Crittografia militare
Parte I

Auguste Kerckhoffs

Giornale di Scienze Militari.

Gennaio 1883.

La crittografia militare.

«La crittografia è un potente ausilio della tattica militare». (Generale Lewal, *Studi di guerra*.)

I. La crittografia nell'esercito

A. Note storiche.

La *Crittografia* o *Arte di cifrare* è una scienza antica come il mondo. Confusa in origine con la telegrafia militare, è stata coltivata fin dai tempi più remoti dai Cinesi, dai Persiani e dai Cartaginesi ed è stata insegnata in Grecia nelle scuole di tattica e tenuta in alta considerazione dai più illustri generali romani[1].
Dopo la modesta scitala dei Lacedemoni ed i trucchi inventati o riferiti da Enea il Tattico[2], fino al famoso tonneau di Kessler[3], i militari hanno escogitato molte tecniche per trasmettere lontano gli ordini segreti o per tenere le loro istruzioni al riparo dalle investigazioni e dalle sorprese del nemico.
Purtroppo, noi non possediamo altro che informazioni molto incomplete riguardo alle tecniche crittografiche utilizzate dagli antichi. Infatti, oltre ai *Commentari* di Enea, non si repertano in merito all'argomento che stiamo trattando altro che accenni sporadici in Polibio[4], Plutarco[5], Dione Cassio[6], Svetonio[7], Aulo-Gellio[8], Isidoro[9] e Giulio l'Africano[10].
Nel Medio-Evo, la crittografia è stata coltivata soltanto dai monaci e dai cabalisti e ancora, nei casi in cui ha avuto un qualche risvolto pratico, gli inventori hanno cercato più di cambiare il senso dei messaggi trasmessi che inventare metodi di corrispondenza più o meno indecifrabili. In quei tempi di ignoranza permalosa, era molto più pericoloso corrispondere ricorrendo ad un linguaggio misterioso o indecifrabile che scrivere *in chiaro* i segreti più compromettenti.
Perfino nel XVII secolo, il semplice fatto di aver avuto una corrispondenza in caratteri segreti era considerato ancora dai tribunali inglesi una circostanza aggravante. Basti ricordare il famoso processo intentato al conte di Somerset, imputato per avvelenamento, in cui il cancelliere Bacone stigmatizzerà come grave indizio a carico del nobile sotto accusa la sua abitudine di scrivere in cifra ai suoi amici.
In verità i nostri padri ricorrevano alla *steganografia*, *artificium sine secreti latentis suspicione scribendi*, piuttosto che alla *crittografia*, nel significato che oggi attribuiamo a questa parola. Si può leggere nelle opere del gesuita Schott[11] ed in un vecchio trattato di crittografia del duca di Brunswick[12], i mille artifici che sono stati inventati successivamente. Ma è con il Rinascimento che la crittografia diventa una vera arte, *ars occulti scribendi*, come si diceva allora ed acquisisce una certa importanza nelle corrispondenze dei principi con i loro ambasciatori e nelle relazioni dei gran signori con i loro fidi.
Si è visto, leggendo le sue lettere indirizzate al landgravio di Hesse, pubblicate qualche anno fa da Rommal, che Enrico IV amava servirsi di una cifra per la sua corrispondenza privata.
Egualmente si sa che Enrico IV, avendo fatto intercettare alcune lettere cifrate indirizzate ad appartenenti alla Lega per il governo spagnolo, incaricasse il matematico Viète di trovarne la chiave. Questi vi riuscì e così il re poté per quasi due anni sorvegliare gli intrighi dei suoi nemici.
Sotto Richelieu, l'*arte di decifrare* le scritture segrete si innalzerà quasi all'altezza delle Scienze di Stato e al dire del maresciallo da campo Beausobre[13] il ministro degli affari esteri aveva perfino un'accademia in cui questa veniva insegnata[14]. Sostenuta dalla prodigalità dei governanti, incoraggiata dall'assenza di onestà politica che caratterizzò i regni successivi, l'arte di decifrare ha conti-

nuato, fino alla rivoluzione di Luglio, ad essere coltivata con successi uguali dalle spie della corona e dagli uomini della *camera nera*.
Tuttavia non ho potuto trovare nessuna traccia precisa dell'impiego della corrispondenza crittografica nell'esercito, durante il XVI secolo, ma si sa con certezza che, a partire dal XVIII secolo, gli ordini ai generali comandanti i fronti o nei paesi nemici non si trasmettevano che per cifra[15].
Nei racconti di guerra del primo Impero spesso sono presenti le comunicazioni crittografiche ed i generali avevano due chiavi: una per la loro corrispondenza reciproca e l'altra per la corrispondenza con lo stato maggiore: la *cifra grande* e la piccola o *cifra banale*. Il barone Fain, segretario di Napoleone I, riferisce che durante la guerra con la Russia questi intrattenesse una corrispondenza cifrata[16]. Si sa anche che, durante la guerra di Spagna, uno spagnolo scoprì il modo per rubare la cifra a Suchet e che se ne servì per agevolare ai suoi compatrioti la riconquista di Mequinenza e di Lerida.
Oggi, la corrispondenza mediante cifre segrete è adottata da tutti gli eserciti europei, ma non è ancora utilizzata in modo sistematico al di fuori degli uffici delle cancellerie.

B. I termini del problema.

I tedeschi hanno adottato il principio che la corrispondenza crittografica debba essere impiegata nel modo più esteso possibile e, infatti, i programmi delle loro scuole militari prescrivono non solo di addestrare gli ufficiali a comporre e a leggere i dispacci segreti ma anche di iniziarli alla conoscenza di tutti i principi teorici dell'arte di decifrare.
E l'articolo 32 del regolamento del 19 gennaio 1874 stabilisce coerentemente che i dispacci militari debbano, per quanto possibile, essere cifrati.
Dunque, in un primo momento, ci si potrebbe meravigliare che, fatte salve alcune eccezioni rare, l'uso della corrispondenza cifrata ancora oggi, nell'esercito francese, sia limitato ai comandanti in capo. Ma un sistema crittografico «*facile* nell'impiego e *sicuro* è una lacuna», dice il generale Lewal, «che è sempre esistita nel nostro esercito[17]». L'ex comandante della Scuola superiore di guerra aggiunge che è vero che esistono molte tecniche adatte a questo scopo e che sarebbe sufficiente adottarne una «all'occorrenza portatile e, nell'uso, alla portata di tutti», ma alcune delusioni sperimentate dallo stato maggiore nella nostra recente campagna di Tunisia, come pure le tecniche insegnate e preconizzate nelle nostre alte scuole militari, non farebbero supporre l'esistenza di un'analogia singolare tra questo sistema *facile* e *sicuro* e la pietra filosofale degli antichi chimici?
Oggi, i nostri generali migliori sono tutti d'accordo nel ritenere che è indispensabile che i diversi comandanti di un'armata abbiano a loro disposizione un sistema di comunicazioni segrete per corrispondere liberamente non solo tra loro e con il comandante in capo, ma anche con i loro ufficiali subordinati. Infatti, il tattico che sto per citare pensa che *sia opportuno dotarsi di una cifra per il tempo di pace e una per quello di guerra, una per i generali, una per i capi di reggimento o di servizio e una per tutti i comandanti di colonna e di postazione*. Questi aggiunge pure ed a ragione che occorrerebbe durante la pace esercitare i nostri ufficiali alla gestione di questa corrispondenza.
«Sono incombenze da prevedere e risolvere prima della guerra», dice lui. «Una volta che le operazioni sono iniziate, è troppo tardi per pensarci. D'altronde, anche in tempo di pace si ha bisogno in qualunque istante di corrispondere in segretezza».
Si legge nelle *Ricerche storiche sull'arte militare* del generale Bardin[18] che l'impiego delle cifre si fosse allargato nel periodo centrale della conflagrazione del 1814 e che quando Napoleone volle riunire al nucleo dell'armata tutte le sue guarnigioni straniere e molte grandi guarnigioni francesi, fu in francese puro e chiaro che Feltre e Berthier inoltrarono i suoi ordini; così, pochi dispacci pervennero a destinazione ed il nemico se ne impossessò della maggior parte. «Può essere - dice Bardin - che la sorte della Francia e l'assetto dell'Europa siano dipese dal mancato ricorso alla crittografia!»
Ma non basta avere una cifra segreta per la corrispondenza, occorre ancora che essa presenti garanzie serie di indecifrabilità. E questo è il lato più debole della maggior parte dei sistemi immaginati fino ai nostri giorni, ma là dove questo difetto capitale è stato eliminato, ci si ritrova in presenza di inconvenienti pratici non meno gravi. Perfino nel ministero della guerra non ci si è rivelati molto fe-

lici finora nella scelta o nella combinazione della cifra. Non è un segreto per nessuno che durante la guerra turco-russa, una domenica fu inviato da un attaché militare che seguiva le operazioni degli eserciti in lotta un dispaccio cifrato che, a causa dell'assenza del capo dell'ufficio incaricato della corrispondenza crittografica, non poté essere decifrato. Il Ministro, che ignorava la chiave del messaggio, ritenne di agire al meglio pregando un ufficiale dello stato maggiore di tentarne la decifrazione anche senza chiave: in capo a qualche ora il crittogramma fu tradotto! Fortunatamente per la segretezza della corrispondenza, l'abile decifratore non era che il figlio del Ministro stesso[19].
Si è potuto vedere negli articoli di necrologio pubblicati nel 1879 sui giornali tedeschi, in occasione della morte del capitano Max Hering, il capo del servizio telegrafico che nel 1870 aveva scoperto il cavo della Senna, quali servizi avesse reso agli assedianti l'assenza di un sistema sicuro di corrispondenza segreta tra l'armata di Parigi ed i generali della provincia.
Io non so cosa si debba pensare delle affermazioni dei giornalisti d'oltre Reno, ma quando vedo dei critici autorevoli dichiarare che la crittografia è «un ausilio potente della tattica militare» penso che il destino di un paese, la sorte di una città o di un'armata, potrebbero di conseguenza dipendere dalla indecifrabilità maggiore o minore di un crittogramma. Allora sono stupefatto nel vedere i nostri saggi ed i nostri professori insegnare e raccomandare per usi bellici dei sistemi di cui un decifratore, per quanto poco provetto, troverebbe certamente la chiave in meno di un'ora.
Non ci si può spiegare altrimenti questo eccesso di fiducia in determinate cifre se non a causa dell'abbandono in cui sono piombati gli studi crittografici in seguito alla soppressione delle camere nere e a motivo della sicurezza delle relazioni postali. È ugualmente permesso credere che le affermazioni poco misurate di certi autori, non meno che l'assenza completa di ogni lavoro serio sull'arte di decifrare le scritture segrete, hanno contribuito grandemente a dare corso alle idee più errate sulla validità dei nostri sistemi di crittografia.
È così che il generale Lewal afferma categoricamente nei suoi *Studi di guerra*[20] che le cifre a base variabile sono illeggibili oppure che se venissero decifrate lo sarebbero *a prezzo di difficoltà inaudite!* Ma lo stesso Voltaire non ha detto, in un articolo consacrato alle scritture segrete - questo all'epoca in cui l'arte di decifrare era al culmine della sua fioritura - che, «quelli che si vantano di decifrare una lettera senza essere addentro alle questioni che questa tratta e senza avere degli appigli preliminari, sono ciarlatani più grandi di quelli che si vantano di capire una lingua che non hanno studiato per nulla?[21]».
Nella prefazione del *Controspione*[22], in cui «il cittadino Dlandol» faceva conoscere nel 1793 le chiavi della cifra di cui si servivano i realisti nelle loro corrispondenze con gli emigrati, viene detto che «questo non era un servizio di poco conto reso alla patria in quelle circostanze, infatti si annientava mediante la pubblicità l'arma più pericolosa dei nemici segreti della Repubblica». Io credo, a mia volta, che per dare risalto ad un tipo di idee diverse, non compio un'azione da cattivo cittadino svelando a tutti uno stato di cose che non sono tanto diverse da quelle finora esposte e di cui i nostri nemici esterni non possano un giorno trarne profitto troppo bene e troppo facilmente.
Nelle pagine che seguono esaminerò prima tutti i desiderata di ogni sistema di crittografia militare, poi spenderò qualche parola sulle diverse cifre, quindi indicherò un nuovo procedimento di decifrazione applicabile ai sistemi più usati di Crittografia a base variabile e concluderò con qualche considerazione sui dizionari cifrati e sui crittografi[23].

II. I desiderata della crittografia militare

Bisogna distinguere bene tra un sistema di scrittura cifrata, immaginato per uno scambio momentaneo di lettere tra persone singole ed un metodo di crittografia destinato a regolare senza limiti di tempo la corrispondenza tra i diversi comandanti di armata. Questi, in effetti, non possono a loro piacimento ed in un dato momento modificare le loro convenzioni come pure non debbono conservare a loro riguardo alcun oggetto o scritto di natura tale da chiarire al nemico il senso dei dispacci segreti che potrebbero cadere nelle sue mani.

Una gran quantità di combinazioni ingegnose possono rispondere alle necessità del primo scopo, ma per il secondo caso occorre un sistema che soddisfi alcune condizioni eccezionali, condizioni che riassumerei nei seguenti sei punti:

1. Il sistema deve essere materialmente, se non matematicamente, indecifrabile;
2. Non deve essere segreto ma potrebbe, addirittura, cadere in mano nemica senza alcun inconveniente;
3. Deve essere possibile comunicare o cambiare la chiave senza il ricorso a note scritte e a completa discrezione dei corrispondenti;
4. Deve essere applicabile alla corrispondenza telegrafica;
5. Deve essere portatile e il suo mantenimento e il suo funzionamento non devono esigere il concorso di molte persone;
6. Infine, è necessario, viste le circostanze che ne richiedono l'applicazione, che il sistema sia di uso semplice, non richieda sforzo mentale, né la conoscenza di una lunga serie di regole operative.

Tutti sono d'accordo sulla ragion d'essere degli ultimi tre desiderata, invece non c'è accordo riguardo ai primi tre.
Infatti alcune persone autorevoli sostengono che l'indecifrabilità assoluta di una cifra non dovrebbe essere considerata una conditio sine qua non per la sua introduzione in servizio presso l'esercito, che le istruzioni cifrate trasmesse in periodo bellico non hanno che un'importanza momentanea e che non richiedono il segreto al di là delle tre o quattro ore successive alla loro emanazione, che ha poca importanza il fatto che il nemico conosca il contenuto di un dispaccio segreto qualche ora dopo la sua intercettazione, che, in una parola, è importante che il sistema abbia una struttura tale da impedire la decifrazione di un suo crittogramma per almeno tre o quattro ore. Aggiungono che la possibilità di cambiare la chiave quando lo si desideri toglie al difetto di non-indecifrabilità tutta la sua importanza.
Questa argomentazione può, a prima vista, sembrare del tutto giusta, ma, in realtà, io la ritengo sbagliata.
In effetti, secondo me, non si può dimenticare che la segretezza delle comunicazioni inviate a distanza mantenga molto spesso la sua importanza oltre il giorno in cui esse sono state trasmesse e senza contare tutte le eventualità che possono presentarsi mi basterà citare il caso in cui un comandante di una città assediata invii informazioni all'armata che deve soccorrerlo. Inoltre, una volta che un crittogramma intercettato è stato decifrato, ogni dispaccio nuovo, scritto con la medesima chiave e che va incontro alla medesima sorte, può essere letto istantaneamente. Accadrà, di conseguenza, che in un tempo più o meno lungo, saranno spediti dispacci in ogni direzione e la loro decifrazione, in qualche modo, sarà già stata realizzata in anticipo: a meno di ammettere che in un corpo d'armata tutte le istruzioni cifrate siano emanate da una sola persona o almeno passino per le mani di un solo uomo, il che riduce la corrispondenza segreta ad un ruolo veramente modesto.
La possibilità di cambiare la chiave quando lo si desideri è certamente una condizione essenziale di ogni sistema crittografico, ma è un vantaggio ingannevole e sulla sua realizzazione concreta non si può fare molto affidamento, specialmente nel corso delle mille peripezie di una campagna militare.
Per quanto attiene alla necessità di segretezza, che, ai miei occhi, costituisce il difetto principale di tutti i nostri sistemi crittografici, vorrei far osservare che essa restringe in qualche modo l'impiego della corrispondenza cifrata esclusivamente ai comandanti in capo. E qui intendo per segretezza, non la chiave propriamente detta, ma tutto ciò che costituisce la parte materiale del sistema: tabelle, dizionari o apparecchiature meccaniche di qualunque tipo che ne consentano la realizzazione. In effetti, non è necessario crearsi dei fantasmi immaginari e sospettare della condotta degli impiegati o degli agenti subalterni, per comprendere che, se un sistema che esige la segretezza sarà conosciuto da un numero molto elevato di persone, questo potrebbe essere compromesso ad ogni incarico conferito ad uno qualsiasi di essi. Secondo questa prospettiva non ci sono i presupposti per condannare l'impiego del dizionario cifrato, che oggi è in uso presso l'esercito.

Forse mi si obietterà che ammettendo il secondo desideratum è quasi impossibile realizzare un sistema completamente indecifrabile. Occorre intendersi: so molto bene che richiedere a queste condizioni che un sistema sia matematicamente indecifrabile è matematicamente impossibile, tuttavia affermo, non senza buone ragioni, che, realizzando completamente tutti i desiderata che ho elencato sopra, si possono combinare perfettamente dei sistemi che, se non matematicamente, almeno praticamente sono indecifrabili.
Sembrerebbe che al ministero della guerra si tratti una questione molto seria: la sostituzione del dizionario cifrato con qualche altro sistema più pratico. Ebbene! Se l'Amministrazione vuole mettere a profitto tutti i servizi che un sistema crittografico di corrispondenza ben combinato può rendere, allora deve rinunciare assolutamente ai metodi segreti e stabilire una volta per tutte che non accetterà un procedimento se non può essere insegnato alla luce del sole nelle nostre scuole militari, se i nostri allievi non saranno liberi di comunicarlo a chi piace loro e se perfino i nostri vicini non potranno adottarlo e copiarlo – se questo conviene loro lo dirò poi. Quando i nostri ufficiali avranno studiato i principi della crittografia ed appreso l'arte di decifrare allora saranno in condizione di evitare i numerosi errori madornali che compromettono la chiave delle cifre migliori ed ai quali sono necessariamente esposti tutti i profani. Solo così questo articolo del regolamento del 19 novembre 1874, che ho menzionato più sopra, potrà ricevere un'applicazione pratica veramente soddisfacente.

III I diversi metodi crittografici

I diversi sistemi di scrittura segreta possono essere suddivisi in tre gruppi principali:

1. Il gruppo che si limita ad una trasposizione semplice delle lettere del testo chiaro;
2. Il gruppo che basa la combinazione della cifra su un'inversione dell'ordine alfabetico;
3. Ed, infine, il gruppo che rappresenta le sillabe, le parole o perfino delle frasi intere mediante numeri o gruppi di lettere[24].

A. Cifratura per trasposizione.

I sistemi che si basano su una trasposizione delle lettere sono molto antichi, essi permettono numerose variazioni ed hanno costituito il fondamento di alcuni apparecchi meccanici, quali le *griglie*, che godono ancor oggi del favore del pubblico[25].
Ecco un esempio di trasposizione elementare: le lettere del dispaccio sono state dapprima scritte secondo l'ordine naturale in un certo numero di righe di un numero determinato di caratteri, poi sono state ricopiate in un ordine convenuto[26], il numero secondo il quale si è creata la seconda disposizione rappresenta la chiave[27].

Une attaque simulée aura lieu demain matin à quatre heures.

[Domani mattina alle ore quattro avrà luogo un attacco simulato].

A	1	2	3	4	5	6	7	8	9	10	11
1	u	n	e	a	t	t	a	q	u	e	s
2	i	m	u	l	e	e	a	u	r	a	l
3	i	e	u	d	e	m	a	i	n	m	a
4	t	i	n	a	q	u	a	t	r	e	h
5	e	u	r	e	s	a	b	c	d	e	f

B	2	11	9	8	5	3	10	1	7	6	4
1	n	s	u	q	t	e	e	u	a	t	a
2	m	l	r	u	e	u	a	i	a	e	l
3	e	a	n	i	e	u	m	i	a	m	d
4	i	h	r	t	q	n	e	t	a	u	a
5	u	f	d	c	s	r	e	e	b	a	e

= **usuqteeuatamlrueuaiaeleanieumiamdihrtqnetauaufdcsreebae**

Basta che il decifratore sospetti il tipo di procedimento utilizzato e vada subito a valutare la frequenza della lettera E, che è quella più frequente ed allora la decifrazione non richiede altro che alcuni tentativi. Basta contare prima di tutto il numero totale delle lettere del crittogramma e di scomporle in due fattori (55 = 5 x 11), un fattore rappresenterà il numero delle righe orizzontali e l'altro quello delle colonne verticali. Soltanto la presenza di una q o di una x, la prima lettera è sempre seguita da una u mentre la seconda ne è preceduta, tradisce il segreto della chiave.
In riferimento ai processi intentati ai nichilisti, i giornali russi ci hanno fatto conoscere la cifra segreta adottata dagli accusati: si tratta di un sistema a trasposizione doppia. Le lettere dopo essere state trasposte una prima volta per colonne, vengono trasposte una seconda volta per righe. Una stessa parola serve come chiave per le due trasposizioni[28]. Per questo scopo essa viene trasformata in un numero, sostituendo ciascuna lettera con una cifra araba in modo tale che il valore di tale cifra corrisponda alla posizione della lettera nella parola secondo la successione alfabetica[29].
Ecco il procedimento applicato alla parola chiave *Schuvalow*:

a	c	h	l	o	s	u	v	w
1	2	3	4	5	6	7	8	9

=

s	c	h	u	v	a	l	o	w
6	2	3	7	8	1	4	5	9

Quindi, se bisogna trasporre una frase come questa:

Vous êtes invité à vous trouver ce soir, à onze heures précises, au local habituel de nos réunions
[Siete invitato a presentarvi questa sera, alle undici precise, al locale in cui abitualmente ci incontriamo].

In una prima fase si procederà come nel caso precedente, poi si continuerà con l'esecuzione della stessa operazione sulle righe.

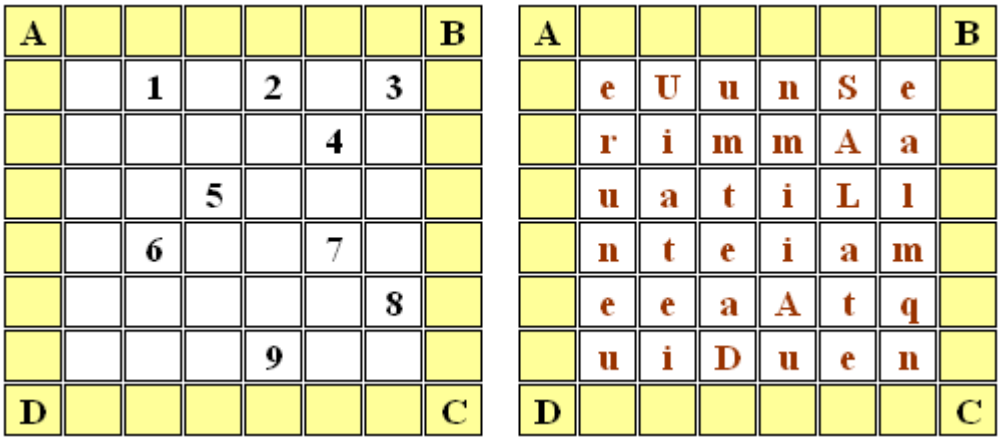
A	1	2	3	4	5	6	7	8	9
1	v	o	u	s	e	t	e	s	i
2	n	v	i	t	e	a	v	o	u
3	s	t	r	o	u	v	e	r	c
4	e	s	o	i	r	a	o	n	z
5	e	h	e	u	r	e	s	p	r
6	e	c	i	s	e	s	a	u	l
7	o	c	a	l	h	a	b	i	t
8	u	e	l	d	e	n	o	s	r
9	e	u	n	i	o	n	s	x	x

B	6	2	3	7	8	1	4	5	9
6	s	c	i	a	u	e	s	e	l
2	a	v	i	v	o	n	t	e	u
3	v	t	r	e	r	s	o	u	c
7	a	c	a	b	i	o	l	h	t
8	n	e	l	o	s	u	d	e	r
1	t	o	u	e	s	v	s	e	i
4	a	s	o	o	n	e	i	r	z
5	e	h	e	s	p	e	u	r	r
9	n	u	n	s	x	e	i	o	x

= **`sciaueselavivonteuvtrersoucacabiolhtnelosuder`**, ecc.

Per quanto questa trasposizione ci possa sembrare complicata, la decifrazione di un crittogramma scritto secondo tale sistema, non presenterà mai delle difficoltà insormontabili nelle lingue in cui alcune lettere non possono presentarsi se non in associazioni determinate, come è il caso della **q** e della **x**, per la lingua francese. Sembra che anche i decifratori russi abbiano portato a conclusione il loro gravoso incarico in un tempo relativamente breve.

Se si adotta un sistema più complicato, questo cessa di essere pratico senza diventare per questo molto più difficile da decifrare.
Ho detto che la griglia[30] si basa sul principio della trasposizione delle lettere. Si tratta di un procedimento ingegnoso, molto utilizzato nel secolo scorso e che i perfezionamenti introdotti di recente ad opera del colonnello austriaco Fleissner sembrano averlo reso indecifrabile[31].
La figura che segue ne raffigura un vecchio modello: si tratta di una placca metallica quadrata, suddivisa in 36 caselle, nove delle quali sono numerate e tagliate in modo da rendere visibile il loro contenuto.
Supponiamo di voler scrivere la frase dianzi citata, con esclusione delle ultime tre parole. Allo scopo posizioniamo la placca su un foglio di carta, sulla quale preliminarmente abbiamo tracciato un quadrato delle stesse dimensioni e scriviamo, nelle caselle scoperte, le prime nove lettere del dispaccio, poi facciamo ruotare da destra a sinistra, in modo che il lato BC prenda il posto del lato AB. Quindi scriviamo le nove lettere successive e si rigira la placca per continuare la medesima operazione fino alla 36ª lettera. Si avrà il seguente crittogramma, in cui, per maggiore chiarezza, ho indicato in maiuscolo le iniziali delle parole.



= **euunserimmaauatillateiameeaatquiduen.**

La griglia del colonnello Fleissner (*neue Patronen-Geheimschrift*) è il frutto di ricerche lunghe e pazienti e può essere variata all'infinito; ma, oltre qualche inconveniente pratico, essa non può, a mio modo di vedere, essere utilizzata in guerra, perché esige il segreto più assoluto.

B. Cifratura per sostituzione

Tra i sistemi che ricorrono alla sostituzione bisogna distinguere quelli a base invariabile, cioè quelli in cui ogni lettera dell'alfabeto è rappresentata, nell'ambito del medesimo crittogramma, dallo stesso carattere o dallo stesso segno da quelli a base variabile, in cui si cambia alfabeto al cambiare di ogni parola o di ogni lettera. Comunemente i primi sistemi sono denominati a *chiave semplice* mentre i secondi a *chiave doppia*.
I sistemi a chiave semplice non offrono nessuna sicurezza mentre i sistemi a chiave doppia comportano soltanto combinazioni più o meno indecifrabili.

1. Sistemi a chiave semplice.

Dal punto di vista della forma, i sistemi a chiave semplice possono essere variati all'infinito; si può non solo variare il normale alfabeto in un numero enorme di modi differenti, ma si possono pure sostituire i caratteri alfabetici con numeri o segni algebrici o astronomici o di fantasia o ancora con gruppi di lettere o di cifre e perfino con parole o frasi intere. Tuttavia, per il decifratore, tutte queste

combinazioni non costituiscono che un solo ed identico sistema che si può volgere in chiaro con un unico procedimento di decifrazione.
Il sistema che è contemporaneamente più semplice e più pratico è quello in cui si cambia il valore delle lettere dell'alfabeto secondo una chiave convenuta.
Noi abbiamo visto, più sopra, come viene trasformata una parola chiave letterale in una chiave numerica. Si può adottare il medesimo procedimento per stabilire l'ordine di successione delle lettere del nuovo alfabeto. Sia *Champigny* la chiave; la chiave numerica che le corrisponde è 241685379. Se noi volessimo ordinare l'alfabeto crittografico secondo questo numero otterremmo:

2	4	1	6	8	5	3	7	9
b	d	a	f	h	e	c	g	i
k	m	j	o	q	n	l	p	r
t	v	s	x	z	w	u	y	

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	d	a	f	h	e	c	g	i	k	m	j	o	q	n	l	p	r	t	v	s	x	z	w	u	y

Tournez les positions de l'ennemi **[Aggirate le posizioni del nemico]**

darà, utilizzando questo alfabeto, il seguente crittogramma:

VNSRQHY JHT LNTIVINQT FH JHQQHOI

Questo sistema è vecchio di duemila anni, infatti, già l'imperatore Augusto se ne serviva per scrivere ai suoi figli[32] e, al dire di Svetonio e di Aulo-Gellio, lo stesso Cesare non aveva niente di meglio, per corrispondere segretamente con i suoi amici, che un alfabeto dove ogni lettera era avanzata di quattro posizioni[33]. Così si utilizza spesso il termine generico di *metodo di Giulio Cesare* per indicare ogni sistema che si basa su una sostituzione semplice delle lettere dell'alfabeto[34].
Importa poco che i caratteri crittografici siano numeri, segni di fantasia o lettere normali dell'alfabeto.
La Bibliothèque nationale [http://www.bnf.fr/] possiede due volumi di lettere cifrate, trovate da Moreau ad Offenburg, nei carri del generale austriaco Klinglin, incaricato del servizio di corrispondenza segreta. In queste lettere, che erano molto compromettenti per il partito realista di quel tempo, ogni carattere del testo chiaro era sostituito sempre con lo stesso numero, composto da due cifre arabe, mentre la fine delle parole vi era indicata con uno zero. È probabile che il generale fosse più abile in tattica militare che in crittografia, perché egli evidentemente ignorava il principio elementare che sto per ricordare. Egli credeva che bastava suddividere arbitrariamente qualche parola per ingannare i decifratori.
Ecco, come esempio, la prima frase di una di queste lettere, datata 31 dicembre 1795:

899952450 44520 455625365211250 *si ce n'est la* 3152891499 14 255452 44520 2311094259467524594995645 44118934 5294 445234114544520.

89	99	52	45	0	44	52	0	45	56	25	36	52	11	25	0	si	ce	n'est	la
r	i	e	n		d	e		n	o	u	v	e	a	u	0	.	.	.	.

31	52	89	14	99	14	25	44	52		44	52	0	23	11	0	94	25	94	67-
c	e	r	t	i	t	u	d	e		d	e		l	a		s	u	s	p

52	45	94	99	56	45		44	11	89	34	52	94		44	52	34	11	45	44	52	0
e	n	s	i	o	n		d	a	r	m	e	s		d	e	m	a	n	d	e	

= **Rien de nouveau, si ce n'est la certitude de la suspension d'armes demandée.**

= **niente di nuovo se non c'è certezza della sospensione delle ostilità che è stata richiesta**

Non posso elencare qui tutti i sistemi a chiave semplice, mi devo limitare a citare tra tutti gli autori antichi Trithemius[35], Porta[36], Blaise de Vigenère[37], Bacone[38], Hermann[39] e Mirabeau[40], che hanno progettato degli alfabeti più o meno ingegnosi, la cui descrizione si può trovare nei trattati specialistici[41]. Tuttavia, queste invenzioni non possono avere per noi null'altro che un interesse puramente storico, esse non sono pratiche e sono tutte decifrabili con un'identica facilità, con l'eccezione di quella di Hermann.

2. Decifrazione dei sistemi a chiave semplice

Qualunque sia il sistema adottato, a base invariabile o variabile, la decifrazione di un suo crittogramma di cui non si possiede la chiave comporta due operazioni nettamente distinte: il calcolo delle probabilità ed una serie di tentativi.
Il calcolo delle probabilità si basa su una particolarità comune a tutte le lingue. La conoscenza che determinate lettere sono più frequenti di altre e che il rapporto di queste ripetizioni viene espresso da un valore medio assai costante per le 9 – 12 lettere principali dell'alfabeto. Così nelle lingue francese, inglese e tedesca la lettera E è quella che ha la frequenza maggiore, in spagnolo è la O, in russo la A ed in italiano la E e la I. Nel francese ogni cinque lettere vi è, in media, una E.
Così, se si dovesse decifrare[42] un dispaccio con l'alfabeto sottostante realizzato con la chiave *Orléans*, si saprebbe subito che è la lettera A quella che avrà la frequenza maggiore.

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
e	f	c	b	a	d	g	l	m	j	i	h	k	n	s	t	q	p	o	r	u	z	x	w	v	y

Votre dépêche a été déchiffrée [Il vostro dispaccio è stato decifrato]

darà, in effetti, un crittogramma in cui, su 26 lettere, la A è ripetuta 9 volte:

ZSRPA BATACLA E ARA BACLMDDPNAA

Un calcolo che ho fatto su alcune circolari del Ministro della guerra mi ha dato una media di 560 consonanti e 440 vocali su 1000 lettere, cioè:

E	=	185	N	=	71	D	=	42	F	=	14	B	=	5
S	=	88	T	=	65	M	=	36	Q	=	10	H	=	4
R	=	78	O	=	57	C	=	34	G	=	8	Z	=	3
I	=	74	U	=	32	P	=	24	X	=	7	Y	=	1
A	=	72	L	=	46	V	=	16	J	=	6	K e H	=	0

Quando si opera su dispacci di una o di due righe, non si può contare che sulla E, ma alcune volte succede che la lettera più frequente sia una S, una R o una I[43].
Oltre alla ripetizione delle lettere considerate isolatamente, bisogna osservare le loro diverse combinazioni binarie e ternarie ed una pletora di altre particolarità, che sarebbe troppo lungo elencare in questa sede.
Così, per le combinazioni binarie della E, si incontrano più spesso **es** e **en**, seguono, per ordine di importanza, **se**, **te**, **et**, **de**, **me**, **el**, **em**, **le**.
Non parlo della composizione stessa delle parole, perché un sistema che conservasse nel testo cifrato la disposizione esteriore delle parole del testo chiaro non presenterebbe alcuna ombra di sicurezza.
In generale basta, nella decifrazione di un crittogramma, conoscere il carattere che cifra la E, per essere sicuri di trovare, per calcolo o per tentativi, il significato di tutte le altre lettere. Si potrebbe perfino assumere preliminarmente che il valore di una cifra si rapporti alla resistenza che essa offre contro l'individuazione del segno ad essa corrispondente[44].
Poiché il mio scopo non è di insegnare al lettore la decifrazione ma di indicargli la tecnica seguita dai decifratori, mi accontenterò di mostrargli un esempio molto elementare di decifrazione di un testo di cui non si possiede la chiave.
Si abbia il crittogramma:

SP Z BOB CSRRSQSPB CB PSXB JBJ PBOOXBJ.

1	2	3	4	5	6	7	8
SP	Z	BOB	CSRRSQSPB	CB	PSXB	JBJ	PBOOXBJ

Il carattere a frequenza maggiore è la *b*. Dico che esso deve corrispondere alla E e faccio il seguente ragionamento:
N° 3: BOB: in fatto di trigrammi che comincino e finiscano con una e, c'è solo *été*.
N° 2: Z: la lingua francese non ha che due monogrammi, *a* e *y*; étè non può essere preceduta da Y, perciò Z = a.
N° 7: JBJ: questo gruppo non può che essere *ses*; è l'unico trigramma che possiede una e nel mezzo, che sia preceduta e seguita dalla medesima lettera.
N° 8: PBOOXBJ: noi conosciamo già cinque lettere di questo gruppo, *.ett.es*; l'unica parola che risponde a questa disposizione è *lettres*.
N°. 1: SP: gli unici bigrammi che possono reggere *été* sono *ça*, *il* e *on*; allora P è una *l*, dunque SP = *il*.
N° 6: PSXB = *lire*.
N° 4. CSRRSQSPB: gia conosciamo cinque cifre: *.i..i.ile*.
La terminazione *ile* indica un aggettivo; in merito agli aggettivi in *ile* di nove lettere che abbiano due *i* nel corpo della parola, il dizionario delle rime non ha che *difficile*.
N°. 5: CB = *de*.

Abbiamo dunque: **Il a èté difficile de lire ses lettres. [È stato difficile leggere le sue lettere.]**
Più un crittogramma è lungo e più è facile decifrarlo. Come regola generale una riga è sufficiente.
Il generale Lewal afferma nei suoi *Etudes de guerre*[45] [Studi di guerra] che una cifra a chiave semplice garantisce *sufficientemente* il segreto per le necessità ordinarie e «per affari senza importanza rilevante».
Non so che cosa si vuole intendere per affari senza importanza rilevante, ma il lettore ha potuto rendersi conto dall'analisi appena effettuata sul crittogramma di cui sopra che un dispaccio scritto in modo simile a questo e che sia lungo due o tre righe, può essere decifrato a vista senza il ricorso ad alcun artificio particolare.
La cifra a chiave semplice può presentare qualche minima garanzia se si osservano le condizioni seguenti:

1. La separazione delle parole non deve comparire nel testo cifrato;
2. Le lettere doppie devono essere evitate;
3. Non si adoperino le maiuscole, né gli accenti, né la punteggiatura. Allo scopo di evitare gli errori di trascrizione è indispensabile pure frazionare i crittogrammi in gruppi di quattro o cinque lettere[46]. Pertanto, il nostro ultimo dispaccio dovrebbe essere crittografato come segue: **il a été dificile de lire ses letres, [è stato difficile legere le sue letere],**

= **SPZBO BCSRS QSPBC BPSXB JBJPB OXBJ**

3. Sistemi a chiave doppia.

Abbiamo visto che le cifre a *chiave doppia* sono quelle in cui si cambia l'alfabeto ad ogni lettera cifrata.
Sono state escogitate molte metodiche a base variabile, ma ce ne sono solo tre o quattro che hanno una rilevanza pratica e che sono ancora al passo coi nostri tempi. Benché differenti per forma, nella sostanza si somigliano tutte e si rifanno al sistema proposto da Blaise de Vigenère nel XVI secolo. Per quasi tre secoli sono state utilizzate nelle comunicazioni segrete dalla maggior parte delle piccoli corti dell'Italia e della Germania ed ancora oggi sono ritenute indecifrabili da persone non al passo coi procedimenti di decifrazione.
Inoltre ogni metodo di scrittura crittografica destinata all'esercito deve poter essere trasmessa telegraficamente. Noi non ci dobbiamo preoccupare che dei sistemi basati unicamente sull'impiego di lettere o di numeri arabi, con l'esclusione di ogni combinazione che esiga l'impiego simultaneo dei due tipi di simboli[47].

a. Sistema di Porta

L'invenzione del primo sistema *letterale*[48] a chiave doppia risale, come ho già detto, al fisico Porta[49], anche se lui stesso fu ben lontano dal comprendere l'importanza dell'introduzione di una chiave propriamente detta nei sistemi di scrittura cifrata, ciò non di meno lo dobbiamo considerare come il fondatore della crittografia.
Porta impiega undici alfabeti differenti, che contraddistingue, come si vede nell'immagine sottostante, con le lettere AB, CD, ecc., o più semplicemente con A, C o B e D.
Se vogliamo scrivere con uno qualsiasi di questi alfabeti, scegliamo, per rappresentare le lettere del testo chiaro, quelle che, nel riquadro stanno loro di fronte.

AB	a	b	c	d	e	f	g	h	i	l	m
	n	o	p	q	r	s	t	v	x	y	z
CD	a	b	c	d	e	f	g	h	i	l	m
	z	n	o	p	q	r	s	t	v	x	y
EF	a	b	c	d	e	f	g	h	i	l	m
	y	z	n	o	p	q	r	s	t	v	x
GH	a	b	c	d	e	f	g	h	i	l	m
	x	y	z	n	o	p	q	r	s	t	v
IL	a	b	c	d	e	f	g	h	i	l	m
	v	x	y	z	n	o	p	q	r	s	t
MN	a	b	c	d	e	f	g	h	i	l	m
	t	v	x	y	z	n	o	p	q	r	s
OP	a	b	c	d	e	f	g	h	i	l	m
	s	t	v	x	y	z	n	o	p	q	r
QR	a	b	c	d	e	f	g	h	i	l	m
	r	s	t	v	x	y	z	n	o	p	q
ST	a	b	c	d	e	f	g	h	i	l	m
	q	r	s	t	v	x	y	z	n	o	p
VX	a	b	c	d	e	f	g	h	i	l	m
	p	q	r	s	t	v	x	y	z	n	o
YZ	a	b	c	d	e	f	g	h	i	l	m
	o	p	q	r	s	t	v	x	y	z	n

Così, se si vuol crittografare con l'alfabeto D o C si trasforma la *a* in *z* e viceversa; *b* in *n* ed *n* in *b* e così di seguito. Ma per sviare i calcoli degli investigatori, Porta, uomo che sa decifrare, raccomanda di scrivere ogni lettera con un alfabeto differente. Inoltre, per non obbligare i corrispondenti a prendere gli undici alfabeti di seguito, la qual cosa ben presto tradisce il segreto, egli propose di adottarne quattro, cinque o sei e di convenire una parola le cui lettere indicano gli alfabeti da scegliere in successione[50]. Questa parola costituisce la *chiave* del crittogramma, la si scrive sotto il testo da cifrare, ripetendola secondo la necessità.

Ecco un esempio con la chiave *roi*:

vot	red	epe	che	est	dec	hif	fre	e
ROI	ROI	ROI	ROI	ROI	ROI	ROI	ROI	R
dhm	ayz	xin	ton	xam	vyy	npo	ymn	x

L'invenzione di Porta, come abbiamo visto, apre, in qualche modo, una nuova era nella storia della crittografia, ma essa presenta due grossi inconvenienti, per cui è stata abbandonata già da molto tempo. In primo luogo, il piccolo numero dei suoi alfabeti e poi la necessità di rappresentare lo stesso alfabeto con due lettere differenti. Come conseguenza di quest'ultimo fatto, una parola di quattro lettere, come *poli*, dà una chiave solo per due alfabeti.

b. La tabula recta o Carré di Vigenère

Il *carré di Vigenère*, detto anche *cifra indecifrabile* o *cifra per eccellenza*, non è altro che il sistema di Porta, semplificato da Blaise de Vigenère, che l'ha descritto, nella forma in cui è ancora in uso ai nostri giorni, nel suo *Traité des Chiffres* [Trattato sulle cifre][51]. Il carré ha goduto di un credito straordinario nelle cancellerie del XVIII secolo, e si potrebbe ritenere che non ne esista uno migliore in base al fatto che lo si utilizza ancora, dopo il 1870, nel ministero della guerra.
Dlandol l'ha fatto conoscere al pubblico, all'epoca della Rivoluzione, nell'opuscolo che ho già citato. Al capitolo VI egli dice che «questa cifra è stata definita la cifra per eccellenza, perché essa unisce il maggior numero di vantaggi che si possano desiderare per una corrispondenza segreta. Essa li possederebbe tutti senza alcuna eccezione», aggiunge, «se non fosse per la sua lentezza procedurale; ma essa compensa molto bene questo inconveniente con la sua incredibile sicurezza. Queste sicurezza è tale che l'intero universo non la può comprendere. Infatti, se non si conosce la parola chiave convenuta dai corrispondenti, si può mostrare un suo dispaccio a tutti, senza che nessuno sia in grado di leggerlo». Certamente il cittadino Dlandol è stato più un grande patriota che un abile decifratore!

La disposizione del carré di Vigenère differisca da quella del quadrato di Porta per il fatto che ricorre ad un *quadrato* ottenendo così tanti alfabeti diversi quante sono le lettere contenute nell'alfabeto[52].

	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

Per quanto riguarda l'utilizzo di questo carré, si procede allo stesso modo utilizzato per il sistema di Porta. Occorre solo notare che l'alfabeto orizzontale superiore rappresenta l'alfabeto in chiaro e che gli altri 26 alfabeti che seguono sono gli alfabeti cifranti.

Si debba cifrare **Détruisez le tunnel [Distruggete la galleria]** con i tre alfabeti corrispondenti alla parola **BAC**, si avrà:

det	rui	sez	let	unn	el
BAC	BAC	BAC	BAC	BAC	BA
eev	suk	teb	mev	vnp	fl

Nulla di più facile che leggere un crittogramma scritto in questo modo, quando se ne conosce la chiave: si trascrive il testo cifrato in blocchi uguali al numero degli alfabeti impiegati, si scrive al di sotto di essi la chiave e si compie l'operazione inversa a quella di cifratura.
Si debba decifrare: **eyfdaolrakhhgmhncfmk** con la chiave **Tunis**. Si troverà:

eyfda	olrak	hhgm	ncfmk
TUNIS	TUNIS	TUNIS	TUNIS
lesvi	vress	ontep	uises

Come vedremo più avanti, i dispacci scritti con il quadrato di Vigenère si decifrano molto facilmente, solo in casi eccezionali tale sistema può offrire qualche sicurezza.

c. Sistema di Saint-Cyr

Questo sistema, in uso da molto tempo, non è altro che una forma mascherata del tableau di Vigenère. A motivo della mancanza di una denominazione propria, io l'ho chiamato col nome della scuola dove oggi viene insegnato e raccomandato caldamente.
Ed eccone la descrizione, derivata dal *Cours d'Art militaire* [Corso di Arte militare] edito nell'anno 1880-81, identico a quello autografato per gli allievi della 1ª divisione[53].
«Lo strumento - si dice nel libro - si compone di una parte *fissa*, al di sotto della quale scorre un *alfabeto mobile doppio*. Allo scopo sono sufficienti due strisce di carta quadrettata[54].

	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	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	b	c	d	e	ecc.

Si prende una parola qualunque di 3 – 5 lettere, per formare la chiave[55]. Adottiamo la parola **BAC** e consideriamo il seguente dispaccio:

Détruisez le tunnel [Distruggete la galleria].

«Se la chiave è di tre lettere, suddividiamo la frase da cifrare in gruppi uguali di tre lettere ciascuno, come nel modo seguente: *dét – rui – sez – let – unn – el*. Si cifrano prima le prime tre lettere di ogni gruppo, poi le seconde e poi, infine, le terze.
Per cifrare le prime lettere, si pone la prima lettera della chiave, la B, presa sull'alfabeto mobile, sotto la lettera A dell'alfabeto fisso (vedi la figura di sopra). Prendendo la prima lettera di ciascun gruppo del dispaccio sull'alfabeto superiore, si scrive la lettera ad essa corrispondente dell'alfabeto inferiore.
Si passa in seguito alle seconde lettere dei gruppi. Per cifrarle si pone la seconda lettera della chiave, la A, sotto la lettera A dell'alfabeto fisso e si ripetono le operazioni che abbiamo appena eseguito. Si procede allo stesso modo per le terze lettere. Il dispaccio sarà cifrato come segue:

det	rui	sez	let	unn	el
BAC	BAC	BAC	BAC	BAC	BA
eev	suk	teb	mev	vnp	fl

Ammettendo, aggiunge il testo, che l'oggetto venga smarrito o catturato, non succede nulla: occorre conoscere la chiave».
È facile vedere che questo procedimento non è che un'abbreviazione del sistema precedente, paragonando nei due sistemi i tre alfabeti che corrispondono alla chiave **BAC**.

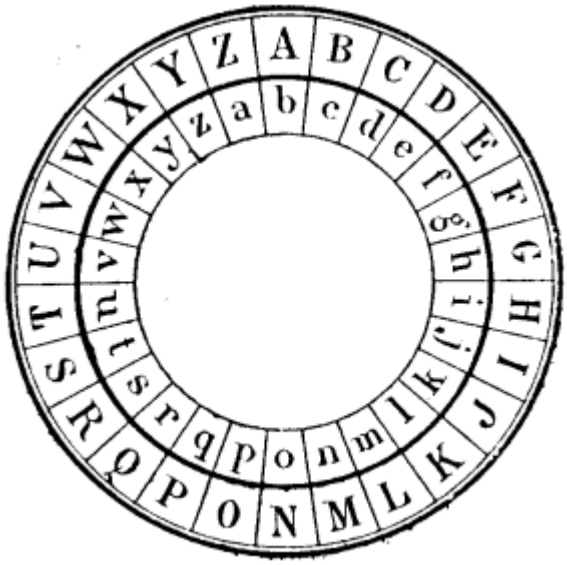
Cifra di Vigenère.

	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

Sistema di Saint – Cyr.

	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	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	b	c	d	e
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	b	c	d	e	
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	b	c	d	e	

Poiché si ottiene il medesimo testo cifrato con i due sistemi, il mittente o il destinatario non si chiedono neppure con quale dei due sistemi sia stato cifrato il dispaccio[56].
L'unico vantaggio che questo sistema presenta rispetto al precedente è che, in caso di perdita, lo strumento può essere ricostruito in due o tre minuti. Dal punto di vista crittografico, esso non ha un vantaggio reale se non alterando l'ordine delle lettere dell'alfabeto mobile.
Si dice nel *Cours d'Art militaire* [Corso d'Arte militare] che si potrebbe costruire lo strumento in un modo tale da renderlo portatile fermandolo al centro dei due cerchi, cosicché uno sia mobile intorno al suo asse venendo così a costituire l'*alfabeto doppio*.



Questa disposizione, rappresentata nella figura precedente, è stata ideata, nel 1563 da Porta[57] ed ha avuto numerose applicazioni, come nella crittografia di Wheatstone e nelle scatole a quadrante mobile che sono state vendute al tempo della guerra d'Italia. Tutti questi apparecchi, alcuni dei quali sono presenti nelle opere recenti di telegrafia e sono presentati come invenzioni meravigliose, non sono in realtà altro che un semplice tableau di Vigenère.

d. Sistema di Beaufort.

È stata apportata al tableau di Vigenère una modifica molto ingegnosa ad opera dell'ammiraglio inglese Francis Beaufort (1857). Anche se a prima vista la modifica sembra riguardare solo l'utilizzo del tableau, in verità essa altera sensibilmente il testo cifrato per dargli agli occhi dei non iniziati un'autentica aria di indecifrabilità. Ecco subito questo tableau:

abc	def	ghi	jkl	mno	pqr	stu	vwx	yza
bcd	efg	hij	klm	nop	qrs	tuv	wxy	zab
cde	fgh	ijk	lmn	opq	rst	uvw	xyz	abc
def	ghi	jkl	mno	pqr	stu	vwx	yza	bcd
efg	hij	klm	nop	qrs	tuv	wxy	zab	cde
fgh	ijk	lmn	opq	rst	uvw	xyz	abc	def
ghi	jkl	mno	pqr	stu	vwx	yza	bcd	efg
hij	klm	nop	qrs	tuv	wxy	zab	cde	fgh
ijk	lmn	opq	rst	uvw	xyz	abc	def	ghi
jkl	mno	pqr	stu	vwx	yza	bcd	efg	hij
klm	nop	qrs	tuv	wxy	zab	cde	fgh	ijk
lmn	opq	rst	uvw	xyz	abc	def	ghi	jkl
mno	pqr	stu	vwx	yza	bcd	efg	hij	klm
nop	qrs	tuv	wxy	zab	cde	fgh	ijk	lmn
opq	rst	uvw	xyz	abc	def	ghi	jkl	mno
pqr	stu	vwx	yza	bcd	efg	hij	klm	nop
qrs	tuv	wxy	zab	cde	fgh	ijk	lmn	opq
rst	uvw	xyz	abc	def	ghi	jkl	mno	pqr
stu	vwx	yza	bcd	efg	hij	klm	nop	qrs
tuv	wxy	zab	cde	fgh	ijk	lmn	opq	rst
uvw	xyz	abc	def	ghi	jkl	mno	pqr	stu
vwx	yza	bcd	efg	hij	klm	nop	qrs	tuv
wxy	zab	cde	fgh	ijk	lmn	opq	rst	uvw
xyz	abc	def	ghi	jkl	mno	pqr	stu	vwx
yza	bcd	efg	hij	klm	nop	qrs	tuv	wxy
zab	cde	fgh	ijk	lmn	opq	rst	uvw	xyz
abc	def	ghi	jkl	mno	pqr	stu	vwx	yza

Emparez-vous des hauteurs [Impadronitevi delle vette], cifrato con la chiave **BAC**, darà il seguente crittogramma:

emp	are	zvo	usd	esh	aut	eur	s
BAC	BAC	BAC	BAC	BAC	BAC	BAC	B
xon	bjy	cfo	hiz	xiv	bgj	xgl	j

Vediamo adesso come si procede. Trovate la lettera *e* nel primo alfabeto orizzontale, scendete in linea retta fino ad incontrare la *b*, quindi compite un angolo retto, a destra o a sinistra, fino all'estremità della colonna e la lettera *x* che ivi troverete è la lettera cifrata cercata. Procedete allo stesso modo per le altre lettere.
I decifratori inglesi, che il sistema di Beaufort ha tanto meravigliato, certamente non sospettavano che si può ottenere il medesimo risultato con il sistema di Vigenère o di Saint – Cyr molto semplicemente invertendo l'alfabeto normale[58].
È facile assicurarsene osservando le due figure seguenti:

Cifra di Vigenère

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

Sistema di Saint – Cyr

	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	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	a	b	c	ecc.
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	b	c	d	ecc.
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	b	c	d	e	ecc.

Il risultato sarà ancora lo stesso se, invece di invertire l'ordine delle lettere dell'alfabeto normale si mette l'alfabeto *a z y x w v u t s r q p o n m l k j i h g f e d c b* nel riquadro, come di seguito indicato:

	A	B	C	D	E	F	G	H	I	J	ecc.
A	a	z	y	x	w	v	u	t	s	r	
B	b	a	z	y	x	w	v	u	t	s	
C	c	b	a	z	y	x	w	v	u	t	
D	d	c	b	a	z	y	x	w	v	u	

e. Sistema di Gronsfeld

Questo sistema differisce dai due precedenti solo per il fatto che può essere elaborato mentalmente senza richiedere l'utilizzo di una tabella o di un apparecchio qualsiasi.
Ecco come M. Bontemps, ispettore delle linee telegrafiche, si esprime in merito[59]: «Supponiamo che si sia scelto come chiave un numero qualsiasi. Lo si scriva al di sotto della frase che si vuole trasmettere tante volte fino ad eguagliare la lunghezza della frase, stabilendo la corrispondenza tra le lettere e le cifre successive. Si prende come lettere da inviare quella dell'alfabeto cifrante che si

trova nell'alfabeto ad una distanza pari a quella dell'alfabeto chiaro e si compone così una scrittura segreta di cui è impossibile scoprire la chiave nemmeno possedendo la perspicacia che Edgar Allan Poe aveva concesso al suo eroe nel romanzo *Lo scarabeo d'oro* o l'intelligenza degli agenti impiegati a decifrare la corrispondenza della duchessa de Berry nel 1832, secondo il racconto che se ne fa nelle memorie di M. Gisquet».
Non dispiaccia all'autore che ho appena citato che il sistema del conte di Gronsfeld non è molto più difficile da decifrare di una modesta cifra a chiave semplice, esso non è, del resto, che una forma mascherata del tableau di Vigenère[60].
Riprendiamo il nostro esempio e si debba ancora una volta cifrare **Détruisez le tunnel [Distruggete la galleria]**, con la chiave 102. Ogni lettera del testo chiaro sarà rappresentata rispettivamente da un'altra, di una posizione più avanti, della stessa posizione o di due posizioni più avanti:

det	rui	sez	let	unn	el
102	102	102	102	102	10
eev	suk	teb	mev	vnp	fl

A condizione di prendere una chiave composta esclusivamente da numeri minori di 10, questo sistema realizza perfettamente il nostro terzo desideratum ed offre anche, se i numeri sono molto piccoli, alcune comodità pratiche, ma questi vantaggi perdono considerevolmente il loro pregio a causa di alcuni appigli che questo sistema fornisce alle investigazioni dei decifratori.

f. Sistema a chiave variabile

Vedremo più avanti che la decifrazione dei sistemi a chiave doppia si basa essenzialmente sulla conoscenza del numero delle lettere che compongono la chiave. Sono state ideate numerose metodiche per impedire ai decifratori di farne il calcolo ed una delle migliori è dovuta ad un membro della Commissione della telegrafia militare. Questi propone di terminare, ad intervalli irregolari, l'ordine di successione degli alfabeti, nel modo indicato dalla chiave, per ricominciare bruscamente dalla lettera iniziale o primo alfabeto. Così, se la chiave è **Epaminondas** [**Epaminonda**], invece di ripetere regolarmente per serie di undici lettere, egli la taglia arbitrariamente e scrive: **epa** + **epaminonda epaminondas** + **epami** + **epamino** + ecc.
Il punto di arresto è indicato da una lettera della chiave, che viene intercalata nel testo cifrato nel punto voluto. Ed ecco un esempio, in cui ho preso come lettera d'arresto la seconda lettera della chiave, cioè la P:

Nous	+	partons	+	de	+	main
EPAM	+	EPAMINO	+	EP	+	EPAM
....	p	.....	p	..	p	....

Per evitare qualsiasi confusione nel significato della lettera d'arresto, questa è sostituita nel testo cifrato dalla cifra araba che corrisponde alla posizione che essa stessa occupa nella parola chiave. Pertanto, nel nostro esempio in cui la lettera P è la seconda lettera della chiave essa sarà sostituita da un 2, in tutte le posizioni in cui essa non ha la funzione di lettera di arresto.
Col carré avremo il seguente crittogramma:

rduePt2rfwagPhtPq2az.

Per impedire al decifratore di fare un tentativo sulle prime lettere del dispaccio, lo si fa precedere da qualche *nulla*, avendo cura di indicare con la lettera d'arresto il punto in cui comincia il testo vero. Il nostro crittogramma potrebbe essere infine scritto:

xmoPrduePt2rfwagPhtPq2az.

Auguste Kerckhoffs
Dottore in lettere
Professore della Scuola di alti studi commerciali e della Scuola Arago.

---

[1]. È sotto la rubrica: *Stéganographie, chiffre* o *écritures secrètes*, che alcuni dizionari enciclopedici recano informazioni sulla crittografia. Gli autori antichi la denominano più o meno correttamente: *ars notarum, ars zipherarum, polygraphia, scotographia, cryptologia, steganologia, cryptomenytices*, ecc. I tedeschi, oggi, parlano di *Geheimschrift* o *Chiffreschrift* e gli inglesi di *cryptography*.

[2] Lettere nascoste nelle suole del messaggero, comunicazioni celate nell'ulcera del corriere o negli orecchini delle donne, dadi bucati con 24 fori attraverso i quali passa un filo, piccioni viaggiatori [http://www.cix.co.uk/~mhayhurst/jdhayhurst/pigeon/pigeon.html], ecc. Enea IV secolo AC) è l'autore militare più antico di cui possediamo gli scritti, nel suo capitolo XXXI dei suoi *Commentari sulla difesa dei luoghi* (tradotto dal maresciallo di campo Beausobre, 1757) è consacrato alle *lettere cifrate e al modo di farle pervenire segretamente*.

[3] L'invenzione di Kessler, che il colonnello Laussedat ha ricordato in una sua conferenza, è esposta in un libro diventato molto raro, pubblicato nel 1616 a Oppenheim ed intitolato: *Unterschiedene bisshero mehrern Theils secreta oder Verborgene geheime Künste*.

[4] Storia romana, libro X, capitolo 44 -48.

[5] Lisandro, capitolo 19.

[6] Capitolo XL, 9; capitolo XLI, 3.

[7] Cesare, capitolo 56, Ottavio, capitolo 88.

[8] Notti attiche, libro XVIII, capitolo 9.

[9] Origini, I, 24.

[10] Si trova in Kestoi, opera sull'arte militare attribuita a Giulio l'Africano, di cui una traduzione francese è data in *Mémoires critiques et historiques de Guischardt*, non è altro che una copia dei *Commentari di Enea*. Filone di Bisanzio, l'autore della *Poliorcetica*, che visse nel II secolo AC, aveva composto un intero trattato sull'*Invio di lettere segrete*, ma quest'opera è andata perduta.

[11] Gasparis Schotti, Schola steganographica, 1665; classis VIII.
[http://www.petitcolas.net/fabien/steganography/steganographica/index.html]

[12] Gustavi Seleni, *Cryptomenytices et cryptographiae* libri IX, 1624.

[13] Vedere *Commentaires sur la défense des places*, pagina 145, Nota del traduttore [NdT: francese].

[14] Si trova il seguente precetto nel *Breviarium Politicorum* del cardinale Mazarino: *Scribere secreta manu tua ne graveris, nisi per zifras scribas*.

[15] Cf. Bardin, *Dictionnaire de l'Armée de terre*, 1843.

[16] Manoscritto del 1812, contenente il sommario degli avvenimenti di quest'anno, per servire la storia di Napoleone ; 1827. – Il colonnello Fleissner (*Handbuch der Kryptographie*) gli attribuisce anche, ma a torto, l'invenzione di una nuova cifra.

[17] *Tactique de marche*, 1876.

[18] Vedere l'articolo *Chiffre stéganographique*.

[19] Il capitano Henri Berthaut, al quale faccio allusione, è certamente uno dei più abili decifratori dello stato maggiore.

[20] Tomo III, pagina 76.

[21] *Dictionaire philosophique*, articolo *Poste*. È assai curioso vedere il conte di Clarendon, nella lettera scritta cent'anni prima al dottor John Barwick, esprimersi in termini analoghi sul conto dei decifratori: « I have heard of many of the pretenders of that skill, and have spoken with some of them, but have found them all to be mountebanks».

[22] Il *Contr'Espion* o le chiavi di tutte le corrispondenze segrete.

[23] Le informazioni bibliografiche sono destinate a chi voglia approfondire questa problematica e sono molto utili perché le opere citate, tranne due o tre di esse, sono tutte rinvenibili nella Biblioteca nazionale [http://www.bnf.fr/].

[24] Mi propongo di pubblicare ben presto un'opera completa sui differenti sistemi crittografici ed in essa renderò volentieri conto di ogni sistema nuovo che mi si vorrà comunicare, a condizione che questo abbia una certa validità pratica.

[25] Vedere Kluber, *Kryptographik*, capitolo XIII. Du Moncel, *Exposés des applications de l'électricité*, III, pagina 530.

[26] Poiché la somma delle lettere del testo chiaro deve essere un multiplo del numero delle colonne orizzontali, si aggiungano, se necessario, delle *nulle* fino a riempire la colonna finale, in questo caso ne occorrono cinque.

[27] Un'apparecchiatura ideata dall'architetto parigino M. Rondepierre, il quale l'ha denominata *Phyrographe*, si basa su questo principio.

[28] È un errore molto grave da parte di colui che ha ideato il sistema.

[29] Suppongo che se una lettera è ripetuta si possano considerare le ripetizioni come altrettante lettere in successione alfabetica.

Ad esempio:

Taganrog =	aaggnort 12345678	= 81325764

[30] Sembra che questa procedura sia stata inventata nel XVI secolo dal matematico italiano Girolamo Cardano. Vedere il suo libro *De subtilitate*, tradotto in francese da Richard Leblanc, *De la subtilité et subtiles inventions*. Paris, 1556. - Vedere pure de Prasse, *De reticulis crytographicis*, Leipzig, 1799.

[31] *Handbuch der Kryptographie*, von Fleissner von Wostrowitz, Wien, 1881.

[32] Svetonio, *Ottavio*, capitolo 88; Isidoro Orig., I, 24.

[33] Svetonio, *Cesare*, capitolo 56; Aulo Gellio, *Notti attiche*, libro XVII, capitolo 9.

[34] Nella Bibbia si incontrano esempi analoghi di inversioni: il profeta Geremia (capitolo XXV, 26) scrive, ad esempio, *Sheshach*, in luogo di *Babel*, sostituendo così le due consonanti b ed l con le lettere sh e ch, che occupano la stessa posizione nell'alfabeto ebraico, partendo da destra e procedendo verso sinistra.

[35] *Poligraphiae libri VI*; composti, dopo la prefazione, nel 1508. Ne è stata fatta una traduzione da Gabriel de Collange: *La Polygraphie et universelle escriture cabalistique de Jean Trithème*; Paris, 1561.
A nome dell'abate Trithemius (1462 - 1516) sono state pubblicate numerose opere di crittografia, senza che si possa sapere con certezza quali siano quelle a lui attribuibili (Cf. Schott, *Schola steganographica*, VII). Io credo che non gli si debba attribuire altro oltre l'invenzione di un sistema di scrittura segreta, in cui le lettere sono sostituite da parole scelte in modo da formare, unendole opportunamente, una missiva o una preghiera, sotto le cui apparenze è difficile supporre l'esistenza di un messaggio segreto (imitato nella *Cryptographie* di Du Carlet, 1644). Egli ha realizzato il grande sogno del suo tempo, il *modus sine secreti suspicione scribendi*. Pertanto non vedo la ragione per cui i tedeschi ed altri l'abbiano proclamato padre della crittografia moderna. A me sembra che questo titolo non possa essere attribuito che a Porta (1540 - 1615)), l'inventore del primo sistema *letterale a chiave doppia* e credo di rendere a Cesare quel che è di Cesare associando al nome del fisico italiano quello del diplomatico francese Blaise de Vigenère (1523 - 1596) che per primo ha presentato nel suo *Traité des chiffres* l'uso del cifrario carré, così com'è utilizzato da tre secoli.

[36] *De furtivis litterarum notis, vulga de ziferis;* Napoli, 1563.

[37] *Traicté des chiffres, ou secrètes manières d'escrire*; Paris, 1586.

[38] Vedere Kluber, *Kryptographik*, pagina 122.

[39] Memoria di Beguélin, letta all'Accademia delle scienze e belle lettere di Berlino; tomo XIV, pagina 369.

[40] Vedere Kluber, op. cit., pagina 79.

[41] Oltre gli autori già citati, si possono consultare anche:
Hanedi, *Steganologia et steganographia nova* (testo in tedesco), Nürnberg, 1617.
Seleni, *Cryptomenycites et cryptographiae* libri IX; 1624.

Frederici, *Cryptographia oder geheime correspondentz*; Leipzig, 1685.
L'articolo *Cifra* nell'*Encyclopaedia* di Rees, 1819 e l'articolo *Cryptography* nell'*Encycolpaedia Britannica*, 1877.
Lacroix, *La Cryptographie ou l'art d'écrire en chiffres*; Paris, 1858.

[42] Poiché già abbiamo i vocaboli *crittografia, crittografico, crittogramma e crittografo* deve essere permesso completare la serie di questi termini adottando il verbo *crittografare*.

[43] Le lettere che in tedesco incontriamo più spesso per ordine di frequenza sono: E, N, i, r, s, t, u, d, a, h. In inglese esse sono: E, T, a, o, n, i, r, i, h, d, l.

[44] Il primo trattato di crittografia in cui si affrontano i principi della decifrazione è dovuto a Porta ed è quello che ho menzionato prima: *De furtivis litterarum notis*.
Le opere principali che hanno affrontato lo stesso problema sono elencate di seguito per ordine cronologico:
L'*Interpretation des chiffres*, derivata dall'italiano di Cospi, da F. I. F. N. P. M. (Padre Niceron); Paris, 1641.
Gravezande, *Introduction la philosophie*; Leyle, 1737, capitolo XXXV. Questo capitolo è stato riprodotto molte volte e si trova, tra l'altro, nel Dictionnaire encyclopédique di Diderot e nella *Cryptographie* di Lacroix.
Breithaupt, *Ars decifratoria sive occultas scripturas solvendi et legendi scientia*; Helmstadt, 1737.
Conrad, *Cryptographia denudata, sive ars deciferandi*; Leyde, 1739.
Thickenesse, *A treatise on the art of deciphering; 1772.*
Kluber, *Kryptographik*; Tübingen, 1809.
Vesin de Romanini, *La Cryptographie dévoilé*; Paris 1857.
Kasiski, *Die Geheimschriften und die Dechiffrirkunst*; Wien, 1881.
Si può leggere utilmente anche il capitolo XV dello *Scarabeo d'oro*, le *Ecritures secrètes dévoilées*,di Charles Joliet e l'eccellente articolo di Prodhomme nel *Dictionnaire des connaissances humaines* di Lunel.

[45] *Tactiques des renseignements*, pagina 76.

[46] Poiché l'amministrazione dei telegrafi conta i dispacci segreti per gruppi di cinque lettere, è preferibile il frazionamento in pentagrammi.

[47] Con ogni probabilità il Ministro delle poste e dei telegrafi non tarderà oltre ad applicare al servizio interno i principi della convenzione internazionale di Londra, in base alla quale non è possibile utilizzare nei messaggi segreti contemporaneamente lettere e cifre.
Vi è ancora una considerazione più importante, cioè che è praticamente impossibile evitare di commettere errori nella trasmissione per via telegrafica dei dispacci cifrati, se non si ha cura di suddividerli in piccoli gruppi di lunghezza fissa di 3 – 5 lettere o perché il funzionamento dell'apparecchio di Hughes si oppone al frazionamento regolare dei dispacci, nel caso dell'impiego simultaneo di cifre arabe e di lettere.

[48] Dico *letterale*, cioè basato sull'impiego delle lettere, perché Trithemius aveva già preconizzato, cinquant'anni prima, di usare delle serie di parole o di frasi in corrispondenza delle lettere del testo chiaro.

[49] *De furtivis litterarum notis*, libro II, capitolo 16.

[50] M. Fleissner attribuisce l'invenzione di questo sistema a Napoleone I. Questo non è l'unico er-

rore storico o bibliografico da rimproverare allo storico austriaco.

[51] Vedere pagina 50, b.

[52] Il Padre Kircher (*Polygraphia nova et universalis*; Roma, 1663) ha sostituito le lettere del tableau di Vigenère con numeri, da qui deriva il nome di *Abacus numeralis* per il suo sistema. Invece di scrivere il testo cifrato nel modo ordinario, Kircher prende una pagina scritta qualsiasi ed indica i numeri del crittogramma per mezzo di punti che colloca sotto le lettere ad intervalli uguali al valore dei numeri ottenuti. Schott ha commentato il sistema di Padre Kircher nella sua *Schola stenographica* e per questo fatto molti autori e Larousse tra essi, gliene attribuiscono la paternità.

[53] Si trova ugualmente una descrizione di questo sistema in Bartels, *Leifaden für den Unterricht auf den königlichen Kriegsschulen*; Berlin, 1881.

[54] Una casa di Berlino (Egert, 61, Kochstrasse) ha fabbricato un apparecchio meccanico per cifrare con questo sistema.

[55] Vedremo più avanti che se i corrispondenti prendono questa raccomandazione alla lettera, occorrerà appena una mezzora per decifrare senza chiave tutti i dispacci cifrati con questo sistema.

[56] Quando l'alfabeto è disordinato [vedere più avanti] il sistema di Saint-Cyr fornisce un testo diverso.

[57] Cf Colorni, *Scotographia, overe Scienza di scrivere oscuro*; Praga, 1593.

[58] È probabile che lo stesso ammiraglio inglese non ha mai creduto alla possibilità di trasformare il suo sistema in cifra carré ordinaria, altrimenti non si spiegherebbe perché M. Morris Beaufort reclami ancora energicamente in questo momento, a favore del suo illustre padre, l'onore di aver dotato il suo paese di un sistema indecifrabile di crittografia (*Cryptography a system of secret writing, by the late admiral sir Francis Beaufort*).

[59] *Les systèmes télegraphiques aèriens, élettriques, pneumatiques* ; Paris, 1876, pagina 261.

[60] In una conferenza tenuta nel 1873 presso la Società di Scienze militari di Vienna, D'Orges ha sostenuto che questa cifra era stata inventata dal generale Trochu (vedere Fleissner, op. cit., pagina 19).