STUDI DI STORIA MEDIOEVALE E DI DIPLOMATICA

PUBBLICATI A CURA
DELL'ISTITUTO DI STORIA MEDIOEVALE E MODERNA
E DELL'ISTITUTO DI PALEOGRAFIA E DIPLOMATICA

2

UNIVERSITA DEGLI STUDI DI MILANO
1977

Un'ottima applicazione quattrocentesca del sistema cifrante monoalfabetico

di Giorgio Costamagna

Un indubbio interesse, da qualche tempo, si è risvegliato da parte degli studiosi per uno degli aspetti più interessanti, se pur tra i più difficili, dello studio delle scritture segrete usate dalle cancellerie italiane tra Medioevo e Rinascimento. Il lettore avrà certamente inteso che ci si vuol riferire in modo particolare a quelle scritture « in cifra », o, come amavano scrivere i nostri avi, « in ziffera », che tanta parte hanno nelle carte conservate negli archivi del nostro Paese e che ancor oggi spesso attendono chi si accinga a decrittarle. Un utilissimo contributo a questi studi è certamente costituito dalla pubblicazione di cifrari e di codici contenenti cifrari di cui ci ha dato un ottimo esempio Lydia Cerioni nel suo studio « La diplomazia Sforzesca nella seconda metà del Quattrocento »[1]. La conoscenza, infatti, dei sistemi di tempo in tempo usati per cifrare, cioè di quelle che potrebbero essere definite le chiavi per decifrare, vale a dire per passare dal testo segreto a quello in scrittura comune, facilita grandemente il compito dell'interprete indicandogli una serie di possibili soluzioni anche quando egli più non abbia la possibilità di rintracciare la chiave o cifrario usato nel caso particolare e sia costretto a quella faticosissima operazione che si usa denominare *decrittazione*, cioè alla ricostruzione del cifrario stesso andato smarrito o per qualsiasi causa rimasto a lui sconosciuto.

In questi ultimi anni, poi, molto opportunamente l'Airaldi, analizzando un cifrario venuto a sua conoscenza[2], ha cercato di valutare le potenziali possibilità di ermeticità offerte dal sistema in esame dando, altresì, una precisa, dettagliata descrizione degli espedienti suggeriti,

---

[1] Cfr. L. Cerioni, *La diplomazia Sforzesca nella seconda metà del Quattrocento e i suoi cifrari segreti*, in *Fonti e Studi del Corpus Membranarum Italicarum*, vol. I e vol. II, Roma, 1970.

[2] G. Airaldi, *Paleografia e criptografia nella Storia genovese del Quattrocento*, in « Studi e documenti su Genova e l'Oltremare », Genova, 1974, pp. 111-152.

nel caso, dai corrispondenti per rendere più difficile la decrittazione.

Proprio per proseguire su questa via si crede opportuno portare a conoscenza degli studiosi i risultati dell'analisi di un cifrario, ricostruito in assenza di ogni elemento decifratore, perché si ritiene più interessante far constatare nel caso particolare come il sistema ed i vari espedienti tendenti a rendere più ermetico il documento siano stati praticamente sfruttati dallo scrivente che non limitare l'indagine soltanto alle soluzioni possibili in teoria. Ciò tanto più ricordando che, specialmente nel periodo indicato, dalla maggiore o minore abilità di colui che usava il cifrario dipendeva la possibilità di rendere più o meno difficile l'opera del decrittatore e si andava lentamente sperimentando ed innovando artifizi atti a perfezionare la « chiusura » dei testi cifrati.

Non solo, ma l'analisi di una decrittazione effettuata può indubbiamente fornire indicazioni molto utili in casi consimili, in cui sia necessario fare a meno di ogni sussidio decifratore; casi che, purtroppo, costituiscono la gran maggioranza tra quanti offerti dalla documentazione conservataci dal tempo.

Si è avuto occasione di osservare, in un precedente studio [3], come le diverse cancellerie italiane abbiano, negli ultimi secoli del Medioevo ed anche in quelli seguenti, preferito ad ogni altro sistema cifrante, per la corrispondenza diplomatica, quello monoalfabetico opportunamente rinforzato da espedienti diversi. E si è avuto altresì modo di constatare, col senno di poi, come tale scelta si dimostrasse tutt'altro che inopportuna e sprovveduta, soprattutto per ragioni pratiche e di applicazione, anche quando i progressi degli studi permisero ad eminenti matematici, quali il Della Porta, il De Vigenère, il Tritemio, di perfezionare quei sistemi teoricamente tanto più ermetici che vanno sotto il nome di sostituzione polialfabetica a chiave.

Si sa che la sostituzione monoalfabetica semplice, che si effettua sostituendo le unità del testo chiaro con segni, lettere o numeri tratti da un unico elenco cifrante, è un sistema poco resistente. Perché, conoscendo la frequenza, cioè il numero delle volte, con cui ogni lettera dell'alfabeto tende, a lungo andare, a presentarsi in ogni lingua, non

---

[3] G. Costamagna, *Tachigrafia notarile e scritture segrete medioevali in Italia*, in *Fonti e Studi del Corpus Membranarum Italicarum*, Roma, 1968, p. 44 e ss.

è difficile identificare subito le lettere più usate e di qui, per successivi confronti, passare all'individuazione di bigrammi e trigrammi e alla ricostruzione di tutti gli elementi del testo. Per questa ragione già alla fine del sec. XIV o all'inizio del seguente [4] si è pensato di prevedere l'uso di più segni, detti *omofoni*, per ogni lettera, da usarsi alternativamente, specie per le vocali, di non usare lettere doppie, troppo facilmente identificabili, e di inserire, qua e là, segni *nullius valoris*, atti soltanto a condurre fuori strada lo sprovveduto decrittatore. Al quale, inoltre, si presentava un crittogramma in scrittura scrupolosamente continua senza distinzione, cioè, tra parola e parola.

Anzi a partire da quell'epoca si usa aggiungere all'alfabeto cifrante un breve elenco, detto *repertorio*, di segni, parole o gruppi di lettere o di cifre particolari, corrispondenti a termini ripetutamente usati, quali, ad esempio, i nomi di persone, di principi e di località, che, troppo spesso ripetuti sfruttando il consueto cifrario avrebbero potuto facilitare la decrittazione.

A questo punto diventa evidente come con tale sistema l'ermeticità di un testo cifrato dipenda in gran parte da colui che provvede a trascrivere le lettere comuni in segni convenzionali e come soltanto attraverso una lenta, continua opera di perfezionamento sia possibile pervenire ai migliori risultati.

La lettera cifrata che si propone all'attenzione del lettore appartiene indubbiamente ad uno dei migliori periodi di attività, in questo campo, della Cancelleria milanese, che deve aver fornito a Spinetta Campofregoso « Ianuensium capitaneus et locumtenens », il cifrario per corrispondere con il Duca di Milano. Si tratta di una missiva in data 24 dicembre 1453, conservata nella serie Carteggi dell'Archivio di Stato di Milano [5].

Appartiene a quel ciclo di anni in cui forte doveva farsi sentire nell'ambiente l'influenza dell'abilità, quale teorico del sistema e sperimentatissimo decrittatore, di Cicco Simonetta. In mancanza di ogni elemento decifratore la decrittazione del testo cifrato ha richiesto note-

---

[4] Ivi, p. 43 e ss.

[5] Archivio di Stato di Milano, Fondo Ducale Visconteo Sforzesco, Carteggio, n. 315. Cfr. tav. allegata.

Si ringrazia vivamente la dott. A. Borlandi, dell'Istituto di Storia Economica dell'Università di Pavia, che con squisita cortesia ha segnalato l'esistenza della lettera cifrata.

voli tempo e fatica, ma soprattutto, ha posto in evidenza come le difficoltà siano dipese in massima parte non da particolari innovazioni del sistema, ma dall'efficacissimo uso degli espedienti a quell'epoca già conosciuti ed usati.

L'elenco cifrante che si è potuto ricostruire risulta essere, infatti, un comunissimo monoalfabetico con *omofoni*, dove questi ultimi, però, sono ancora segnati soltanto in corrispondenza delle vocali, mentre alla metà del sec. XV già comunemente si usano *omofoni* in corrispondenza di tutte le lettere dell'elenco cifrante. Doveva esistere anche, come si può constatare da pochi segni di cui non è stato possibile trascrivere le lettere comuni corrispondenti, un elenco di parole e di nomi *a repertorio*, del quale, tuttavia, non si può ricostruire l'esatta entità e la corrispondenza, data l'esiguità del testo in esame. Praticamente non usate le lettere *nullius valoris*, pur così utili per rendere più difficile la decrittazione, l'abilità del cifratore si rivela tutta nell'uso degli *omofoni* e nella capacità di dosare gli stessi in modo che nessun segno appalesi una preminenza consistente sugli altri e permetta l'individuazione delle lettere più usate. In effetti invece dei soliti 20 o 21 segni corrispondenti alle lettere dell'alfabeto il decrittatore si trova di fronte a oltre 40 segni, la frequenza in percentuale sul totale di ognuno dei quali non corrisponde a quella di alcuna lettera dell'alfabeto normale. Così, ad esempio, una delle più basse frequenze risulta assegnata ad un segno che a decrittazione effettuata corrisponde ad un omofono della vocale *o*, molto usata, mentre una sola unità supera la frequenza del 7 % in percentuale sul numero totale degli elementi quando la lettera *e* raggiunge di norma e oltrepassa il 13 %. Si assiste, cioè, ad un appiattimento delle frequenze che non permette alcuna operazione basata sulla valutazione delle stesse. In tali condizioni a chi si accinga alla decrittazione non resta che tentare delle ipotesi, rintracciare dei gruppi di segni uguali e supporre che corrispondano a parole che possano assumere un qualche senso nel testo. Ma si tratta di operazione lunga e difficile e che, oltre tutto, può portare a risultati sorprendenti e fuorvianti. Nel caso in questione, ad un certo momento, si è voluto ipotizzare che le ultime cinque lettere del testo cifrato corrispondessero alla parola « Doria », conosciutissimo cognome ricordato nella lettera stessa, vale a dire ad un gruppo con i segni corrispondenti alle vocali *a* e *o* rispettivamente in ultima e quart'ultima posizione. Passati alla sostituzione delle ricordate vo-

cali ai segni che si supponeva ad esse corrispondenti ci si dovette convincere che in certe occasioni l'operazione poteva dare l'impressione di essere risolutiva, ma che in altre risultava completamente inefficiente. La ragione stava nel fatto che occorreva pensare, invece, alla parola « resposta » che, vedi caso, segna le stesse vocali *a* e *o* nella identica successione e numerazione del nome « Doria », rispettivamente in ultima e quart'ultima posizione. Il che evidentemente poneva il decrittatore nella fortunata coincidenza di aver rintracciato il giusto valore dei segni corrispondenti alle vocali ricordate ma lo portava, d'altra parte, su di una pista sbagliata suggerendogli una corrispondenza alle lettere *d*, *r* ed *i* assolutamente errata.

Accanto all'ottimo uso degli omofoni occorre, inoltre, osservare come nel testo cifrato ci si valga con altrettanta bravura di altri espedienti, tali l'assenza completa di segni uguali susseguentisi, rivelanti lettere in coppia e l'interruzione delle parole a fine riga non effettuata per sillaba.

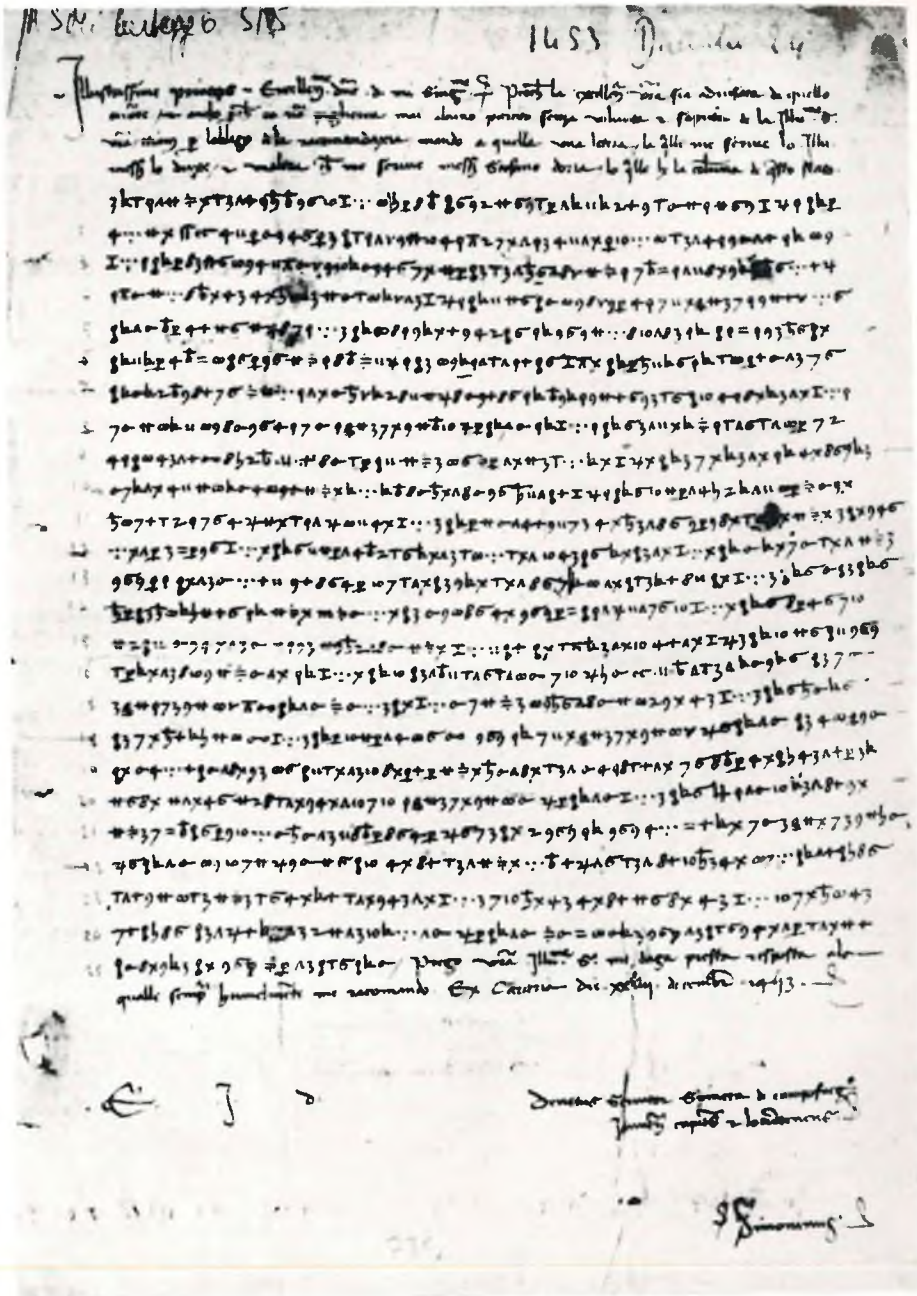
E' da ricordare, altresì, come risulti quanto mai efficace l'uso di segni convenzionali nel repertorio in luogo di parole intere, risultando spesso quest'ultime troppo trasparenti per i riflessi e le ricordanze che immancabilmente mantengono con il pensiero che le ha generate.

In conclusione, facendo tesoro delle esperienze compiute, si può affermare come alla metà del sec. XV, pur valendosi di sistemi strutturalmente semplici, si sapesse raggiungere un alto grado di sicurezza.

Trascrizione della parte cifrata della lettera

1) . . . Et perché per infino a qui io mi sono comportato in pace con questo
2) Duce . . . dagandoge sperarc(i)a de volere e dare Gavi per denari et in
3) questo meco andava adatando le cose per forma che liberamente io viv-
4) eva cum fede de fare capitare questa cosa in mano de la excelentia vo-
5) stra io dico cum le vestimente indoso et non cum arme et se bene fose

6) stato di bisogno che mi havese interpreiso questo fato et pi-
7) giare lo
stato in mi lo haverea fato ma cum anemo et intencione posa
8) de metere que-
la cità in mano de la excelencia vostra et questo era et he pro-
9) prio lo
desiderio mio . . . ma posa che io ho receputo queste letere et
10) de molte
altre da citadini che tuti m'afermano farsi questo acordio tra
11) Iohane
Filipo e lo Duce per via de questo cardinale de Fermo non
12) me p(ar) che esendo
vero e bono questo acordio potere più per adeso tesere questa
13) tela perché
non ge serea via ni modo al presente per molti respeti ma se
14) questo asesto
fose fiticio et che . . . havese animo de non observarlo a questo
15) modo la
cosa anderea bene in forma che quasi se poteria dire questa
16) mosa non
potere manchare et questa seria propria la via . . ., pertanto se la
17) excelencia vostra havese qualche informacione de questo fato
18) se l'è fiticio questo acordio o non et la excelencia vostra se
19) digna-
se advisarme saperea megio che farne per adempire lo mio
20) desiderio et
come credo comprender a la excelencia vostra questo verà a
21) termine
ch'el bisognava fare a mio modo volese o non et non dubite la
22) excelencia
vostra in alcuna cosa de mi perché vi iuro per mia fede ilu-
23) strisimo
principe che podete prendere quela fede de mi come de quale
24) fide-
lisimo servitore o creatura vostra habiate. Non responderò preci-
25) samente se non ho resposta



Archivio di Stato di Milano, Fondo Ducale Sforzesco, Carteggio n. 315