lettera con quella che la segue di un certo numero di posti nell'alfabeto normale.

Nel Medioevo non si ebbe una sostanziale evoluzione dei sistemi crittografici. Nel Rinascimento invece la crittografia ebbe notevole impulso; nuovi sistemi di cifratura furono ideati da Leon Battista Alberti, sul cui codice torneremo più avanti, da Giovan Battista Della Porta, celebre fisico napoletano (1540-1615), inventore della camera oscura, autore fra l'altro di un trattato *De furtivis literarum notis* (Napoli 1563), da Gerolamo Cardano, proprio lui: quello dell'equazione di terzo grado, medico e matematico (1501-1576), che, durante la sua sfortunata esistenza, trattò anche di argomenti crittografici in *De subtilitate* (Lione 1554). Fuori d'Italia troviamo il tedesco Tritemio (Johannes da Trittenheim, 1462-1516), autore della *Polygrafia* (Francoforte 1550) e della *Steganographia, hoc est ars per occultam scripturam animi sui voluntatem absentibus aperiendi* (Francoforte 1606-1622). Alcuni metodi di Tritemio sono riportati nel libro recente di Umberto Eco: Il pendolo di Focault. Il francese Blaise de Vigenère (1522-1596) autore di un *Traicté des chiffres ou secrètes manières d'escrire* (Parigi 1586) merita una descrizione a parte.

Il codice di Vigenère fu considerato "sicuro" per più di 200 anni. Fu un ufficiale prussiano ad ideare un test statistico (test di Kasiski) che distrusse il codice.

Nel sec. XVII fu attribuita sempre maggiore importanza alle scritture in cifra e le varie Nazioni adottarono sistemi di cifratura sempre più complessi.

Quindi, come è facilmente intuibile anche per i non addetti ai lavori, la

Crittologia nasce e prolifera come supporto per le comunicazioni militari. Con il passare dei secoli i metodi sono cambiati. I Crittografi naturalmente sono sempre a caccia di nuovi codici che i Crittoanalisti scoprono sistematicamente. E' interessante notare che in questa perenne caccia le invenzioni dalle più rudimentali alle più sofisticate giocano un importante ruolo.

A parte il cifrario di Giulio Cesare ricordato prima, va ricordato l'antico sistema persiano di trasmettere segnali accendendo fuochi su località elevate; simili sistemi di comunicazione furono usati dai greci, cartaginesi e romani, e addirittura fino ai tempi della guerra anglo-boera.

Si è ideato di tutto, alcuni scrivevano messaggi sulle foglie che servivano a bendare le piaghe purulente dello schiavo-corriere; durante le guerre persiane un messaggio fu impresso a fuoco sul cranio nudo di uno schiavo, al quale vennero poi fatti ricrescere i capelli.

Scipione l'Africano concepì un sistema di comunicazione recentemente molto usato dall'Unione Sovietica: inviare in altri paesi spie esperte travestite da domestici degli ambasciatori.

Nel sesto secolo, la rete informativa dell'Impero bizantino era divenuta uno dei fondamenti dello stato: agenti mercanti erano sparsi in tutto il paese con un sistema di import-export.

L'invenzione di alcuni dei più importanti sistemi di comunicazione viene fatta risalire ad Alessandro il Grande. Ad una certa distanza dal suo quartier generale, il Macedone aveva infatti costituito un vero e proprio ufficio di raccolta dati, basato sulle informazioni ottenute da agenti inviati nei paesi nemici. Costoro avevano anche il compito di spargere notizie false sulle intenzioni e le mosse di Alessandro, in modo da disorientare il nemico o indurlo a svelarsi. Insomma, un sistema simile a quello impiegato durante la 2^a guerra mondiale dall'ammiraglio americano Nimitz contro i giapponesi subito *prima della battaglia di Midway*.

Durante il Rinascimento, una rete fittissima di agenti copriva l'Europa: fra i più attivi erano quelli del Papato. Ma neanche il Papa poteva star tranquillo: il segretario di Adriano VI si dice fosse una spia dell'Imperatore Carlo V, al corrente di tutti i segreti del Papa e della sua corte.

Con la Riforma nasce così la "spia ideologica". Uomini e donne di ogni ceto sociale divennero traditori della loro patria per servire gli interessi di una delle due fazioni cristiane in lotta. Il miglior servizio di spionaggio dell'epoca era probabilmente quello spagnolo: l'agente principale di Filippo II era nientemeno che l'ambasciatore inglese a Parigi, Sir Edward Stafford, il quale fra l'altro riuscì a fornire agli spagnoli notizie sulla flotta di Sir Francis Drake, pronta a salpare contro l'Invincibile Armata. A questo punto però si inserì nel gioco Sir Francis Walshingham, che, raccolte le prove del tradimento di

Stafford, decise di sfruttarlo a suo vantaggio, così tramite Stafford si ottennero molteplici informazioni, ad esempio l'elenco preciso di tutte le spie spagnole in Inghilterra.

Padre Giuseppe, religioso al servizio del Cardinale Richelieu, fu famoso per la sua scuola di informatori. Essi trovarono pane per i loro denti solo con il servizio segreto inglese, guidato allora da Thurloe, abilissimo collaboratore di Cromwell.

Verso la fine del XVIII secolo il primato dell'organizzazione spionistica passa dall'Inghilterra alla Francia: Napoleone domina l'Europa, non solo con la potenza degli eserciti e con il genio strategico, ma anche con l'efficienza della sua rete di informatori. Tra questi il più grande di tutti, Karl Schulmeister.

Presentato da Savary a Napoleone con le parole "Ecco, Sire, un uomo tutto cervello e senza cuore, ai Vostri ordini", Schulmeister si accinse a quella che resta forse la più incredibile azione di spionaggio della storia: diventare capo del servizio di informazioni militari della coalizione avversa a Napoleone. Schulmeister si trasferì a Vienna ed offrì informazioni strategiche di grande importanza e *assolutamente vere.*

In meno di un anno, Schulmeister riuscì a farsi nominare capo del servizio di informazioni austriaco: da quel momento fu come se Napoleone stesso potesse esaminare i piani strategici del nemico.

Le vittorie di Ulm e di Austerlitz furono in gran parte dovute a Schulmeister, che non solo informava Napoleone delle mosse nemiche, ma forniva agli Alleati false indicazioni.

Nel 1900 la tecnica fa spietati passi avanti e i mezzi di comunicazione subiscono una vera e propria rivoluzione: la fotografia, il telegrafo, la radio, il telefono, l'aereo. Nascono i servizi militari organizzati. A volte forse anche più di uno per nazione. In Italia durante la 2^a guerra vi erano ad esempio i seguenti

Servizio Informazioni Militari (SIM) dell'Esercito

Servizio Informazioni Militari (SIS) della Marina

Servizio Informazioni Aeronautica (SIA) dell'Aeronautica

Centro di Controspionaggio Militare e Servizi Speciali (CCMSS) alle dipendenze del Ministro della Guerra

Organizzazione di Vigilanza e Repressione Antifascista (OVRA)

Chiusa l'era delle spie romantiche e degli avventurieri di genio, i nuovi personaggi saranno soprattutto colonnelli inglesi a riposo con l'hobby della decifrazione; giornalisti mondani affiliati da anni da qualche servizio segreto; taciturni camerieri turchi e scienziati atomici convinti che una potenza diversa dalla loro patria avrebbe fatto un uso più giusto dei terribili segreti di cui erano

effettivi di truppe, dati bellici o altre informazioni. Ecco un esempio di codice molto elementare.

Cliente = Alleato	Acquistare = Attaccare
Merce = Esercito nemico	Ditta = Divisione in soccorso
Interpellare = Comunicare a ...	Inviare = Far saltare

Per messaggi di questo tipo era necessario avere fantasia e tempo a disposizione. A causa della loro ingenuità essi apparivano subito come cifrati. Non erano così adatti per trasmettere informazioni di una certa importanza. E' bene che i messaggi cifrati sembrino veri. Messaggi convenzionali venivano alle volte inviati anche per mezzo di inserzioni nei giornali:

"Vendesi terreni per 10 ettari, 2 fabbricati, 823 bovini"

può essere benissimo un messaggio in cui 102823 è la chiave da usare per decifrare un successivo o precedente messaggio.

L'abilità consiste nel pensare il testo in modo da non destare il sospetto e da non richiamare l'attenzione dell'avversario.

Il mezzo più usato da quando esiste è stata la radio. Con essa è possibile inviare tempestivamente qualsiasi messaggio al proprio centro, da questo è possibile ricevere in ogni momento ordini e informazioni. Le trasmissioni avvenivano ad ore prestabilite ed iniziavano sempre con la sigla di una delle parti. Il dispaccio veniva trasmesso cifrato, con un sistema la cui chiave era conosciuta quasi sempre da un solo trasmettitore che, una volta raccolte le informazioni, le cifrava per affidarle all'agente incaricato di effettuare la trasmissione. Così questi inviava al centro una serie di numeri o lettere a lui stesso incomprensibili. Nel corso dell'emissione l'operatore inseriva il cosiddetto *parity check* che segnalava eventuali errori dovuti al canale e il *security check*, cioè un errore, una parola sbagliata sempre uguale, in modo che il centro avesse la certezza che l'agente stava trasmettendo liberamente. La radio presentava il grave inconveniente di poter essere individuata dalle stazioni di ascolto e di intercettazione avversari.

Come si è detto, i messaggi, prima di essere trasmessi, venivano tradotti "in cifra" secondo particolari metodi appositamente studiati.

I vari sistemi di cifratura possono a grandi linee raggrupparsi in tre categorie: sistemi *a trasposizione*, sistemi *a sostituzione* e sistemi *misti*. Nei primi la traduzione del linguaggio chiaro in linguaggio segreto ha luogo mediante una specie di anagramma degli elementi dei testi chiari; nei secondi mediante sostituzione degli elementi stessi con cifre crittografiche, cioè con segni convenzionali, o con gruppi di tali segni; nei terzi mediante entrambe le

operazioni, eseguite successivamente l'una dopo l'altra in un certo ordine.

I sistemi a sostituzione consistono nel mettere al posto di ogni lettera (o gruppo di lettere, o parole o frasi del testo) un'altra lettera (o numero, o gruppo di lettere o di numeri). La sostituzione letterale può essere *monoalfabetica* o *polialfabetica* secondo che ha luogo in base a un solo alfabeto cifrante o a più alfabeti cifranti, da adoperare in blocco, ma con una certa legge, di volta in volta, prestabilita.

Ad esempio il seguente messaggio: "**Appuntamento ora X....**" può essere così trasmesso:

BQQVMUBNFOUPPSPZ...

L'alfabeto usato in questo caso è un alfabeto slittato di un posto, nel quale la B ha preso il posto della A, la C della B, la D della C e così via.

Naturalmente l'alfabeto cifrante si può ottenere spostando di due, tre, quattro, anche ventisei posti l'alfabeto vero.

Un altro messaggio: "**giorno X ora Y In arrivo navi ed aerei alleati ...**" cifrato per trasposizione senza chiave diviene:

GIIE INEA OADT RRAI NREA OIRB XVEC OOID RNAE AALF YVLG

Esso si ottiene scrivendo su di un rettangolo il messaggio da inviare nel modo seguente:

GIORNOXORAY

INARRIVONAV

IEDAEREIALL

EATIABCDEFG

La cifratura può aver luogo per *lettere*, per *sillabe*, o per *gruppi* di un numero fisso di lettere (*poligrammi*), o per *frasi*, o in modo promiscuo. La maggior parte degli autori ripartisce i sistemi di cifratura nelle due categorie di sistemi letterali o di sistemi a repertorio. I primi consistono nella trasposizione e/o sostituzione delle lettere o di poligrammi. I secondi consistono invece nella sostituzione delle parole e delle frasi. Questa operazione può essere seguita da una seconda cifratura, o **sopracifratura**, per trasposizione e/o per sostituzione delle relative cifre crittografiche. I segni convenzionali che rappresentano gli elementi del linguaggio chiaro possono essere di qualsiasi genere, ma nei tempi moderni è frequente l'uso di segni adoperati nella corrispondenza telegrafica. Sono usati i segni della normale scrittura, e per lo

più si usano o sole cifre arabe o sole lettere e si formano gruppi di un numero fisso di elementi.

Molto comuni sono i sistemi a gruppi di cinque lettere o di cinque cifre arabe, ovvero di dieci lettere costituenti un insieme pronunciabile, tali essendo i massimi tassabili per una parola nelle comunicazioni telegrafiche internazionali.

La convenzione in base alla quale si eseguono le operazioni di sostituzione e di trasposizione è sovente rappresentata da una *chiave*, cioè da una serie di numeri o di lettere, il cui uso può spiegarsi mediante esempi.

ESEMPIO

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

e salta

saltano

La parola "ginepro" formata da lettere tutte distinte è la chiave. Il metodo di cifratura è ovvio. Da notare che per il fatto che da s → a z ci sono troppe lettere fisse potrebbe essere conveniente cambiare la parola chiave.

La cifratura può anche essere eseguita mediante l'uso di griglie, cioè di poligoni di cartone o di altra materia ripartiti in caselle, delle quali un certo numero forate. Il tipo originario è la griglia quadrata, ideata dal Cardano, con la quale la cifratura ha luogo sovrapponendo quadrati di cartone forati in un certo modo convenuto. Il messaggio viene scritto nei fori della griglia appoggiata su di un foglio di carta quadrettata, ruotando il cartoncino in un modo stabilito quando tutte le fessure sono state riempite. Dopo aver tolto la griglia, si rilevano le lettere o colonna per colonna, sia in senso verticale che in senso orizzontale, oppure mediante l'aiuto di una "chiave" come nei casi precedenti.

1° quadrato					
	1				
2					
	3		5		
		4		6	
					7
				8	

2° q. ruotato di 90° ant.					
				7	
			6		8
		5			
			4		
1		3			
	2				

più si usano o sole cifre arabe o sole lettere e si formano gruppi di un numero fisso di elementi.

Molto comuni sono i sistemi a gruppi di cinque lettere o di cinque cifre arabe, ovvero di dieci lettere costituenti un insieme pronunciabile, tali essendo i massimi tassabili per una parola nelle comunicazioni telegrafiche internazionali.

La convenzione in base alla quale si eseguono le operazioni di sostituzione e di trasposizione è sovente rappresentata da una *chiave*, cioè da una serie di numeri o di lettere, il cui uso può spiegarsi mediante esempi.

ESEMPIO

Alfabeto chiaro	A	B	C	D	E	F	G	H	I	L	M		
Alfabeto cifrato	g	i	n	e	p	r	o	a	b	c	d		

e salta

	N	O	P	Q	R	S	T	U	V	W	Z		
	f	h	l	m	q	s	t	u	v	w	z		
	g	i	n	o	p	r							

saltano

La parola "ginepro" formata da lettere tutte distinte è la chiave. Il metodo di cifratura è ovvio. Da notare che per il fatto che da s → a z ci sono troppe lettere fisse potrebbe essere conveniente cambiare la parola chiave.

La cifratura può anche essere eseguita mediante l'uso di griglie, cioè di poligoni di cartone o di altra materia ripartiti in caselle, delle quali un certo numero forate. Il tipo originario è la griglia quadrata, ideata dal Cardano, con la quale la cifratura ha luogo sovrapponendo quadrati di cartone forati in un certo modo convenuto. Il messaggio viene scritto nei fori della griglia appoggiata su di un foglio di carta quadrettata, ruotando il cartoncino in un modo stabilito quando tutte le fessure sono state riempite. Dopo aver tolto la griglia, si rilevano le lettere o colonna per colonna, sia in senso verticale che in senso orizzontale, oppure mediante l'aiuto di una "chiave" come nei casi precedenti.

1^o quadrato					
	1				
2					
	3		5		
		4		6	
					7
				8	

2^o q. ruotato di 90^o ant.					
				7	
			6		8
		5			
			4		
1		3			
	2				

testo chiaro LA CRITTOGRAFIA E' INTERESSANTE

	L									E			N				
A									A		I	T					
	C		I					I					E		E		
		R		T					F					R		S	
					T	G		A									S
				O			R									A	

Gli spazi vuoti vengono riempiti ad esempio con lettere casuali.

Per eliminare in parte le ripetizioni che compaiono necessariamente in ogni crittogramma, specialmente nei testi molto lunghi, si ricorre alla sopracifratura, operazione che consiste nel cifrare di nuovo il testo ottenuto con la prima cifratura, magari cifrando parzialmente il testo o usando un cifrario tipo quello dell'Alberti, nel quale cambiare alfabeto è facile.

Naturalmente il destinatario per poter decifrare un crittogramma doveva compiere operazioni inverse a quelle eseguite dal mittente.

Da un punto di vista storico, possiamo dire che nel Medio Evo, per le condizioni politiche, i codici segreti vengono usati poco ed in genere solo per nascondere nomi di personaggi importanti.

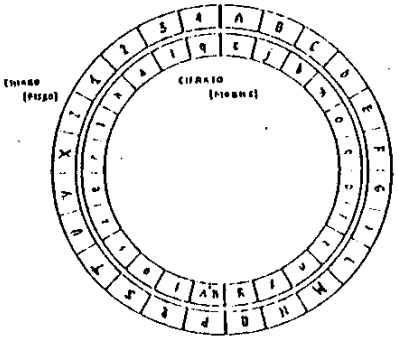
Verso la fine del Medio Evo, con l'inizio delle relazioni diplomatiche tra i vari stati, i codici segreti diventano una necessità.

Secondo ricerche storiche dovute a Meister (1902) l'uso sistematico dei codici segreti ebbe inizio nella Corte Papale, nelle Repubbliche e Signorie Italiane, a partire dal 1300 .

E' in questo periodo che la Crittografia ha una grossa evoluzione. Troviamo un cambiamento radicale, infatti nascono i primi codici segreti che non usano un solo alfabeto cifrante, ma molti alfabeti cifranti. Tali codici si chiamano codici polialfabetici.

Il primo codice polialfabetico è dovuto ad un illustre pensatore italiano: Leon Battista Alberti - architetto, urbanista, pedagogo, matematico e crittografo. E' suo, su commissione del segretario pontificio, Leonardo Dato, il primo codice polialfabetico della storia, messo a punto intorno al 1466.

Esso era costituito mediante due cerchi concentrici. Nel disco più esterno appare l'alfabeto in chiaro formato da 24 caselle, 20 delle quali contenenti lettere (mancano per ragioni di sicurezza crittografica, le lettere che si presentano con minore frequenza, cioè J, K, Y, W, Q, H) e le rimanenti quattro i numeri 1, 2, 3, 4.



Il disco interno contiene una permutazione di altre 24 lettere (manca la lettera w ed è u = v) formanti l'alfabeto cifrante. Esso può ruotare rispetto al primo disco.

Si fissa, prima di cominciare a criptare il messaggio, una lettera dell'alfabeto in chiaro detta indice del codice. Poiché c'è una corrispondenza biunivoca tra le caselle dei due dischi, allora alla lettera scelta come indice del codice, sia ad esempio F, corrisponde una ed una sola lettera del disco interno. Come prima lettera del testo cifrato si scrive la lettera corrispondente ad F e poi ogni lettera del messaggio viene sostituita con la corrispondente sempre del disco più interno. Supponiamo ora che dopo un certo numero di lettere (anche uno solo) si desideri cambiare alfabeto per rendere più difficile una possibile decrittazione. Si scelga allora uno dei numeri 1, 2, 3, 4 che sono a disposizione, ad esempio il numero 2, che va pensato come inserito nel testo in chiaro. A questo numero si sostituisce la lettera che gli corrisponde nella corrispondenza data dai due dischi. Fatto ciò, si ruota il disco finché la lettera corrispondente al numero scelto non si vada a situare esattamente sotto l'indice del codice, la lettera F nel nostro caso. Questa operazione cambia la biezione tra l'alfabeto in chiaro e quello cifrante quindi otteniamo un altro alfabeto, fino a che non decidiamo di fissare un nuovo numero e così via.

La tendenza del periodo è quella di costruire algoritmi per cifrare semplici. Troviamo altri codici polialfabetici (ricordiamo, ad esempio, quelli di G.Cardano e di Bellaso) e nasce l'uso della parola chiave principalmente per merito di un altro italiano, Giovan Battista Della Porta (1563), l'inventore della camera oscura. Con riferimento alla tavola Della Porta (pag. seguente) vediamo l'uso della parola chiave in quel codice .

Si comincia con il fissare una parola del tutto arbitraria ma contenente lettere tutte distinte (ciò perché ad ogni parola corrisponderà un diverso alfabeto); sia AMBRISEMLO (abbiamo tolto tre I). Si scrive tale parola sotto il messaggio un numero di volte tale da "coprire" il messaggio stesso, indi si usano le tavole come nel seguente esempio.

ESEMPIO.

Cosa ne facciamo della parola chiave? Ogni lettera di essa, *ad esempio* a, ci dice *quale alfabeto dobbiamo usare* per criptare la lettera del messaggio corrispondente. Nel caso generale quindi si deve dare una permutazione dell'alfabeto per ogni lettera della parola chiave. La costruzione di queste permutazioni costituisce il codice stesso. Come esempio vediamo il sistema Porta

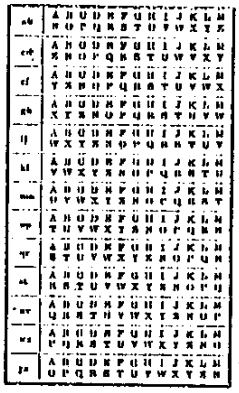


Tavola Della Porta

Nelle tavole di Della Porta le lettere minuscole scritte in testa danno il nome all'alfabeto di quella riga, che è ottenuto dividendo l'alfabeto in due parti di 13 lettere ognuna e stabilendo una biezione tra i due insiemi di 13 elementi. Allora se la lettera della parola chiave che stiamo considerando è una a oppure una b, *si cripta la lettera del testo corrispondente con l'alfabeto di nome* ab, e così via. Vediamo un esempio:

testo in chiaro: FRANCO EUGENI SPEDISCE UN TESTO SEGRETO

parola chiave : ambris emloam brisemlo am brise mloambr

testo cifrato : skniyk paoxap fknutlxx hg gwjcd lzzeygj

Per essere in grado di compilare i messaggi secondo i sistemi esposti, gli operatori devono conoscere sia le chiavi sia i sistemi di cifratura. Alle volte invece si sono usati codici cifranti, cioè fascicoli contenenti liste di cifre o di lettere da sostituire alle rispettive voci. Queste liste possono essere costituite da parole, frasi, o periodi, più frequentemente usati nei messaggi, con a fianco un gruppo cifrante, numerico o letterale, che può trasmettersi via telegrafo.

I sistemi monoalfabetici sono i più antichi; l'alfabeto cifrante è stabilito in un qualsiasi modo convenzionale e si può fare uso anche di *segni nulli*, nonché di *omofoni*, cioè di più segni rappresentanti la stessa lettera dell'alfabeto

normale, usabili indifferentemente.

I sistemi polialfabetici derivano tutti dalle tabelle ideate dall'Alberti, da Porta e da Tritemio.

Tritemio, citato ampiamente da Umberto Eco nel pendolo di Focault, usava rivestire i suoi molteplici codici, molti basati su peculiarità del latino, di misticismo. L'idea base fu quella di aggiungere molte parole in modo che il messaggio finale avesse senso compiuto. In Tritemio appare anche il **quadrato latino** 26x26 usato come tavola per cifrare e decifrare. Questo quadrato può essere visto come la tavola di addizione di Z_{26} qualora che sia

A = 0, B = 1, ..., Z = 25.

Un codice polialfabetico, che ha raggiunto maggiore notorietà, è quello dovuto al francese Blaise de Vigenère.

Egli nel 1586 pubblica il suo codice nel quale fa uso di una tavola quadrata, già introdotta dall'abate Tritemio e nota come tavola di Vigenère, sulla quale vi è veramente molto da dire. Il quadrato è passato alla storia come quadrato o *chiffre carré* del Vigenère. Esso è stato molto in voga, sino a epoca relativamente recente, per scopi militari e diplomatici.

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

Ogni riga della tavola è un alfabeto di Cesare, a cui diamo il nome della lettera posta a sinistra. Per criptare un messaggio si usano tanti alfabeti di Cesare quante sono le lettere della parola chiave.

ESEMPIO

Testo chiaro : IO SONO NATO A TERAMO

CHIAVE : te ramo tera m oteram

TESTO CIFRATO: bs jozc geko m hxvrma

La tavola è un quadrato latino cioè una matrice in ogni riga e colonna della quale vi è una permutazione della prima riga o colonna. Si tratta anche della tabella additiva delle classi resto modulo 26, quindi un esempio di gruppo finito. Il segreto di questo codice è tutto nella parola chiave. Quindi, il destinatario del messaggio (e si spera solo lui, oltre il mittente) conosce la parola chiave. Allora è in grado di decifrare il messaggio in arrivo usando il procedimento al contrario (ovvero la sottrazione modulo 26).

Per l'uso della suddetta tabella si adotta generalmente una chiave letterale consistente per lo più in una parola o in una frase, e la cifratura ha luogo sostituendo ogni lettera del testo chiaro con quella della colonna verticale, nel punto d'intersecazione delle colonne comincianti rispettivamente con la lettera da cifrare e con la corrispondente lettera della chiave, o viceversa.

Possono pure compilarsi tabelle per cifratura polialfabetica aventi per alfabeto base un alfabeto intervertito, che sia cioè una permutazione dell'alfabeto ordinario.

Sono stati ideati anche sistemi a rappresentazione numerica, nei quali gli alfabeti cifrati sono costituiti da numeri, ma essi non differiscono in maniera sostanziale, agli effetti del segreto crittografico, da quelli letterali.

I sistemi polialfabetici possono essere *a chiave fissa,* a chiave variabile, *a interruzione della chiave e autocifranti.* Nei sistemi a chiave variabile e in quelli a interruzione della chiave occorre stabilire per convenzione il modo in cui si deve segnalare al destinatario del messaggio il cambio o l'interruzione nell'uso della chiave. Nei sistemi autocifranti si adopera la chiave per le prime lettere del testo e si usa poi, come chiave, o lo stesso testo chiaro o il testo segreto ottenuto.

Può ricorrersi per la sostituzione polialfabetica all'uso di **macchine cifranti,** ciò che consente di eseguire rapidamente le operazioni di cifratura,

pure adoperando chiavi diverse e di notevole lunghezza. La cifratura per sostituzione può anche aver luogo per poligrammi, cioè per gruppi di un numero fisso di lettere, e per frazioni di lettere, cioè sostituendo le singole lettere del testo chiaro con gruppi di lettere o di cifre o di altri segni convenzionali, che si sottopongono poi a seconda cifratura. Potrebbe pure aver luogo per sillabe, ma i sistemi di questo tipo sono rarissimi e invero poco pratici. Le macchine cifranti moderne sono naturalmente i computer, ove tutto è veloce e dove la grande mole di lavoro non conta.

I sistemi *a repertorio*, che si ritengono ideati nel sec. XVII, sono di larghissimo uso nei tempi moderni, in quanto consentono maggior garanzia di sicurezza in confronto dei sistemi letterali e producono, d'altra parte, una notevole economia di spese telegrafiche. I repertorî, altrimenti chiamati codici, vocabolarî telegrafici, dizionarî cifrati, ecc., sono libri o anche programmi di computer contenenti un certo numero di voci, a ciascuna delle quali corrisponde un gruppo cifrante, composto generalmente di quattro o cinque lettere dell'alfabeto o cifre arabe.

3.- IL PROBLEMA DEI CRITTOANALISTI: INTERVENGONO GLI STATISTICI

Una simpatica storiella crittografica mostra come a volte non è bene fidarsi di piccole statistiche per dedurre.

Un intruso vuole carpire la parola d'ordine di un accampamento militare. Si nasconde dietro un cespuglio in prossimità dell'accesso e ascolta.

la sentinella domanda: dodici?
il 1° soldato risponde: sei! e passa;

la sentinella domanda: dieci?
il 2° soldato risponde: cinque! e passa;

la sentinella domanda: otto?
il 3° soldato risponde: quattro! e passa;

la sentinella domanda: sei?
il 4° soldato risponde: tre! e passa;

la sentinella domanda: quattro?

l'intruso risponde: due! e viene fulminato da un colpo di fucile perché per passare bisognava dire il numero delle lettere componenti il numero della domanda, quindi sette e non due!

La decrittazione dei crittogrammi è la traduzione di essi in linguaggio chiaro, eseguita da chi non sia a conoscenza dei cifrari e delle chiavi costituenti la base del segreto.

I metodi usati per decrittare i messaggi si basano su considerazioni statistiche, in particolare sulle caratteristiche di ciascuna lingua, cioè sul fatto che in ogni lingua le singole lettere, alcuni bigrammi e trigrammi e certe parole si ripetono più frequentemente di altre. Si chiama logoscopico il calcolo statistico delle parole, frasi e periodi che più frequentemente si riscontrano nel linguaggio. Il lavoro di decrittazione consiste in successive induzioni e deduzioni in merito al presumibile significato dei testi presi in esame e può essere agevolato da alcune circostanze favorevoli, quali il possesso di più testi cifrati relativi allo stesso testo chiaro, ma ottenuti con cifrari diversi, la conoscenza anche vaga del sistema di cifratura adottato, la conoscenza parziale o totale del testo chiaro corrispondente a qualche testo cifrato del quale si sia in possesso. Quindi cifrando un testo chiaro, se ad ogni lettera, o gruppo di lettere o parole si sostituisce un determinato segno, questo si ripeterà con la stessa frequenza del testo chiaro: cosicché alla lettera o alla cifra più frequentemente ripetuta nel testo cifrato, con ogni probabilità corrisponderà la lettera o la parola più frequente nel linguaggio chiaro.

Le basi linguistiche della decrittazione consistono nelle caratteristiche particolari di ciascuna lingua e cioè nelle sequenze percentuali delle lettere, dei bigrammi e trigrammi più comuni e di alcune parole, nelle sequenze percentuali delle lettere e di alcune parole tra di loro, nelle sequenze obbligate o molto probabili, in quelle escluse o assai poco probabili, nelle terminazioni più frequenti delle parole, ecc.. I dati caratteristici delle principali lingue sono contenuti in varie opere di crittografia.

Ad esempio nella lingua italiana il 45% delle lettere sono vocali e le sequenze con le quali si ripetono le varie lettere sono le seguenti:

A = 10,41 %	B = 0,95 %	C = 4,28 %
D = 3,82 %	E = 12,63 %	F = 0,75 %
G = 2,01 %	H = 1,10 %	I = 11,62 %
L = 6,61 %	M = 2,58 %	N = 6,49 %
O = 8,71 %	P = 3,26 %	Q = 0,57 %
R = 6,70 %	S = 6,04 %	T = 6,06 %
U = 3,04 %	V = 1,51 %	Z = 0,93 %

Nel seguente messaggio cifrato:

VSNHQ HPNFM HVHLA RQRQR VZUND LHQZN

si contano 5 H, 4 N, 4 Q, 3 R e 3 V alcune delle quali con ogni probabilità saranno vocali. Perciò quasi sicuramente la H corrisponderà alla "e".

Appare evidente che con ogni probabilità la prima parola, dato l'argomento di cui si tratta, sarà "spie" e quindi V = S e S = P. Perciò il crittogramma è stato ottenuto con un alfabeto spostato di tre posti. Una accurata verifica ci darà il seguente testo chiaro: **"Spie nemiche seguono nostri agenti".**

Bisogna però precisare che questi non sono che i metodi più semplici di decrittazione.

Ove non si conosca o presuma a quale sistema crittografico appartiene il metodo di cifratura, si deve anzitutto eseguire questa indagine, la quale spesso non presenta grandi difficoltà, avendo i varî sistemi tipici particolari caratteristiche. Non è raro tuttavia, e ciò avviene generalmente per i sistemi misti, che nel testo non si rilevino sufficienti indizî per la determinazione del sistema di cifratura; in questi casi il lavoro di crittoanalisi è, naturalmente, più difficile e può anche non portare, in mancanza di circostanze favorevoli, a un pratico risultato.

La decrittazione dei sistemi letterali a trasposizione si tenta mediante successive disposizioni e spostamenti delle lettere del testo cifrato, sino a quando non si riscontra qualche combinazione di lettere, parte di parola o parola, che valga a mettere sulla buona via.

Per i sistemi letterali a sostituzione monoalfabetica la decrittazione consiste nella ricostruzione dell'alfabeto cifrante.

Sia dato ad esempio il seguente crittogramma, che si presume riferirsi a un testo chiaro scritto in lingua italiana:

KSAJOHTQSVTKHXHJKTQPZJHQMTZFJATXS
ZQTJNNZTXJDTKHSXHFTPHMHEYSNZTDTE
TKKTETQEHKHJOHTQSILAASZHDTETQMSZS
QOJNJQJFSZHEJQJ

Il calcolo delle frequenze letterali dà il seguente risultato: 17 t; 13 h; 12 j; 10 q; 10 s; 8 z; 7 k; 6 e; 4 a; 4 n; 4 x; 3 d; 3 f; 3 m; 3 o; 2 p; 1 i; 1 l; 1 v; 1 y.

Il confronto delle suddette frequenze con quelle medie della lingua italiana (e 12,6%; i 11,6%; a 10,3%; o 8,7% ecc.) fa presumere che quattro delle lettere T, H, J, Q, S rappresentino le 4 vocali a, e, i, o; nel testo si riscontrano i

gruppi lo stesso posto; confrontando le frequenze suddette con quelle medie della lingua è possibile quasi sempre intuire il significato delle lettere più frequenti e formare in tal modo, in successivi tentativi, gruppi di lettere, parti di parole e parole, tenendo conto del presumibile contenuto del messaggio. Se gli alfabeti convenzionali sono disposti normalmente (tabella del Vigenère e simili) la conoscenza del significato di una lettera in un alfabeto ha per conseguenza quella del valore di tutte le altre lettere nello stesso alfabeto. Ciò non si verifica per i sistemi ad alfabeti intervertiti, nei quali però, se l'interversione è regolare, si ha l'equidistanza relativa delle varie lettere in tutti gli alfabeti e, conseguentemente, si deduce dal significato di una lettera in più alfabeti cifranti il valore che hanno in tutti questi alfabeti le lettere di cui si conosca il significato soltanto per uno di essi.

Per i sistemi a rappresentazione numerica, tanto monoalfabetici quanto polialfabetici, i metodi di decrittazione non sono diversi da quelli innanzi indicati per le rispettive categorie di sistemi a rappresentazione letterale.

La decrittazione dei sistemi a repertorio si tenta in base al confronto della frequenza dei gruppi cifranti con quella delle parole di uso più frequente nella lingua e cioè delle cosiddette parole vuote più importanti (articoli, verbi ausiliari, preposizioni, congiunzioni). La posizione di questi gruppi nel testo, il presumibile contenuto del messaggio, ed eventualmente la conoscenza, parziale o totale, di qualche testo chiaro corrispondente a un testo cifrato di cui si disponga, danno modo di intuire il significato di altri gruppi e di procedere nel lavoro di decrittazione.

La decrittazione dei repertorî ordinati e non sopracifrati è in linea di massima possibile, ove si disponga di testi aventi complessivamente una lunghezza opportuna, dato che la conoscenza o presunzione del significato di alcuni gruppi cifranti costituisce una guida di grande importanza. Circostanza particolarmente favorevole è l'esistenza di serie di gruppi che facciano pensare a una parola, generalmente nome proprio, cifrata mediante cifratura delle lettere o delle sillabe. Per esempio, se in un testo ottenuto con un repertorio di 10.000 voci che si ritenga in lingua italiana e in ordine normale, si riscontra una serie di gruppi come la seguente, si deve presumere che essa rappresenti un nome proprio e che i singoli gruppi corrispondano a una vocale o a una consonante secondo queste indicazioni:

3733	3409	7462	7462	0002	7462	4517
conson	vocale	conson.	conson.	vocale	conson.	vocale

Il gruppo 0002 è senza dubbio uguale ad a; i gruppi 3409 e 4517, data la distanza dall'inizio del cifrario e la loro distanza rispettiva equivalgono

presumibilmente ad e ed i; la consonante rappresentata da 3733 è molto probabilmente f. Il gruppo 7462 sarà presumibilmente corrispondente a p, r, s, ma, poiché delle tre ipotesi "Feppapi", "Ferrari", "Fessasi" la seconda è evidentemente la più probabile, può concludersi ritenendo 7462 = r. In tal modo si pongono dei punti di riferimento abbastanza attendibili per la ricostruzione del cifrario ed è agevole proseguire il lavoro di decrittazione, deducendo anzitutto, in base al calcolo delle frequenze, il significato delle parole vuote più importanti.

Per i repertorî paginati e sempre non sopracifrati si procede in maniera analoga, tenendo conto non soltanto delle frequenze dei singoli gruppi cifranti, ma anche di quelle complessive dei gruppi contenuti in ogni pagina.

Molto più difficile è la decrittazione dei repertorî intervertiti e non sopracifrati per la mancanza di qualsiasi ordine nella disposizione dei gruppi cifranti corrispondenti alle voci chiare; il lavoro, generalmente, può avere pratico risultato soltanto ove ricorra qualche circostanza favorevole o soccorra un'intuizione particolarmente felice, e comunque disponendo di un adeguato numero di messaggi cifrati.

Il problema della decrittazione dei sistemi a codice (intervertito o non) sopracifrato è di estrema complessità ed è anche piuttosto lungo descrivere casi particolari per farsi una idea. Comunque va detto che un tale problema è di fatto teoricamente impossibile se non vi sono sovrapposizioni nell'impiego del verme di sopracifratura. Se sovrapposizioni vi sono, si riesce ad eliminare la complicazione dovuta al verme lavorando sulle "differenze" fra i gruppi costituenti la differenza prima dei messaggi. Il "procedimento" usato è piuttosto complesso ed è praticamente impossibile descriverlo in questo lavoro.

Il problema è molto più complicato che nei codici di Cesare o comunque monoalfabetici. Si pensi che il codice di Vigenère è stato usato da vari eserciti resistendo ai vari "attacchi" che i crittoanalisti gli hanno dato per ben tre secoli. Nel 1863 un ufficiale prussiano, Kasiski, forza il codice di Vigenère con un metodo noto come test di Kasiski. Il test di Kasiski è basato sui seguenti punti:

- Il messaggio è sufficientemente lungo.
- Il primo passo è "trovare la lunghezza della parola chiave".
- Il secondo passo è "trovare le lettere della parola chiave".

Circa il primo passo iniziamo con il ricercare nel messaggio cifrato tutte le sequenze (cioè i gruppi) di tre o più lettere consecutive che si ripetono. E' molto probabile che a sequenze uguali del cifrato corrispondano sequenze

uguali del testo in chiaro. In ogni caso è questa una ipotesi di lavoro compatibile con la lunghezza del messaggio. Se così è vuol dire che le prime lettere di sequenze eguali sono state criptate con lo stesso alfabeto della tavola di Vigenère, analogamente le seconde, le terze, ... Da ciò segue che alle prime lettere delle sequenze uguali corrisponde la stessa lettera della parola chiave, analogamente alle seconde lettere e così via. Ma allora la distanza (= numero delle lettere) tra due sequenze uguali è un multiplo della lunghezza della parola chiave.

Quanto è lunga la parola chiave? Molto probabilmente la sua lunghezza è pari al M.C.D. delle distanze tra le sequenze uguali tra loro, che si ripetono.

Chiaramente una distanza "strana" tra due sequenze uguali, nel senso che non ha divisori comuni con le altre distanze, deve essere scartata; questo è il motivo per cui abbiamo detto "molto probabilmente la sua lunghezza ...". Ciò accade quando due sequenze uguali non corrispondono a due sequenze uguali del testo in chiaro.

Trovata la lunghezza d della parola chiave cerchiamo le lettere che la compongono. Notiamo che, nel testo cifrato, alla prima lettera, alla $(d+1)$-ma lettera, alla $(2d+1)$-ma lettera, ... corrisponde la stessa lettera della parola chiave e quindi tutte queste lettere sono state criptate con uno stesso codice di Cesare (cioè con una stessa riga del quadrato di Vigenère). Segue, ripetendo il ragionamento, che la seconda, la $(d+2)$-ma, la $(2d+2)$-ma riga sono anche loro crittografate usando uno stesso codice di Cesare. In definitiva ciascuna delle righe seguenti sono crittografate con una stessa lettera della parola chiave:

{I, $(d+1)$-ma, $(2d+1)$-ma, ...}

{II, $(d+2)$-ma, $(2d+2)$-ma, ...}

{III, $(d+3)$-ma, $(2d+3)$-ma, ...}

.....

.....

{d-ma, 2d-ma, 3d-ma, ...}

Le lettere di ognuno di questi insiemi sono state criptate con lo stesso codice di Cesare. Allora studiamo la frequenza delle lettere in ognuno di essi, con lo stesso metodo usato nei codici di Cesare. Scoperta una lettera, è noto il codice di Cesare usato, e quindi anche il nome dell'alfabeto (cioè la lettera che compare in testa), che ci dà la lettera della parola chiave. Allora il codice di Vigenère è forzato e quindi perde il suo interesse.

Dall'idea di Vigenère si ottiene un codice completamente sicuro, precisamente il codice di Vernam (1926). Questo è un codice del tipo di Vigenère nel quale si usa una parola chiave avente una lunghezza pari alla lunghezza del messaggio. Sembra che il telefono rosso, che fino a qualche anno fa esisteva tra la Casa Bianca e il Cremlino, facesse uso di un codice di Vernam per comunicare.

Per i sistemi crittografici, ben rari invero nei tempi moderni, in cui gli elementi del testo chiaro siano rappresentati con segni convenzionali diversi dalle lettere dell'alfabeto e dalle cifre arabe, la decrittazione si tenta in modi analoghi a quelli indicati per i sistemi a rappresentazione letterale o numerica, nei quali possono tramutarsi i sistemi suddetti, sostituendo con gruppi di lettere o di cifre i segni convenzionali speciali.

SOMMARIO.- Dalla crittografia, arte di costruire codici segreti, l'uomo ha costruito la crittoanalisi che è l'arte di scoprire il segreto dei codici. Nella crittoanalisi, intervengono metodi di tipo statistico e principalmente un modo di pensare logico-statistico. Molte di queste idee sono traducibili didatticamente, anche a livello Scuola Media inferiore come appare anche da un recente lavoro di L.Berardi, presentato al convegno dei nuclei didattici del C.N.R., tenutosi a L'Aquila nel 1989, nel quale si riferisce in relazione alla compiuta sperimentazione di alcune unità didattiche aventi come oggetto la crittografia.

RINGRAZIAMENTI

Gli Autori desiderano ringraziare vivamente l'Ammiraglio di squadra Giovanni MORO per gli utili consigli ed i colloqui avuti sugli argomenti trattati e per la cura con cui Egli ha riletto il nostro manoscritto, migliorandone la qualità.

BIBLIOGRAFIA

[1] C. Amè, Guerra segreta in Italia, Casini, Roma 1954.

[2] B. Baldessari, Aspetti probabilistici della crittografia, Atti 1o Simposio Nazionale su stato e prospettive della ricerca crittografica in Italia, Roma 30-31 Ottobre 1987.

[3] H. Becker e F.C. Piper, Cipher systems, Northwood Books, London 1982.

[4] L. Berardi, Some remarks about an electronic signature derived from a generalized RSA-code, J. of Information & Opti. Scien., in corso di stampa.

[5] L. Berardi e A. Beutelspacher, I buoni angeli custodi, ovvero i protettori di un messaggio, Archimede 2-3, 1988.

[6] L. Berardi e M. Di Fonso, Protezione delle informazioni su personal computer, Atti cit. in 2 .

[7] L. Berardi e F. Eugeni, Blocking sets e teoria dei giochi: origini e problematiche, (dedicato al Prof. Renato Nardini per il suo 70-mo compleanno), Atti Sem. Mat. Fis. Univ. Modena, 34, 1988.

[8] L. Berardi e F. Eugeni, Strutture geometriche, crittografia e sistemi di sicurezza richiedenti un quorum, Atti cit. in 2 .

[9] L. Berardi e B. Rizzi, Generalizziamo il codice RSA e la funzione di Eulero, Atti cit. in 2 .

[10] A. Beutelspacher, Encyphered Geometry: some applications of Geometry to Cryptography, Annals of Discrete Math., 37, 1988.

[11] A. Beutelspacher, La scuola elementare della teoria dei codici, Quad. n. 1, suppl. did., Sem. Geom. Comb. Univ. de L'Aquila, 1983.

[12] A. Beutelspacher, Kriptologie, Wieweg-Sohn, 1987.

[13] O. Brugia, S. Improta e W. Wolfowicz, Segretezza e autenticazione nelle moderne reti di telecomunicazioni, Rel. Int. 2B 63385, Fondazione Ugo Bordoni, Roma 1985.

[14] O. Brugia, Sistemi crittografici a chiave pubblica, Quad. Scuola Super. "G. Reiss Romoli" n. 4673, 1985.

[15] N. Cera e A. Maturo, Generazione di numeri pseudo-casuali per mezzo di relazioni di ricorrenza sui campi di Galois, Fac. di Arch. Università di Pescara, 1981.

[16] M. Cerasoli, F. Eugeni e M. Protasi, Matematica discreta, Casa Editrice Zanichelli, in corso di stampa.

[17] Conti, Servizio segreto, De Luigi, Roma, 1945.

[18] D. E. Denning, Cryptography and data security, Addison-Wesley, 1983.

[19] W. Diffie e M.E. Hellman, New directions in cryptography, IEEE Trans. on Information Theory, vol. IT-22, n. 6, Nov. 1976.

[20] L. Gioppi, La crittografia diplomatica, militare e commerciale, Milano, 1897.

[21] M. Givierge, Course de cryptographie, Parigi, 1925.

[22] W. Heise e P. Quattrocchi, Informations und Codierung Theorie, Springer Verlag, Berlin-Heidelberg-New York-Tokio, 1983.

[23] M.E. Hellman, La crittografia a chiave pubblica, Le Scienze, 10, 1981.

[24] A. Ind, A history of modern espionage, Hodder & Stoughton, Londra, 1965.

[25] F.W. Kasiski, Die Geheimschriften und die Dechiffrirkunst, Berlino, 1863.

[26] A. Kerckhoffs, La cryptographie militaire, Parigi, 1883.

[27] A. Maturo, Messaggi cifrati per mezzo di numeri pseudo-casuali ottenuti a partire da successioni in algebre di supporto, Atti cit. in 2 .

[28] F. Mazzei, Sicurezza e riservatezza delle informazioni negli enti e nelle imprese, Franco Angeli Editore, Milano 1983.

[29] W.W. Peterson e E.J. Weldon, Error correcting codes, MIT Press, Cambridge, Massachussets, 1980.

[30] R.L. Rivest, A. Shamir e L. Adelman, A method of obtaining digital signatures and public key cryptosystem, Comm. of the ACM, vol. 21, n. 2, Febbraio 1978.

[31] A. Rizzi, On the sum (Modulo m) of two statistical variables, Boll. Union. Mat. Ital., 13, 1976.

[32] A. Rizzi, Generazione di simboli binari pseudo-casuali per mezzo di relazioni ricorrenti su campi di Galois, Statistica, 1982.

[33] A. Rizzi, Aspetti logici dell'analisi dei dati, Dipart. di Stat., Prob. e Stat. Appl. Univ. Roma "La Sapienza", n. 1, 1984.

[34] A. Rizzi, Alcune considerazioni sulle problematiche delle banche di dati, Dipart. di Stat., Prob. e Stat. Appl. Univ. Roma, 5, 1984.

[35] A. Rizzi, Alcune analisi statistiche della lingua italiana, Dipart. di Stat., Prob. e Stat. Appl. Univ. Roma, n. 6, 1984.

[36] A. Rizzi, Alcune considerazioni sulla crittografia, Conferenza di apertura al 1o Simposio Italiano su stato e prospettiva sulla ricerca crittografica in Italia, Atti cit. in 2.

[37] L. Sacco (Gen.), Manuale di crittografia, Litografia Covi, Roma 1947. Ristampa anastatica a cura della Scuola Superiore "G. Reiss Romoli", L'Aquila 1986.

[38] W. Schellenberg, Le memorie, Longanesi, 1960.

[39] R. Seth, Secret servants. The true story of Japanese espionage, Paperback, New York, 1968.

[40] A. Sgarro, Crittografia, Franco Muzzico Ed., Padova 1986.

[41] A. Shamir, How to share a secret, Comm. ACM, vol. 22, 1979.

[42] C.E. Shannon, A mathematical theory of communications, BSTJ 27, 1984.

[43] C.E. Shannon, Communication theory of secret systems, BSTJ 28, 1984.

[44] G. Tallini, Le geometrie di Galois e le loro applicazioni alla statistica e alla teoria della informazione, Rend. di Mat. Roma, 19, 1960.

[45] G. Tallini, Introduzione alla teoria dei Codici, Seminario Univ. L'Aquila, Febbraio 1979.

[46] P. Valerio, De la cryptographie, Parigi, 1893.

[47] G.S. Vernam, Cipher printing telegraph systems for secret wire and radio telegraphig communications, J. AIEE, 45, 1926.

[48] C.F. Vesin de' Romani, La cryptographie dévoilée, Parigi, 1857.

[49] M. Zanotti, Crittografia, Milano, 1928.