Interlingvistikaj Kajeroj

Saturno, Giove, Marte e Filippo: le quattro chiavi del Codice Bellaso

Saturno, Jupitero, Marto kaj Filippo: la kvar ŝlosiloj de la Kodo de Bellaso

Massimo Rizzardini

Tradukis Elena Marazzi

InKoj. Interlingvistikaj Kajeroj 1:2 (2010), 91–138 ISSN 2037-4550
http://riviste.unimi.it/index.php/inkoj/

ABSTRACT *Il vero modo di scrivere in cifra con facilità, prestezza et securezza* è un'operetta scritta e pubblicata nel 1564 da Giovan Battista Bellaso, sconosciuto diplomatico di origini bresciane. In poche pagine, l'autore esponeva i risultati delle sue ricerche in un ambito misterioso e sospettato: quello della crittografia. Divisi in quattro metodi e in numerose varianti, i sistemi polialfabetici spiegati nel manuale seguivano e miglioravano i "dischi cifranti" di Leon Battista Alberti (che con ogni probabilità Bellaso non conosceva), anticipavano la celebre tavola di Vigenère e guidavano il lettore meno esperto nel complicato mondo dei codici segreti. Quattrocento anni prima del codice Enigma di Arthur Scherbius.

RESUMO *Il vero modo di scrivere in cifra con facilità, prestezza et securezza* estas verketo skribita kaj eldona en 1564 de Giovan Battista Bellaso, nekonata diplomato brescia laŭ naskiĝo. En malmultaj paĝoj, la aŭtoro prezentas la rezultojn de la ĝiaj esploroj en mistera kaj suspekta kadro: la kriptografio. Disitaj en kvar metodoj kaj multaj variantoj, la polialfabetaj sistemoj klarigitaj en la manlibro sekvis kaj plibonigis la "ĉifrantajn diskojn" de Leon Battista Alberti (kiujn probable Bellaso ne sciis), anticipis la konan tabelon de Vigenère kaj gvidis la malpli ekspertan leganton tra la komplika mondo de la sekretaj kodoj. Kvarcent jarojn antaŭ Enigma codo de Arthur Scherbius.

InKoj. Interlingvistikaj Kajeroj 1:2 (2010), 91–138 ISSN 2037-4550
http://riviste.unimi.it/index.php/inkoj/

Introduzione/Enkonduko

Giovan Battista Bellaso, della cui vita non ci è dato di sapere quasi nulla[1], può essere considerato il pioniere della crittografia moderna[2], materia che dominò senza conoscere il *De componendis cyfris*[3] di Leon Battista Alberti e che seppe innovare prima dei più illustri colleghi Blaise de Vigenère[4] e Della Porta[5]. Bresciano di nascita e nobile di sangue, fu a Camerino per il cardinale Duranti e a Roma, nel 1549, a servizio del cardinale Pio da Carpi. Questo particolare, talora passato in secondo piano, acquista una luce diversa se si considera che i sistemi crittografici di sua invenzione furono verosimilmente utilizzati presso la curia pontificia, sensibile – come le cancellerie di mezza Europa - alla segretezza dei messaggi e delle relazioni. Affidò alle carte i suoi risultati a partire dall'anno 1553, con l'opera *La cifra del sig. Giouan Battista Bellaso, gentil'huomo bresciano nuouamente da lui medesimo ridotta a grandissima breuita & perfettione*, stampata a Venezia e dedicata al poligrafo Girolamo Ruscelli, ovvero colui che sotto le mentite spoglie del reverendo Donno Alessio Piemontese avrebbe pubblicato, due anni più tardi, il primo libro di *Secreti* a stampa e il primo bestseller della storia dell'editoria. Se sui legami con Ruscelli cala il silenzio storiografico (complice, probabilmente, il silenzio delle fonti), sappiamo che il 1555 è anche l'anno del suo secondo volume, *Noui et singolari modi di cifrare de l'eccellente dottore di legge messer Giouan Battista Bellaso nobile bresciano, con le sue regole & essempi con somma & chiara breuita composti*. Mandati alle stampe da Lodovico Britannico cinque giorni prima di Natale, introducevano il *contrasegno* ovvero frase convenzionale e il "segno nullo", rappresentato in questo caso dalla *y*. Gli esperti crittografi e gli agenti al servizio dei governi dovettero attendere il 1564 per conoscere la *summa* dei suoi studi, che infine apparvero ne *Il vero modo di scrivere in cifra con facilita, prestezza et securezza*, di nuovo per i tipi di Britannico (ma nella persona di Giacomo) e dedicata al cardina-

Giovan Battista Bellaso, pri kies vivo ni kvazaŭ nenion scias[6], povas esti konsiderata la pioniro de la moderna kriptografio[7], temo kiun li mastris sen koni la *De componendis cyfris*[8] de Leon Battista Alberti, kaj kiun li novigis antaŭ la pli eminentaj kolegoj Blaise de Vigenre[9] kaj Della Porta[10]. Brescia laŭ naskiĝo, li estis en Camerino por la kardinalo Duranti, kaj en 1549 en Romo deĵoris por la kardinalo Pio da Carpi. Ĉi tiu detalo, kelkfoje duarange, akiras novan lumon se oni konsideras ke la kriptografiaj sistemoj de lia invento probable estis uzitaj ĉe la pontifika kurio, sentema pri sekreteco de mesaĝoj kaj rilatoj - kiel kancelarioj de duona Eŭropo. Ekde 1553 li konfidis siajn rezultojn al paperoj, per la verko *La cifra del sig. Giouan Battista Bellaso, gentil'huomo bresciano nuouamente da lui medesimo ridotta a grandissima breuita & perfettione*, presita en Venecio kaj dediĉita al hektografisto Girolamo Ruscelli, tiu, kiu sub falsa vesto de la reverendo Donno Alessio Piemontese eldonis, post du jaroj, la unuan libron de *Secreti* kaj la unuan furorlibron de la eldonarto. Se pri la ligoj kun Ruscelli la historiografia interezo malaltiĝis, ni scias ke en 1555 li eldonis la duan volumon, *Noui et singolari modi di cifrare de l'eccellente dottore di legge messer Giouan Battista Bellaso nobile bresciano, con le sue regole & essempi con somma & chiara breuita composti*. Sendita al la presado de Ludovico Britannico kvinajn tagojn antaŭ Kristnasko, ĝi enkondukis la *contrasegno*, tio estas la konvencia frazo, kaj la "senrezulta" signo, en tiu kazo simbolita de la *y*. La ekspertaj kriptografoj kaj la oficistoj, kiuj deĵoris por la regadoj, devis atendi 1564 jaron por scii la *summa* de liaj studoj, kiuj finfine aperis en *Il vero modo di scrivere in cifra con facilita, prestezza et securezza*, ancoraŭ por la tipoj de Britannico (sed en la persono de Giacomo), kaj dediĉita al la kardinalo Alessandro Farnese. La malgranda volumo komenciĝis kun la dek tri *singolar qualità delle cifre* (specialaj kvalitoj de la ciferoj) kaj poste ilustris kvar polialfabetaj

le Alessandro Farnese. Il volumetto si apriva con le tredici *singolar qualità delle cifre* e passava a illustrare quattro sistemi polialfabetici di cifratura: analizziamoli uno per uno.

sistemoj de ĉifrado: ni analizas unuope.

I.

Il primo sistema di cifratura proposto da Bellaso è un sistema polialfabetico con parola chiave (*dittione* SATURNO) che si dispone *a questo modo*:

La unua sistemo de ĉifrado proponita de Bellaso estas polialfabita sistemo kun ŝlosilvorto (*dittione* SATURNO), kiu pretiĝas ĉi tiel:

S	A	B	C	D	E	F	G	H	I
T	U	R	N	O	L	M	P	Q	X

. Le 10 lettere della prima riga restano immutate, mentre le 10 sottostanti "ruotano" fino a generare 10 alfabeti diversi, così che per ogni lettera esistono 10 diverse corrispondenze:

. La dek literoj en la unua linio restas neŝanĝitaj, dum la dek substarantaj literoj "turniĝas" ĝis generi dek malsamaj alfabetoj, tiel ke ĉiuj literoj havas po dek malsamaj respondoj:

1	S	A	B	C	D	E	F	G	H	I
	T	U	R	N	O	L	M	P	Q	X

2	S	A	B	C	D	E	F	G	H	I
	X	T	U	R	N	O	L	M	P	Q

3	S	A	B	C	D	E	F	G	H	I
	Q	X	T	U	R	N	O	L	M	P

4	S	A	B	C	D	E	F	G	H	I
	P	Q	X	T	U	R	N	O	L	M

5	S	A	B	C	D	E	F	G	H	I
	M	P	Q	X	T	U	R	N	O	L

6	S	A	B	C	D	E	F	G	H	I
	L	M	P	Q	X	T	U	R	N	O

7	S	A	B	C	D	E	F	G	H	I
	O	L	M	P	Q	X	T	U	R	N

8	S	A	B	C	D	E	F	G	H	I
	N	O	L	M	P	Q	X	T	U	R

9	S	A	B	C	D	E	F	G	H	I
	R	N	O	L	M	P	Q	X	T	U

10	S	A	B	C	D	E	F	G	H	I
	U	R	N	O	L	M	P	Q	X	T

. Come si evince in modo intuitivo guardando lo schema alfabetico, le corrispondenze fra le lettere sono da leggersi dall'alto verso il basso e viceversa. Per esempio, nell'alfabeto numero 10, la S sarà cifrata come U e la U come S. La formazione dei 10 diversi alfabeti può essere pensata come un sistema di due ruote concentriche: quella esterna, fissa, corrisponde alla prima riga; quella interna, mobile, si sposta segno per segno, come si può vedere mettendo in evidenza il "percorso" della T, che nel primo alfabeto occupa la prima posizione della seconda riga e nel decimo l'ultima (le lettere che seguono, scalano a loro volta, per cui la X, che nel primo alfabeto occupa l'ultima posizione, dal secondo alfabeto "ricomincia", per così dire, dalla prima) :

. Kiel oni intuicie deduktas rigardante la alfabetan skemo, la respondoj de la literoj devas estis legitaj al supre suben kaj inverse. Ekzemple, an la deka alfabeto, la S estos ĉifrita kiel U, kaj la U kiel S. La formado de la dek malsamaj alfabetoj povas esti pensita kiel sistemo de du samcentraj radoj: la ekstera, fiksa rado kongruas la unuan linion, la interna, movebla rado moviĝas ĉiusigne, kiel oni povas vidi evidentigante la "vojon" de la litero T, kiu en la unua alfabeto okupas la unuan pozicion de la dua linio, kaj en la deka alfabeto okupas la lastan pozicion (la sekvantaj literoj postvenas laŭgrade, tiel ke la X, kiu en la unua alfabeto okupas la lastan pozicion, ekde la dua alfabeto "rekomencas", por tiel diri, de la unua pozicio):

1	S	A	B	C	D	E	F	G	H	I
	T	U	R	N	O	L	M	P	Q	X

2	S	A	B	C	D	E	F	G	H	I
	X	**T**	U	R	N	O	L	M	P	Q

3	S	A	B	C	D	E	F	G	H	I
	Q	X	**T**	U	R	N	O	L	M	P

4	S	A	B	C	D	E	F	G	H	I
	P	Q	X	**T**	U	R	N	O	L	M

5	S	A	B	C	D	E	F	G	H	I
	M	P	Q	X	**T**	U	R	N	O	L

6	S	A	B	C	D	E	F	G	H	I
	L	M	P	Q	X	**T**	U	R	N	O

7	S	A	B	C	D	E	F	G	H	I
	O	L	M	P	Q	X	**T**	U	R	N

8	S	A	B	C	D	E	F	G	H	I
	N	O	L	M	P	Q	X	**T**	U	R

9	S	A	B	C	D	E	F	G	H	I
	R	N	O	L	M	P	Q	X	**T**	U

10	S	A	B	C	D	E	F	G	H	I
	U	R	N	O	L	M	P	Q	X	**T**

. Il ruolo della X, (*et quando occorresse descriverla per lettera, se farà*

. La rolo de la X (*et quando occorresse descriverla per lettera, se far un*

un ponto sopra la lettera, che significarà la x) è assimilabile all'odierna barra spaziatrice. Se il messaggio da cifrare, scrive Bellaso, è il seguente:

ponto sopra la lettera, che significarà la x) estas simila al la hodiaŭa spacoklavo. Se, Bellaso skribas, la mesaĝo ĉifrenda estas la sekvanta:

IN OGNI ARTE INOGNI SCIENTIA LAINVENTIONE FUSEMPRE LAPIU BELLA PARTE CHESIA

andrà prima di tutto trasformato in questo modo:

ĝi estas unue transformita tiel:

INXOGNIXARTEXINOGNIXSCIENTIAXLAINVENTIONEXFUSEMPREXLAPIUXBELLAXPARTEXCHESIAX

. A questo punto, sopra ogni parola (*dittione*) si scrive il numero progressivo: IN(X) corrisponde a 1

OGNI(X) corrisponde a 2
ARTE(X) corrisponde a 3
...
CHESIA(X) corrisponde a 11, quindi a 1

. L'importanza del progressivo è presto detta: a ogni *dittione* corrisponde un diverso alfabeto, tale che – per dirla à la Bellaso – *con il primo alfabeto tu cifri inx, mettendo una lettera per l'altra, cioè, quelle di sopra per quelle di sotto, et quelle di sotto per quelle di sopra; con il secondo alfabeto, tu cifri ognix, con il terzo alfabeto, tu cifri artex, con il quarto alfabeto, tu cifri inognix [...] Et cifrate diece dittioni, tu ritorni da capo sempre cifrando una dittione con la x, per alfabeto* [...]. Tabella alfabetica alla mano, il risultato finale del sistema di Bellaso sarà questo:

. Kaj post tio, oni skribas super ĉiuj vortoj (*dittione*) la sinsekvan numeron: IN(X) kongruas al 1

OGNI(X) kongruas al 2
ARTE(X) kongruas al 3
...
CHESIA(X) kongruas al 11, tio estas al 1

. La graveco de la sinsekvo estas ĉi tiu: al ĉiu *dittione* kongruas malsaman alfabeton, tiel - laŭ Bellaso - *con il primo alfabeto tu cifri inx, mettendo una lettera per l'altra, cioè, quelle di sopra per quelle di sotto, et quelle di sotto per quelle di sopra; con il secondo alfabeto, tu cifri ognix, con il terzo alfabeto, tu cifri artex, con il quarto alfabeto, tu cifri inognix* [...] *Et cifrate diece dittioni, tu ritorni da capo sempre cifrando una dittione con la x, per alfabeto* [...]. Se oni rigardas rekte la alfabetan tabelon, la lasta rezulto de la sistemo de Bellaso estas ĉi tiu:

XCIEMDQSXDBNAMFGOFMBMLUGDLPCSMOHFTHEOIHTDTGOXBCHXEBODRHFOPCNGFRAIMHTXUI

. Seguiamo passo passo le operazioni. Sappiamo dall'esempio sopracitato che la prima parola della frase cifrata è IN, cui seguirà la X della barra spaziatrice. Le prime tre cifre sono dunque XCI, che dalla tabella del primo alfabeto sappiamo corrispondere a I (X), N (C), X (I). Passiamo alla seconda parola o dittione, OGNI, connotata dal numero progressivo 2 (corrispondente al secondo alfabeto) e composta di quattro cifre più la X della barra spaziatrice, per un totale di 5. Dalla tavola del secondo alfabeto, si può vedere che le cifre EMDQS corrispondono a O (E), G (M), N (D), I (Q), X (S): OGNIX, esattamente come la seconda parola della frase cifrata. E così via, non senza notare, tuttavia, che il codice di Bellaso cifra SIENTIA(X) in luogo di SCIENTIA(X), BELA(X) in luogo di BELLA(X) e SIA(X) in luogo di CHESIA(X)[11]. Ecco qui di seguito la tavola completa:

1	X	C	I
	I	N	X

2	E	M	D	Q	S
	O	G	N	I	X

3	X	D	B	N	A
	A	R	T	E	X

4	M	F	G	O	F	M	B
	I	N	O	G	N	I	X

5	M	L	U	G	D	L	P	C
	S	I	E	N	T	I	A	X

. Ni sekvas la operaciojn paŝon post paŝo. Per la surmenciita ekzemplo ni scias ke la unua vorto de la menciita frazo estas IN, al kiu sekvos la X de la spacoklavo. La unuaj tri ĉifroj estas do XCI, kiujn ekde la unuealfabeta tabelo oni scias ke ili kongruas al I (X), N (C), X (I). Ni transiras al la dua vorto aŭ *dittione*, OGNI, indikita per la sinsekva numero 2 (kiu kongruas al la dua alfabeto), kaj komponita el kvar ĉifroj plus la X de la spacoklavo, entute kvin ĉifroj. Per la tabelo de la dua alfabeto oni povas vidi ke la ĉifroj EMDQS kongruas al O (E), G (M), N (D), I (Q), X (S): OGNIX, ekzakte kiel la dua vorto de la ĉifrita frazo. Kaj tiel plu, tamen ne sen noti ke la kodo de Bellaso ĉifras SIENTIA(X) antastaŭ SCIENTIA(X), BELA(X) anstataŭ BELLA(X) kaj SIA(X) anstataŭ CHESIA(X)[12]. Jen ĉi tie la kompleta tabelo:

6	S	M	O	H	F	T	H	E	O	I	H	T	D
	L	A	I	N	V	E	N	T	I	O	N	E	X

7	T	G	O	X	B	C	H	X	E
	F	U	S	E	M	P	R	E	X

8	B	O	D	R	H	F
	L	A	P	I	U	X

9	O	P	C	N	G
	B	E	L	A	X

10	F	R	A	I	M	H
	P	A	R	T	E	X

1	T	X	U	I
	S	I	A	X

. Se disponiamo per il lungo la striscia cifrata, comprensiva degli spazi indicati dalla cifratura della X, si otterrà dunque

. Se ni aranĝas laŭlonge la ĉifritan strion, inkluzive la lokojn indikitajn de la ĉifrado de la X, do oni akiras:

XCI EMDQS XDBNA MFGOFMB MLUGDLPC SMOHFTHEOIHTD TGOXBCHXE BODRHF OPCNG FRAIMH TXUI

, ossia una striscia scomponibile in 11 dittioni e in 71 caratteri.

, tio estas strio disigebla laŭ 11 *dittioni* kaj 71 literoj.

II.

Il secondo sistema, che come si vedrà mette a disposizione tre diversi metodi di cifratura, si forma con la *dittione* IOVE, disposta come segue:

La dua sistemo, kiu, kiel oni vidos, disponigas tri malsamajn metodojn de ĉifrado, formiĝas kun la *dittione* IOVE, lokita ĉi tiel:

I	O	A	B	C	D	F	G	H	L
V	E	M	N	P	Q	R	S	T	X

. Rispetto alla tavola del primo metodo, che generava a partire dalla parola chiave 10 alfabeti diversi, in questo secondo metodo Bellaso mostrava la possibilità di criptare un messaggio con una tavola di 5 alfabeti, contrassegnati, in luogo del numero progressivo, da 5 combinazioni di 4 lettere ciascuna:

. Kompare al la tabelo de la unua metodo, kiu generis dek malsamajn alfabetojn ekde la ŝlosilvorto, en ĉi tiu dua metodo Bellaso elmontris la eblon ĉifri mesaĝon per tabelo el kvin alfabetoj, markitaj per 5 kombinoj, po 4 literoj, antastaŭ la sinsekva numero:

IDVQ	I	O	A	B	C	D	F	G	H	L
	V	E	M	N	P	Q	R	S	T	X

OFER	I	O	A	B	C	D	F	G	H	L
	X	V	E	M	N	P	Q	R	S	T

AGMS	I	O	A	B	C	D	F	G	H	L
	T	X	V	E	M	N	P	Q	R	S

BHNT	I	O	A	B	C	D	F	G	H	L
	S	T	X	V	E	M	N	P	Q	R

CLPX	I	O	A	B	C	D	F	G	H	L
	R	S	T	X	V	E	M	N	P	Q

. Se IOVE è la parola chiave del sistema, si può dire che il numero chiave sia invece il 5. Cinque sono infatti gli alfabeti e 5, secondo uno schema modellato sul primo metodo, sono gli spostamenti compiuti dalla lettera V che, come raffigurato nella tavola sottostante, nel primo alfabeto occupa la prima posizione e nell'ultimo, appunto, la quinta:

. Se IOVE estas la ŝlosilvorton de la sistemo, oni povas diri ke la ŝlosilnumero estas male 5. Kvin estas fakte la alfabetoj kaj, konforme al skemo modelita laŭ la unua metodo, kvin estas la movoj faritaj de la litero V, kiu, kiel prezentita en la suba tabelo, okupas en la unua alfabeto la unuan pozicion kaj, en la lasta alfabeto, precize, la kvinan:

IDVQ	I	O	A	B	C	D	F	G	H	L
	V	E	M	N	P	Q	R	S	T	X

OFER	I	O	A	B	C	D	F	G	H	L
	X	**V**	E	M	N	P	Q	R	S	T

AGMS	I	O	A	B	C	D	F	G	H	L
	T	X	**V**	E	M	N	P	Q	R	S

BHNT	I	O	A	B	C	D	F	G	H	L
	S	T	X	**V**	E	M	N	P	Q	R

CLPX	I	O	A	B	C	D	F	G	H	L
	R	S	T	X	**V**	E	M	N	P	Q

. Allo stesso modo, all'osservatore più attento non sarà sfuggito che le 5 combinazioni di 4 lettere poste - in luogo del numero progressivo – a identificazione dei 5 alfabeti, sono formate a partire dalle prime due lettere del primo alfabeto (la I e la V della parola chiave IOVE) e su ciascuna delle due righe dalla quinta successiva (la D e la Q). La tavola qui di seguito illustra, in modo esemplificativo, la disposizione delle tabelle alfabetiche pensate da Bellaso:

. Sammaniere, la pli skrupola observanto ne preteratentas ke la 5 kombinoj de 4 literoj, lokitaj pro identigi la 5 alfabetojn anstataŭ la sinsekva numero, estas komponitaj ekde la unuaj du literoj de la unua alfabeto (la I kaj la V de la ŝlosilvorto IOVE), kaj el ĉiuj du linioj ekde la kvina sekvanta (la D kaj la Q). La posta tabelo ilustras, kiel ekzemple, la aranĝon de la alfabetaj tabeloj pripensitaj de Bellaso:

IDVQ	**I**	O	A	B	C	**D**	F	G	H	L
	V	E	M	N	P	**Q**	R	S	T	X

OFER	I	**O**	A	B	C	D	**F**	G	H	L
	X	V	**E**	M	N	P	Q	**R**	S	T

AGMS	I	O	**A**	B	C	D	F	**G**	H	L
	T	X	V	E	**M**	N	P	Q	R	**S**

BHNT	I	O	A	**B**	C	D	F	G	**H**	L
	S	**T**	X	V	E	M	**N**	P	Q	R

CLPX	I	O	A	B	**C**	D	F	G	H	**L**
	R	S	T	**X**	V	E	M	N	**P**	Q

. Se si osserva la posizione – evidenziata in rosso – delle lettere che compongono le combinazioni che identificano gli alfabeti, si può vedere che queste sono generate dalla successione delle prime lettere I, D, V, Q, del primo alfabeto, e secondo il medesimo intervallo di 5 posizioni. Infatti, nel secondo alfabeto la combinazione è data dalle successive O, F, E, R, e così via, sino all'ultima C, L, P, X, dove la P è prima della X perché secondo la consueta immagine della ruota, dobbiamo pensare che la X sia "ruotata" dietro la P, che nella seconda riga del primo alfabeto, difatti, la precede.

. Se oni observas la pozicion - markitan ruĝe - de la literoj kiuj komponas la kombinojn, kiuj identigas la alfabetojn, oni povas vidi ke ĉi tiuj estas kaŭzitaj pro la sinsekvo de la unuaj literoj I, D, V, Q de la unua alfabeto, kaj laŭ la sama intervalo 5-pozicia. Fakte en la dua alfabeto la kombino estas komponita el la sekvantaj literoj O, F, E, R, kaj tiel plu, ĝis la lasta C, L, P, X, kie la P estas antaŭa al la X ĉar, laŭ la kutima imago de la rado, ni devas pensi ke la X turniĝas post la P, kiu en la dua linio de la unua alfabeto estas fakte antaŭa.

IIa.

Così Bellaso spiega la prima variante del secondo metodo di cifratura: *il primo modo è questo: tu pigli un versetto volgare ò latino, ò in altra lingua, et la minuta, tu la fai a questo modo attaccando le dittion picciole alle maggiore.* L'esempio serve a chiarire meglio le idee. Immaginiamo che il messaggio da cifrare sia il seguente:

Tiel Bellaso klarigas la unuan varianton de la dua metodo de ĉifrado: *il primo modo è questo: tu pigli un versetto volgare ò latino, ò in altra lingua, et la minuta, tu la fai a questo modo attaccando le dittion picciole alle maggiore*. La ekzemplo utilas klarigi la ideojn. Ni imagas ke la mesaĝo ĉifrenda estas la sekvanta:

LA VIRTÙ FU SEMPRE DA MALIGNI INVIDIATA

Ora, seguendo le regole di Bellaso, per prima cosa accorpiamo le *picciole dittioni* alle parole più lunghe, così come lui stesso ci mostra:

Nun, laŭ la reguloj de Bellaso, antaŭe ni parigas la *picciole dittioni* (etaj vortoj) al la pli longaj vortoj, kiel li elmontras nin:

LAVIRTÙ FUSEMPRE DAMALIGNI INVIDIATA

. Fatto ciò, scegliamo quale versetto chiave utilizzare per la cifratura del messaggio. Bellaso suggerisce:

. Poste, oni elektas kiun verseton oni uzas por ĉifri la mesaĝon. Bellaso sugestas:

OPTARE MELIORA FERRE OMINIA

. Il versetto sarà, in un certo senso, il nostro contatore e i suoi caratteri serviranno a identificare, in luogo dei numeri, le singole parole (unificate le minori con le maggiori) che compongono la frase. Dal momento che il messaggio da cifrare è composto di sole 4 unità, i primi 4 caratteri del versetto (OPTA) saranno associati alle singole parole, in questo modo:

. La verseto estas iasence la mezurilon, kaj siaj literoj servas identigi, anstataŭ numerojn, la unuopajn vortojn (la pli grandaj vortoj unuiĝinte kun la pli malgrandaj), kiuj komponas la frazon. Tial ke la mesaĝo ĉifrenda estas komponita el nur kvar unuoj, la unuaj kvar literoj de la verseto (OPTA) estas asociitaj al la unuopaj vortoj, ĉi tiel:

O	P	T	A
LAVIRT	FUSEMPRE	DAMALIGNI	INVIDIATA

. Qualora la frase fosse composta di molte parole “riunite”, superiori ai caratteri alfabetici del versetto, si procederà ricominciando dalla prima lettera del medesimo, esattamente come nei 10 alfabeti del primo metodo si ricominciava dal numero 1. Dal versetto dipende la possibilità di cifrare o decrittare il messaggio - pena l’inevitabile

. En la kazo ke la frazo estas komponita el multaj ”kunigita” vortoj, kiuj superas la alfabetajn literojn de la verseto, oni pluiras rekomencante ekde la unua literoj de la samo, ekzakte kiel, en la dek alfabetoj de la unua metodo, oni rekomencis ekde la numero 1. De la verseto dependas la eblo ĉifri aŭ deĉifri la mesaĝon - alikaze neevitebla

fallimento – poiché le lettere poste sopra la parola identificano, a loro volta, quale alfabeto utilizzare per primo. Torniamo all'esempio sopracitato: sappiamo che la prima parola riunita LAVIRTÙ è contrassegnata da una O. Questo significa che si comincerà dal secondo alfabeto, vale a dire da quello identificato dalla combinazione OFER, nella quale è appunto presente la lettera O, e che la lettera L di LAVIRTÙ dovrà essere cifrata, tabella alla mano, con la lettera T. Ora si procederà passando all'alfabeto successivo, ossia il terzo. La seconda lettera essendo una A, dalla tabella del terzo alfabeto si può vedere che essa va cifrata con una U e così via fino al quinto e poi di nuovo dal primo. È lo stesso Bellaso a darci la soluzione (corretta):

malsukceso - ĉar la literoj lokitaj sur la vortoj identigas siavice kiun alfabeton utiligi kiel la unua. Oni revenas al la ekzemplo surmenciita: oni scias ke la unua kunigita vorto LAVIRTÙ estas markita per O. Ĉi tiu signifas ke oni devas komenci ekde la dua alfabeto, alivorte ĉi tiu identigita per la kombino OFER, en kiu prezise estas la litero O, kaj ke la litero L de LAVIRTÙ devos esti ĉifrata, kun la tabelo en la mano, per la litero T. Nun oni pluiras pasante al la sekvanta alfabeto, tio estas la tria. Ĉar la dua litero estas A, laŭ la tabelo de la tria alfabeto oni povas vidi ke ĝi devas esti ĉifrita kiel U, kaj tiel plu ĝis la kvina alfabeto kaj de nove ekde la unua. Estas Bellaso mem kiu donas al ni la (ĝustan) solvon:

TUBRFLA MIHBDHFA MTAESSNBX TFCUPTXAM

, dove la prima lettera T del primo codice (TUBRFLA) è la lettera L cifrata con il secondo alfabeto (OFER), la prima lettera M del secondo codice (MIHBDHFA) è la F cifrata con il quinto alfabeto (CLPX), la prima lettera M del terzo codice (MTAESSNBX) è la D cifrata con il quarto alfabeto (BHNT) e la prima lettera T del quarto codice (TFCUPTXAM) è la I cifrata con il terzo alfabeto (AGMS).

, kie la unua litero T de la unua kodo (TUBRFLA) estas la litero L ĉifrita per la dua alfabeto (OFER), la unua litero M de la dua kodo (MIHBDHFA) estas la F ĉifrita per la kvina alfabeto (CLPX), la unua litero M de la tria kodo (MTAESSNBX) estas la D ĉifrita per la kvara alfabeto (BHNT), kaj la unua litero T de la kvara kodo (TFCUPTXAM) estas la I ĉifrita per la tria alfabeto (AGMS).

IIb.

La seconda variante del secondo metodo di Bellaso differisce dalla prima perché *in questo si mette una lettera maiuscola nel principio d'ogni dittione, pigliandole confusamente dal detto alfabeto de maiuscole, le qual lettere fanno quello medemo effetto che fanno le lettere del versetto, te insegnano andare à ritrovare la lettera allo alfabeto de maiuscole, et andare*

La dua varianto de la dua metodo de Bellaso diferencas de la unua ĉar *in questo si mette una lettera maiuscola nel principio d'ogni dittione, pigliandole confusamente dal detto alfabeto de maiuscole, le qual lettere fanno quello medemo effetto che fanno le lettere del versetto, te insegnano andare à ritrovare la lettera allo alfabeto de maiuscole, et andare al suo al-*

*al suo alfabeto picciolo à cominciare à cifrar la dittione, che seguita, con la quale sta attaccata la detta lettera [...]*Se l'autore pecca di chiarezza, ma non di metodo, è bene ripartire dalla tavola alfabetica utilizzata nella prima variante:

fabeto picciolo à cominciare à cifrar la dittione, che seguita, con la quale sta attaccata la detta lettera [...]. Se la aŭtoro kulpas pro malklareco, sed ne pri metodo, estis bone rekomenci ekde la alfabeta tabulo uzita en la unua varianto:

IDVQ	I	O	A	B	C	D	F	G	H	L
	V	E	M	N	P	Q	R	S	T	X

OFER	I	O	A	B	C	D	F	G	H	L
	X	V	E	M	N	P	Q	R	S	T

AGMS	I	O	A	B	C	D	F	G	H	L
	T	X	V	E	M	N	P	Q	R	S

BHNT	I	O	A	B	C	D	F	G	H	L
	S	T	X	V	E	M	N	P	Q	R

CLPX	I	O	A	B	C	D	F	G	H	L
	R	S	T	X	V	E	M	N	P	Q

. A partire dall'esempio dell'autore, immaginiamo di dover cifrare questo messaggio:

. Laŭ la ekzemplo de la aŭtoro, oni imagas la devon ĉi tiu mesaĝon traduki:

virtuti omnia parent

. Dal momento che in questa variante non è previsto il ricorso a un versetto, all'inizio di ogni parola sarà bene apporre una lettera maiuscola, che a sua volta rimanderà a una delle 4 lettere delle 5 combinazioni (IDVQ, OFER, AGMS, BHNT, CLPX) che identificano

. Konsiderinte ke en ĉi tiu varianto la sinturno al verseto estas neantaŭvidita, ĉe la komenco de ĉiu vorto estos bone poni ĉefliteron, kiu siavice resendos al unu el la kvar literoj de la kvin kombinoj (IDVQ, OFER, AGMS, BHNT, CLPX), kiuj identigas la respondajn

i 5 corrispondenti alfabeti. Per prima cosa, dunque, si apporranno queste iniziali maiuscole alle parole del messaggio in chiaro:

kvin alfabetojn. Unue, do oni metas ĉi tiujn ĉefliterojn al la vortoj de la komenca mesaĝo ankoraŭ ĉifrenda:

Mvirtuti Lomnia Fparent

. Il passaggio, come si può vedere, è molto più rapido del versetto della prima variante. La soluzione sarà dunque:

. La transigo, kiel oni vidas, estas pli multe rapida ol la verseto de la unua varianto. La solvo estas do:

Masihois Lsactx Fduldbl

. Riassumendo, vediamo "in chiaro" come è stato criptato il messaggio di Bellaso. Dall'iniziale maiuscola M della prima *dittione* Masihois sappiamo che il nostro sguardo deve correre al terzo alfabeto, contrassegnato dal codice AGMS. Infatti, la a di Masihois sta per v. A questo punto, la seconda lettera di Masihois, cioè la s, sarà la cifra della lettera i, come appunto risulta dal quarto alfabeto, successivo a quello da cui siamo partiti con la decrittazione. Come nel caso della prima variante con versetto, dopo aver identificato qual è il primo alfabeto dei 5 possibili da cui cominciare la decrittazione, si procede col successivo fino alla parola seguente, contrassegnata con un'altra maiuscola e quindi con un altro alfabeto dal quale ricominciare la decrittazione. Se, per esempio, l'alfabeto dal quale cominciare è il quarto, si passerà al quinto e poi al primo, al secondo e così via. Lo stesso procedimento sarà seguito per la seconda *dittione*, Lsactx, la cui iniziale maiuscola L ci riporta al quinto alfabeto, contrassegnato dal codice CLPX. La prima lettera s, infatti, è la cifra che sta per o, prima lettera della seconda parola da decrittare, *omnia*. Ancora una volta il codice proposto da Bellaso si è rivelato esatto e in piena corrispondenza con la frase in chiaro *virtuti omnia*

. Resumante, ni klarigas kiel la mesaĝo de Bellaso estis ĉifrita. Ekde la ĉeflitero M de la unua *dittione* Masihois ni scias ke nia rigardo devas iri al la tria alfabeto, markita per la kodo AGMS. Fakte, la *a* de Masihois estas anstataŭas la *v*-n. Nun, la dua litero de Masihois, la *s*, estos la ĉifro de la litero *i*, kiel rezultas laŭ la kvar alfabeto sekvanta al tiu ekde kiu oni ekiris deĉifradi. Kiel en la kazo de la unua varianto kun verseto, poste oni identigis kiun alfabeton inter la eblaj kvinoj estas la unua ekde kiu komenci la deĉifradon, oni pluiras kun la sekvanta alfabeto ĝis la posta vorto, markita per alia ĉeflitero, kaj do kun alia alfabeto, laŭ kiu rekomencas la deĉifrado. Ekzemple, se la komenca alfabeto estas la kvara, oni transiras al la kvina kaj do al la unua, al la dua kaj tiel plu. La sama procedo estu sekvata per la dua *dittione*, Lsactx, kies la ĉeflitero L reportas al la kvina alfabeto, markita per la kodo CLPX. La unua litero *s*, estas fakte la ĉifro de la litero *o*, la unua litero de la dua vorto por deĉifri, *omnia*. Ankoraŭfoje, la kodo proponita de Bellaso estas ĝusta kaj en plena respondo kun la frazo *virtuti omnia parent*. Kaj, konklude per sia vortoj, *con questo modo de cifrare, se puo cifrare acomodamente senza fare la minuta*.

parent. E per concludere con le sue parole, *con questo modo de cifrare, se puo cifrare acomodamente senza fare la minuta*.

IIc

Introducendo la terza variante, che consente di poter cifrare un messaggio senza ricorrere né al versetto né alle iniziali maiuscole, Bellaso spiega che *la prima dittione tu la comintij sempre a cifrar al primo alfabeto, cifrando una lettera per alfabeto al modo detto, et la prima lettera d'ogni dittione de la minuta, te insegna andare all'alfabeto de maiuscole, et al suo alfabeto picciolo a cominciar à cifrare la dittione che segue.* Ripartiamo, ancora una volta, dalla consueta tavola alfabetica del secondo metodo:

Prezentante la trian varianton, kiu permesas ĉifri mesaĝon sen verseto nek ĉefliteroj, Bellaso klarigas ke *la prima dittione tu la comintij sempre a cifrar al primo alfabeto, cifrando una lettera per alfabeto al modo detto, et la prima lettera d'ogni dittione de la minuta, te insegna andare all'alfabeto de maiuscole, et al suo alfabeto picciolo a cominciar à cifrare la dittione che segue*. Ni rekomencas ankoraŭfoje ekde la kutima alfabeta tabelo de la dua metodo:

IDVQ	I	O	A	B	C	D	F	G	H	L
	V	E	M	N	P	Q	R	S	T	X

OFER	I	O	A	B	C	D	F	G	H	L
	X	V	E	M	N	P	Q	R	S	T

AGMS	I	O	A	B	C	D	F	G	H	L
	T	X	V	E	M	N	P	Q	R	S

BHNT	I	O	A	B	C	D	F	G	H	L
	S	T	X	V	E	M	N	P	Q	R

CLPX	I	O	A	B	C	D	F	G	H	L
	R	S	T	X	V	E	M	N	P	Q

. L'esempio che Bellaso ci propone di cifrare,

. La ekzemplo kiun Bellaso proponas ĉifri,

ave maria gratia plena

, e che dà come soluzione il codice

, kaj kiu donas kiel solvo la kodon

mob cxie qlthxu frdbe

, come si può vedere, ha in sé le regole della propria cifratura. Partendo sempre come regola dal primo alfabeto e procedendo con quello successivo, si cifra la prima parola ave e si arriva, con la e, al terzo alfabeto. Passando alla parola successiva, *maria*, non si continua dal quarto alfabeto, ma si riparte dal terzo, poiché la prima lettera della parola precedente "in chiaro", la *a* di *ave*, è l'indizio (e quindi la regola da osservare strettamente, pena l'inefficacia della cifratura) che ci riporta al terzo alfabeto, contrassegnato appunto dal codice AGMS. In altri termini, l'ordine alfabetico di cifratura di una parola dipende sempre dall'iniziale della parola che precede, come la soluzione di Bellaso dimostra opportunamente. Infatti, chi vorrà sottoporre a verifica il codice cifrato, potrà constatare che *gratia* produce il codice *qlthxu* poiché l'iniziale *m* della parola precedente, *maria*, rimanda al terzo alfabeto contrassegnato dal codice AGMS, dal quale si sa che la cifratura della lettera *g* di *gratia* è appunto la lettera *q*. Lo stesso dicasi per il codice *frdbe*, cifratura della parola *plena*, la cui prima lettera *p* è cifrata come *f* poiché la *g* di *gratia* indica che bisogna cominciare a cifrare dal terzo alfabeto (AGMS). Infine, a margine di questa terza variante, in verità Bellaso ne introduceva una quarta, basata sulla consueta introduzione della *x* a mo' di barra spaziatrice e – in questo specifico caso – utilizzata anche come chiave per comprendere da quale alfabeto ricominciare la decrittazione. Si prenda l'esempio della frase

, kiel oni vidas, havas en si mem la regulojn de la sia ĉifrado. Komencante ĉiam kiel regulo ekde la unua alfabeto kaj pluirante kun la sekvanta, oni ĉifras la unuan vorton *ave* kaj alvenas, kun la *e*, al la tria alfabeto. Pasante al la sekvanta vorto, *maria*, oni ne daŭras kun la kvara alfabeto, sed rekomencas de la tria, ĉar la unua litero de la antaŭa vorto, la *a* de *ave*, estas la indico (kaj do la regulo stricte observenda, alikaze la ĉifrado estas senefika) kiu reportas al la tria alfabeto, markita per la kodo AGMS. Alivorte, la alfabeta ordo de la ĉifrado de unu vorto dependas ĉiam de la inicialo de la antaŭa vorto, kiel la solvo de Bellaso oportune elmontras. Fakte, kiu volas submeti al kontrolo la ĉifritan kodon, tiu povos konstati ke *gratia* produktas la ĉifron *qlthxu* ĉar la inicialo *m* de la antaŭa vorto, *maria*, resendas al la tria alfabeto markita per la kodo AGMS, de kiu oni scias ke la ĉifrado de la litero *g* de *gratia* estas precize la litero *q*. Oni diras la samon pri la kodo *frdbe*, ĉifro de la vorto *plena*, de kiu la unua litero *p* estas ĉifrita kiel *f*, ĉar la *g* de *gratia* indikas ke oni necesas komenci ĉifri ekde la tria alfabeto (AGMS). Fine, marĝene ĉi tiun trian varianton, Bellaso vere enkondukis kvaran, bazitan sur la kutima enkonduko de la *x* kiel spacoklavo, kaj - en ĉi tiu specifa okazo - utiligita ankaŭ kiel ŝlosilo por kompreni de kiu alfabeto rekomenci la deĉifradon. Oni konsideras kiel ekzemplo la frazon

ars lunga vita brevis

, successivamente trasformata in

, sekve transformita en

arsxlungaxvitaxbrevis

, e con la cifratura (scritta dallo stesso Bellaso)

, kaj kun la ĉifrado (skribita de la sama Bellaso)

mglarcbrvabrheoelditl.

, basata su un meccanismo non molto dissimile da quello precedente, la cifratura del messaggio comincia dal primo alfabeto e procede fino al terzo (la parola *ars* è infatti costituita di tre lettere) e di seguito al quarto con la *x* dello spazio cifrata con la *a*, come comporta la tavola del quarto alfabeto. Questo è l'indizio che ci consente di sapere che per decrittare la lettera successiva, cioè la prima lettera della seconda parola della frase (*r*), dobbiamo cominciare dal quarto alfabeto, dove si scopre che infatti si tratta di una *l*, per la precisione la *l* di *lunga*. Per coloro che vogliano cimentarsi, il codice è suscettibile di una verifica che scopre, per errore di Bellaso o dello stampatore non ci è dato di saperlo[13], che la penultima cifra *t* dovrebbe più opportunamente essere una *x*. La striscia cifrata corretta è dunque

, bazita sur mekanismo ne multe malsimila de la antaŭa, la ĉifrado de la mesaĝo komencas per la unua alfabeto kaj pluiras ĝis la tria (la vorto *ars* estas fakte komponita de tri literoj) kaj sekve ĝis la kvara kun la *x* de lo spaceto ĉifrita kun la *a*, kiel implicas la tabelo de la kvara alfabeto. Ĉi tiu estas la indico kiu konsentas al ni scii ke por deĉifri la sekvantan literon, tio estas la unua litero de la dua vorto de la frazo (*r*), oni devas komenci de la kvara alfabeto, kie oni eltrovas ke fakte ĝi estas litero *l*, precize la *l* de *lunga*. Por tiuj, kiuj volas elprovi, la kodo estas kontrolebla, kaj oni eltrovas ke, oni ne scias ĉu kulpe de Bellaso aŭ de la presisto[14], la antaŭlasta ĉifro *t* devus pli oportune esti *x*. La ĝusta ĉifrita linio estas do

mglarcbrvabrheoeldixl

in luogo di

anstataŭ

mglarcbrvabrheoeldidtl

. Lascio a Bellaso la facoltà di concludere: *con questo quinto*[15] *singolar modo de cifrar, se cifra ancor senza fare la minuta*.

. Mi cedas al Bellaso la permeson konkludi: *con questo quinto*[16] *singolar modo de cifrar, se cifra ancor senza fare la minuta*.

III.

Il terzo metodo proposto da Bellaso (in verità sarebbe il sesto, ma si devono considerare le quattro varianti precedenti come "figlie" dello stesso procedimento) comporta l'utilizzo di una tavola polialfabetica più complessa. Per cominciare, dopo gli alfabeti formati a partire dalle parole SATURNO e IOVE, per restare in ambito cosmologico Bellaso ricorre alla *dittione* MARTE, che genera il primo alfabeto sottostante

La tria metodo proponita de Bellaso (vere ĝi estas la sesa, sed oni devas konsideri la antaŭajn kvar variantojn kiel "filinojn" de la sama procedo) implicas utiligi polialfabetan tabulon pli malsimplan. Por komenci, post la alfabetoj formitaj de la vortoj SATURNO kaj IOVE, por resti en la kosmologia kadro Bellaso ekuzas la *dittione* MARTE, kiu generas la unuan postan alfabeton:

MDTP	M	A	R	B	C	D	F	G	H	I
	T	E	L	N	O	P	Q	S	V	X

, contrassegnato dal codice MDTP e formato – come negli esempi precedenti – dalla consueta regola delle 5 posizioni, come si può vedere nella tavola completa dei 5 alfabeti:

, markita per la kodo MDTP kaj komponita - kiel en la antaŭaj ekzemploj - ekde la kutima regulo de la kvin pozicioj, kiel oni povas vidi en la kompleta tabelo de la kvin alfabetoj:

MDTP	**M**	A	R	B	C	**D**	F	G	H	I
	T	E	L	N	O	**P**	Q	S	V	X

AFEQ	M	**A**	R	B	C	D	**F**	G	H	I
	X	T	**E**	L	N	O	P	**Q**	S	V

RGLS	M	A	**R**	B	C	D	F	**G**	H	I
	V	X	T	E	**L**	N	O	P	Q	**S**

BHNV	M	A	R	**B**	C	D	F	G	**H**	I
	S	**V**	X	T	E	L	**N**	O	P	Q

CIOX	M	A	R	B	**C**	D	F	G	H	**I**
	Q	S	V	**X**	T	E	L	N	**O**	P

. Se guardiamo alla quinta tavola, come per il metodo precedente dobbiamo notare che nella combinazione CIOX la O viene prima della X perché la X le è, in un certo senso, ruotata alle spalle. Le tabelle potranno dirsi complete solo quando sarà introdotta, rispetto ai metodi precedenti, un'ulteriore corrispondenza con *dittioni* in luogo di lettere, *che nello scrivere occorrono spesso*. Non più solo cifre, dunque, bensì intere parole entrano nel fitto sistema di corrispondenze di Bellaso, che allo schema precedente (variato solo nella disposizione degli alfabeti, formati a partire da MARTE invece che da IOVE, e di conseguenza nei codici identificativi) aggiunge altre due righe per la cifratura di termini di uso comune. Vero è che, per ovvi motivi, l'autore pensa in modo particolare alle parole che rientrano con maggior frequenza nei messaggi cifrati per lo scambio di informazioni militari, politiche, diplomatiche, ecc..., simili per struttura a un moderno telegramma e strutturati per una comunicazione rapida, efficace e a basso rischio di fraintendimenti. Le tavole così

. Se oni rigardas la kvinan tabelon, kiel por la antaŭa metodo, oni devas rimarki ke en la kombino CIOX la O antaŭiras la X-n, ĉar la X iasence turniĝas malantaŭe kompare al ĝi. Oni povas diri ke la tabeloj estas kompletaj nur kiam, kompare al la antaŭaj metodoj, estos enkondukita plua respondo, per *dittioni* anstataŭe literoj, *che nello scrivere occorrono spesso*. Ne nur ĉifroj, sed ja kompletaj vortoj eniras en la densan sistemon de respondoj de Bellaso, kiu al la antaŭa skemo (ŝanĝita nur en la aranĝo de la alfabetoj, komponitaj de la vorto MARTE anstataŭ IOVE, kaj konsekvence en la identigaj kodoj) aldonas aliajn du liniojn por ĉifri ordinarajn vortojn. Veras ke, pro evidentaj motivoj, la aŭtoro pensas aparte al la vortoj kiuj envenas ofte en la ĉifritaj mesaĝoj, en la interŝanĝo de militaj, politikaj, diplomataj, kaj tiel plu, informoj, kiuj similas strukture modernan telegramon kaj estas strukturitaj por komunikado rapida, efika kaj per malgranda risko de miskomprenadoj. La tabeloj tiel komponitaj estigas do la postan kradon, reproduktita komplete en *Il vero modo*

composte daranno dunque luogo alla griglia sottostante, riprodotta per intero ne *Il vero modo di scrivere in cifra:*

di scrivere in cifra:

MDTP	altra	alcuno	assai	accio	accioche	ancora	ancorache	benche	che	che
	M	A	R	B	C	D	F	G	H	I
	T	E	L	N	O	P	Q	S	V	X
	che	cosa	cosi	come	certi	della	debba	dica	detto	deve

AFEQ	del	doppo	dubio	essere	essendo	essa	eccellente	fussi	forsi	gratia
	M	A	R	B	C	D	F	G	H	I
	X	T	E	L	N	O	P	Q	S	V
	grata	grande	havuta	havemo	hanno	habia	imperoche	ilche	ilquale	In ogni

RGLS	intutto	ilvostro	ilnostro	imperio	lettera	laquale	lequale	laonde	lamolto	molto
	M	A	R	B	C	D	F	G	H	I
	V	X	T	E	L	N	O	P	Q	S
	modo	male	mondo	mille	non	Non	nostro	nella	ogni	ognicosa

BHNV	per	perilche	per	perci	percioche	poco	poter	prego	poi	possa
	M	A	R	B	C	D	F	G	H	I
	S	V	X	T	E	L	N	O	P	Q
	quanto	quella	quando	questa	qualche	recevuta	scritta	scrisse	scrivo	stata

CIOX	sopra	sono	sempre	signor	signoria	tutto	tanta	virtu	vostra	una
	M	A	R	B	C	D	F	G	H	I
	Q	S	V	X	T	E	L	N	O	P
	habiamo recevute le vostre lettere	le vostre lettere me sono state gratissime	laviso che me datime accaro per diversi rispetti	ve dicemo in risposta della vostra che etc.	usareti ogni diligentia p saper la verita de questo fatto	quanto piu presto me dareti aviso che tanto piu accaro	se confidemo nella vostra prudenza etc.	e stato resolto nel nostro consilio che	non mancari esequie quanto ve habiamo scritto	desideremo haver piu particolar aviso de questo fatto

. Nonostante l'utilizzo di tabelle alfabetiche differenti, il terzo metodo si può considerare una sorta di riassunto delle tre varianti del secondo e un'anticipazione del quarto, più complesso e meno intuitivo dei precedenti. L'esempio di Bellaso spiega opportunamente come utilizzare le tabelle e le loro possibilità di cifratura. La frase

. Kvankam la uzado de malsimilaj alfabetaj tabeloj, la tria metodo povas esti konsiderita kiel resumo de la tri variantoj de la dua metodo, kaj antaŭigo de la kvara, kiu estas pli malsimpla kaj malpli intuicia ol la antaŭaj. La ekzemplo de Bellaso klarigas oportune kiel utiligi la tabelojn kaj siajn eblojn de ĉifrado. La frazo

havemo inteso della vostra venuta laqual mestata molto acara perilche

dovrà essere trasformata tenendo conto che alcune parole sono comprese nella tabella alfabetica di cifratura (per es. *havemo* corrisponde alla lettera L dell'alfabeto contrassegnato dal codice AFEQ), mentre per le altre bisognerà utilizzare uno dei metodi già adoperati nelle 3 varianti del secondo metodo. Come modello iniziale, Bellaso ripropone l'espediente del versetto

devos esti transformita konsiderate ke kelkaj vortoj estas entenataj en la alfabeta tabelo de ĉifrado (ekzemple, *havemo* kongruas al la litero L de la alfabeto markita per la kodo AFEQ), dume por la aliaj vortoj oni necesos utiligi unuelan metodo jam uzitan en la tri variantoj de la dua metodo. Kiel komenca ekzemplo, Bellaso reproponas la artifikon de la verseto

, che *à far la minuta*, come direbbe l'autore, comporterà la seguente trasformazione:

, kiu *à far la minuta*, kiel la aŭtoro dirus, implicos la postan transformon:

	O			P		T		A	
havemo	inteso	della	vostra	venuta	laqual	mestata	molto	acara	perilche

. Le parole associate alle lettere del versetto sono quelle non suscettibili di cifratura diretta secondo le tabelle alfabetiche. Queste *dittioni comprese nella cartella de la cifra, che non hanno sopra le lettere del versetto, la cifra con doi lettere, a questo modo, mira con l'occhio nella cartella a qual alfabeto picciolo sia quella dittione, et piglia una lettera maiuscola, quale a lui piace delle quattro lettere maiuscole, che stanno da capo dal detto alfabeto piciolo, et la compagna con la lettera del detto alfabeto piciolo, che posta sopra ò sotto della detta dittione, che'l vuol cifrare, come per esempio diremo, a cifrar molto, toremo la, g, maiuscola, et la, i, del suo alfabeto piciolo, che sotto a molto a questo modo, gi, et così, gi, dirà molto*. Consapevole o non consapevole che fosse, Bellaso confonde un po' le acque del lettore, perché l'esempio della parola *molto* cifrata come GI è soltanto uno dei 4 possibili (il codice della tabella corrispondente essendo RGLS, *molto* potrà essere cifrata indifferentemente RI, GI, LI, SI) e peraltro non è quello che – come vedremo – sarà utilizzato nella cifratura della frase esemplificativa. Ripartiamo da quella e vediamo qual è la striscia cifrata secondo il metodo "misto" che comprende il ricorso al versetto. La soluzione finale darà:

. La vortoj asociitaj al la literoj de la verseto estas tiuj ne rekte ĉifreblaj laŭ la alfabetaj tabeloj. Ĉi tiuj *dittioni comprese nella cartella de la cifra, che non hanno sopra le lettere del versetto, la cifra con doi lettere, a questo modo, mira con l'occhio nella cartella a qual alfabeto picciolo sia quella dittione, et piglia una lettera maiuscola, quale a lui piace delle quattro lettere maiuscole, che stanno da capo dal detto alfabeto piciolo, et la compagna con la lettera del detto alfabeto piciolo, che posta sopra sotto della detta dittione, che'l vuol cifrare, come per esempio diremo, a cifrar molto, toremo la, g, maiuscola, et la, i, del suo alfabeto piciolo, che sotto a molto a questo modo, gi, et così, gi, dirà molto*. Konscie aŭ ne, Bellaso konfuzas la leganton, ĉar la ekzemplo de la vorto *molto* ĉifrita kiel GI estas nur unuela kvar eblo (ĉar la kodo de la responda tabelo estas RGLS, *molto* povas esti ĉifrita indiferente RI, GI, LI, kaj SI), kaj cetere - kiel oni vidos - ĝi ne estas tiu, kiu estis uzita en la ĉifrado de la ekzempla frazo. Oni reekiras de tiu, kaj oni vidu kiu estas la ĉifrita linio laŭ la "miska" metodo kiu inkludas la sinturnon al la verseto. La fina solvo estas:

ql pbabmh pp ch hrdace ld tribsmt li tlvve va

. Abbiamo detto che si tratta, in un certo senso, di un metodo "misto". Vediamo il perché. Seguendo passo dopo passo le indicazioni di Bellaso, sappiamo che la cifratura "a coppie di lettere" (come nel caso di *ql, pp, ch, ld, li, va*) sta a significare che delle due è l'una: o si tratta della cifra di una parola composta di sole due lettere, oppure si tratta di un "codicillo" che copre un'intera parola compresa nella cifratura delle 5 tabelle alfabetiche. In questo caso, tuttavia, se si guarda con attenzione il messaggio da cifrare, Bellaso si è premurato di riunire le parole brevi a quelle più lunghe – grazie all'espediente già utilizzato nella prima variante del secondo metodo - e ha quindi sciolto a monte la possibilità di confusione da parte del decrittatore. La *qual* è dunque divenuta *laqual* e *mi è stata*, secondo il medesimo "trucco", *mestata*. Si presti ora attenzione alle tabelle alfabetiche di cifratura. Come nei metodi precedenti, ogni codice identifica attentamente la tabella associata. Nella cifratura a coppie la prima lettera sarà dunque da attribuire al codice, mentre la seconda individuerà la parola cifrata nella tabella corrispondente. Per esempio, la sigla QL sta a indicare che nella tabella contrassegnata dal codice AFEQ la lettera L cifra la parola posta al di sotto, *havemo*; la sigla PP cifra la parola *della* posta sotto la P della tabella contrassegnata dal codice MDTP; la sigla CH sta per *vostra*, parola posta al di sopra della H della tabella con codice CIOX; la sigla LD rimanda alla parola riunita *laquale*, posta al di sopra della D nella terza tabella con codice RGLS; la sigla LI ancora alla terza tabella, dove sopra la I è collocata la parola *molto*, che come già anticipato alcune righe sopra non è cifrata secondo l'esempio precedente GI ma come, appunto, LI; con la sigla VA sappiamo invece che la tabella è la quarta con codice BHNV e che sopra la lettera A si trova la parola riunita *perilche*. A questo punto, non resta che decrittare le altre, per le quali si agirà come nella prima variante (IIa) del se-

. Ni diris ke ĝi estas, iasence, "miksa" metodo. Ni vidu la kialon. Sekvante paŝon post paŝo la indikojn de Bellaso, oni scias ke la ĉifrado "literopare" (kiel en la kazo de *ql*, *pp*, *ch*, *ld*, *li*, *va*) signifas ke aŭ ĝi estas la ĉifro de vorto komponita el nur du literoj, aŭ ĝi estas "kodeto" kiu kovras tutan vorton, entenata en la ĉifrado de la kvin alfabetaj tabeloj. Tiukaze, tamen, se oni observas atente la ĉifrendan mesaĝon, Bellaso zorgis rekunigi la mallongajn vortojn al la longaj vortoj - merite al la artifiko jam uzita en la unua varianto de la dua metodo - kaj tial li antaŭsolvis la eblon de konfuzo de la ĉifristo. *La qual* estas do *laqual*, e *mi stata*, laŭ la sama artifiko, *mestata*. Nun ni atentu al la alfabetaj tabeloj de ĉifrado. Kiel en la antaŭaj metodoj, ĉiu kodo identigas atente la asociitan tabelon. En la ĉifrado literopare la unua litero estos do atribuenda al la kodo, dume la dua identigas la ĉifritan vorton en la asociita tabelo. Ekzemple, la siglo QL indikas ke en la tabelo markita per la kodo AFEQ la litero L ĉifras la substarantan vorton, *havemo*; la siglo PP ĉifras la vorton *della*, lokita sub la P de la tabelo markita per la kodo MDTP; la siglo CH estas por *vostra*, vorto kiu estas supre la litero H de la tabelo kun la kodo CIOX; la siglo LD resendas al la komponita vorto *laquale*, lokita supre al la D en la tria tabelo kun kodo RGLS; la siglo LI resendas ankoraŭ al la tria tabelo, kie supre al la I estas la vorto *molto*, kiu - kiel ni diris pli frue - ne estas ĉifrita, laŭ la antaŭa ekzemplo, GI, sed LI; por la siglo VA oni scias ke la tabelo estas la kvara kun kodo BHNV, kaj ke sur la litero A oni trovas la kunigitan vorton *perilche*. Nun oni devas nur deĉifri la aliajn literojn, por kiuj oni agas kiel en la unua varianto (IIa) de la dua metodo, tio estas rigardante la unuan literon de la verseto O, kiu siavice indikas de kiu alfabeta tabelo komencas la deĉifrado: la kvina, markita per la kodo CIOX. La unua litero de la ĉifrita *dittione*, la *p* de *pbabmh*, indikas ke la *i* estas la unua litero de la neĉifrita vorto, al kiu sekvas la

condo metodo, vale a dire guardando alla prima lettera del versetto O, che a sua volta ci indica da quale tabella alfabetica cominciare la decrittazione: la quinta, contrassegnata dal codice CIOX. La prima lettera della *dittione* criptata, la *p* di *pbabmh*, ci indica dunque che è la *i* la prima lettera della parola in chiaro, alla quale farà seguito la *n* cifrata con la *b* della prima tabella, poiché dopo la quinta abbiamo ricominciato a contare, appunto, dalla prima tabella alfabetica. E così via, con lo stesso schema applicato alla seconda parola riunita cifrata, quella *hrdace* associata alla lettera del versetto e quindi alla prima tabella contrassegnata dal codice MDTP, la cui lettera *h* cifra la *v*, prima lettera della *dittione venuta*. Non pago, Bellaso anziché esaurire il terzo metodo a un metodo "misto" che utilizzi soltanto la prima variante del secondo metodo, lo estende anche alle altre due possibilità, tenendo a precisare che *il medemo dico de quelli, che vorranno cifrar senza versetto, liquali non metteranno lettere nel principio de le dittioni compresi nella cartella de la cifra, similmente dico de quelli che vorranno cifrare senza versetto, et senza mettere lettere nel principio de le dittioni, ma voranno cifrare al terzo modo* [terza variante del secondo metodo II.c], *le quali non cifreranno le dittioni compresi nella cartella de la cifra con la lettera de la precedente dittione, ma le cifreranno al modo di sopra insegnato*. Riassumendo e semplificando: per quanto concerne l'applicazione del secondo metodo, rimane inalterata la cifratura (*ql, pp, ch, ld, li, va*) delle parole incluse nelle 5 tabelle alfabetiche, mentre al posto della cifratura a mezzo versetto si ricorrerà, come già illustrato, al prefisso di una maiuscola che identifichi la tabella alfabetica da cui procedere con la decrittazione. In questo caso la striscia criptata risultante sarà la seguente:

litero *n* ĉifrita kun la *b* de la unua tabelo, ĉar post la kvina oni rekomencas nombri precize de la unua alfabeta tabelo. Kaj tiel plu, kun la sama skemo aplikita al la dua vorto markita per la kodo MDTP, kies litero *h* ĉifras la literon *v*, la unua litero de la *dittione venuta*. Bellaso, anstataŭ ol kompletigi la trian metodon kiel "miksa" metodo, kiu utiligas nur la unuan varianton de la dua metodo, etendas ĝin ankaŭ al la aliaj du ebloj, specifante ke *il medemo dico de quelli, che vorranno cifrar senza versetto, liquali non metteranno lettere nel principio de le dittioni compresi nella cartella de la cifra, similmente dico de quelli che vorranno cifrare senza versetto, et senza mettere lettere nel principio de le dittioni, ma voranno cifrare al terzo modo* [la tria varianto de la dua metodo, II.c], *le quali non cifreranno le dittioni compresi nella cartella de la cifra con la lettera de la precedente dittione, ma le cifreranno al modo di sopra insegnato*. Por resumi kaj simpligi: koncerne la aplikadon de la dua metodo, estas neŝanĝita la ĉifrado (*ql*, *pp*, *ch*, *ld*, *li*, *va*) de la vortoj entenataj en la kvin alfabetaj tabeloj, dume, anstataŭ la ĉifrado per verseto, kiel jam montrite oni reiru al la prefikso de ĉeflitero, kiu indikas la alfabetan tabelon de kiu progresi kun la deĉifrado. Tiukaze la rezultanta ĉifrita linio estas la sekvanta:

ql Fvdbdgd pp ch Badbirv ld Cqahrvce li Tenxxs va

, dove la *F* di *Fvdbdgd* sta a indicare che, cominciando a decrittare

, kie la *F* de *Fvdbdgd* indikas ke, komencante la deĉifrado ekde la

dalla seconda tavola, si può ricavare che la prima lettera *v* sta per la *i*, prima lettera di inteso; che la *B* di *Badbirv* indica la quarta tabella, dove la prima lettera *a* è la cifra di *v*, prima lettera di *venuta*; che la *C* di *Cqahrvce* rimanda alla quinta tabella, dove *q* è la cifra di *m*, prima lettera di *mestata*; infine, che la *T* di *Tenxxs* indica la prima tabella, dove *e* è la cifra di *a*, prima lettera di *acara*. Se invece si vuole applicare la terza variante, la più complessa di quelle esposte nel secondo metodo, si otterrà come striscia criptata:

dua tabelo, oni povas eltiri ke la unua litero *v* estas por la *i*, la unua litero de *inteso*; ke la litero *B* de *Badbirv* indikas la kvaran tabelon, kie la unua litero *a* ĉifras la *v*-n, la unua litero de *venuta*; ke la *C* de *Cqahrvce* resendas al la kvina tabelo, kie *q* estas la ĉifro de *m*, la unua litero de *mestata*; finfine, ke la *T* de *Tenxxs* indikas la unuan tabelon, kie la *e* estas la ĉifro de *a*, la unua litero de *acara*. Se anstataŭe oni volas apliki la trian varianton, tio estas la pli kompleksa el tiuj prezentitaj en la dua metodo, oni obtenos kiel ĉifrita linio:

ql xcrcac pp ch rcambs ld sdgarv li enxxs va

, dove, rimasta inalterata la cifratura (*ql, pp, ch, ld, li, va*) delle parole incluse nelle 5 tabelle alfabetiche, dalla prima parola *xcrcac* sappiamo che si prende avvio dalla prima tabella (infatti la *x* sta per la *i* di *inteso*); che per la seconda parola *rcambs* si riparte dalla tabella che ha il codice identificativo che comprende la prima lettera della parola precedente in chiaro (la *i* di *inteso* rimanda al codice CIOX identificativo della quinta tabella, quindi la *r* di *rcambs* sta per la *v* di *venuta*); che per la terza parola *sdgarv* si va alla quarta tabella con codice BHNV (poiché *venuta* comincia con la *v*), dove la prima lettera *s* è cifra di *m*, prima lettera di mestata; che, infine, da questa *m* sappiamo che per la parola *enxxs* dobbiamo andare alla prima tabella con codice identificativo MDTP, dove scopriamo che la *e* sta per *a*, prima lettera - non a caso - della parola acara. Cos'altro sapere? Ascoltiamo le parole di Bellaso: *le dittione, che sono poste nella cifra, si devono pigliar in ogni genere, et numero, come sarebbe adire, altra, per altra intenderemmo altri altre altra, et per havuta, havuti, havuto, per quanta, quante, quanta, quanti: et cosi dico dell'altre dittioni*. Insomma, per l'autore l'importante era che mittente e destinatario potessero comprendersi aldilà di ogni differenza. E, aggiungiamo noi, di ogni ostacolo.

, kie, dum restas neŝanĝita la ĉifrado (*ql*, *pp*, *ch*, *ld*, *li*, *va*) de la vortoj entenataj en la kvin alfabetaj tabeloj, ekde la unua vorto *xcrcac* oni scias ke oni devas komenci de la unua tabelo (fakte la *x* estas por la *i* de *inteso*); ke por la dua vorto *rcambs* oni restartas de la tabelo markita per la kodo kiu inkludas la unuan literon de la antaŭa neĉifrita vorto (la *i* de *inteso* resendas al la kodo CIOX kiu identigas la kvinan tabelon, do la *r* de *rcambs* estas por la *v* de *venuta*); ke por la tria vorto *sdgarv* oni iras al la kvara tabelo kun kodo BHNV (ĉar *venuta* komencas per la *v*), kie la unua litero *s* ĉifras *m*-n, la unua litero de *mestata*; ke, finfine, de ĉi tiu litero *m* oni scias ke por la vorto *enxxs* ni devas iri al la unua tabelo kun kodo MDTP, kie oni eltrovas ke la *e* ĉifras la *a*-n, rekte la unua litero de la vorto *acara*. Kion alian oni volas scii? Oni aŭskultas la vortojn de Bellaso: *le dittione, che sono poste nella cifra, si devono pigliar in ogni genere, et numero, come sarebbe adire, altra, per altra intenderemmo altri altre altra, et per havuta, havuti, havuto, per quanta, quante, quanta, quanti: et cosi dico dell'altre dittioni*. Sume, por la aŭtoro estis grava ke la sendanto kaj la adresato povus interkompreniĝi trans ĉiu diverseco. Kaj, ni aldonas, trans ĉiu obstaklo.

IV.

Per spiegare il quarto e ultimo metodo, senza dubbio il più intricato sia per il cifratore che per il decrittatore, Bellaso usa – stranamente, data la difficoltà oggettiva – poche parole a titolo di presentazione. *La cifra, che segue, se compone con due dittioni, con una si forma l'alfabeto, che sta da capo delle maiuscole, et con l'altra, lo alfabeto che va per traverso à rota, come è detto di sopra, liquali doi soli alfabeti si mutano mutando la cifra, il resto de la cifra, stà sempre ad un modo.* Fin qui, Bellaso non è molto chiaro. Cominciamo dalla nuova tabella polialfabetica che l'autore utilizza per questo metodo di cifratura, riprodotta qui di seguito:

Por klarigi la kvaran kaj lastan metodon, sendube la pli komplikan kaj por la ĉifristo kaj por la deĉifristo, Bellaso uzas - strange, se oni konsideras la objektivan malfacilon - malmultajn vortojn kiel enkondukon. *La cifra, che segue, se compone con due dittioni, con una si forma l'alfabeto, che sta da capo delle maiuscole, et con l'altra, lo alfabeto che va per traverso à rota, come è detto di sopra, liquali doi soli alfabeti si mutano mutando la cifra, il resto de la cifra, stà sempre ad un modo.* Ĝis ĉi tie, Bellaso estas malklara. ONi komencu de la nova polialfabeta tabelo ke la aŭtoro uzas por ĉi tiu metodo de ĉifrado, poste reproduktita:

P	pv	pe	pn	pt	pi	pa	pr	pm	pd	px	pb	pc	pf	pg	ph
	aa	ea	ia	oa	va	A	aa	ae	ai	ao	av	A	accio	altra	ancora

H	hh	hv	he	hn	ht	hi	ha	hr	hm	hd	hx	hb	hc	hf	hg
	ab	eb	ib	ob	vb	B	ba	be	bi	bo	bv	B	benche	che	che

I	ig	hh	iv	ie	in	it	ii	ia	ir	im	id	ix	ib	ic	if
	ac	ec	ic	oc	vc	C	ca	ce	ci	co	cv	Ch	cosa	como	della

L	lf	lg	lh	lv	le	ln	lt	li	la	lr	lm	ld	lx	lb	lc
	ad	ed	id	od	vd	D	da	de	di	do	dv	D	debba	detto	doppo

V	vc	vf	vg	vh	vv	ve	vn	vt	vi	va	vr	vm	vd	vx	vb
	ae	ee	ie	oe	ve	E	ea	ee	ei	eo	ev	E	esso	essendo	essere

S	sb	sc	sf	sg	sh	sv	se	sn	st	si	sa	sr	sm	sd	sx
	af	ef	if	of	vf	F	fa	fe	fi	fo	fv	F	forsi	fvssi	finche

A	ax	ab	ac	af	ag	ah	av	ae	an	at	ai	aa	ar	am	ad
	ag	eg	ig	og	vg	G	ga	ge	gi	go	gv	G	gratia	grave	grato

B	bd	bx	bb	bc	bf	bg	bh	bv	be	bn	bt	bi	ba	br	bm
	ah	eh	ih	oh	vh	H	ha	he	hi	ho	hv	H	abia-mo	avvto	hanno

C	cm	cd	cx	cb	cc	cf	cg	ch	cv	ce	cn	ct	ci	ca	cr
	ai	ei	ii	oi	vi	I	ia	ie	ii	io	iv	I	impe-rio	impo	impe-roche

D	dr	dm	dd	dx	db	dc	df	dg	dh	dv	de	dn	dt	di	da
	al	el	il	ol	vl	L	la	le	li	lo	lv	L	leqva-li	liqva-li	lettera

E	ea	er	em	ed	ex	eb	ec	ef	eg	eh	ev	ee	en	et	Ei
	am	em	im	om	vm	M	ma	me	mi	mo	mv	M	molto	modo	mon-do

F	fi	fa	fr	fm	fd	fx	fb	fc	ff	fg	fh	fv	fe	fn	ft
	an	en	in	on	vn	N	na	ne	ni	no	nv	N	non	nostra	nella

G	gt	gi	ga	gr	gm	gd	gx	gb	gc	gf	gg	gh	gv	ge	gn
	ao	eo	io	oo	vo	O	oa	oe	oi	oo	ov	O	oltra	ogni	ogni-cosa

M	mn	mt	mi	ma	mr	mm	md	mx	mb	mc	mf	mg	mh	mv	me
	ap	ep	ip	op	vp	P	pa	pe	pi	po	pv	P	per	per	per-che

N	ne	nn	nt	ni	na	nr	nm	nd	nx	nb	nc	nf	ng	nh	nv
	aq	eq	iq	oq	vq	Q	st	st	st	st	qv	Q	qvali	qvella	qvesta

O	ov	oe	on	ot	oi	oa	or	om	od	ox	ob	oc	of	og	oh
	ar	er	ir	or	vr	R	ra	re	ri	ro	rv	R	qvan-to	qvan-do	qval-che

Q	qh	qv	qe	qn	qt	qi	qa	qr	qm	qd	qx	qb	qc	qf	qg
	as	es	is	os	vs	S	sa	se	si	so	sv	S	signor	signo-ria	scritto

R	rg	rh	rv	re	rn	rt	ri	ra	rr	rm	rd	rx	rb	rc	rf
	at	et	it	ot	vt	T	ta	te	ti	to	tv	T	scris-se	tvtto	tanto

T	tf	tg	th	tv	te	tn	tt	ti	ta	tr	tm	td	tx	tb	tc
	av	ev	iv	ov	vv	V	va	ve	vi	vo	vv	V	vostro	vero	vna

X	xc	xf	xg	xh	xv	xe	xn	xt	xi	xa	xr	xm	xd	xx	xb
	br	dr	gn	lt	nq	X	pr	rl	rp	rt	st	X	Vostra Sig.	le vostre lettere	qvanto più presto

Y	yb	yc	yf	yg	yh	yv	ye	yn	yt	yi	ya	yr	ym	yd	yx
	ch	fr	gr	mn	nt	Y	rc	rm	rs	sc	tr	Y	il Signor Iddio	le cose passano	me racomando

Z	zx	zb	zc	zf	zg	zh	zv	ze	zn	zt	zi	za	zr	zm	zd
	cr	gl	lm	nc	pn	Z	rd	rn	rt	sp	tr	Z	habiamo recevvte	havemo spiacer	fatime raccom.

. Rispetto alle tavole alfabetiche precedenti, almeno a un primo sguardo – e non solo – la disposizione di questa tabella appare meno intuitiva e sembrerebbe suggerire un utilizzo più complesso. Tanto per cominciare, Bellaso sorvola sulla parola chiave per la formazione degli alfabeti. Dopo SATURNO, IOVE e MARTE, il lettore si chiede a quale espediente questa volta abbia fatto ricorso. Se è vero che la tabella, laddove ben interpretata, può correre in aiuto, è tuttavia all'incipit del dotto libello che occorre volgere le pagine, fino a scoprire che alle tre citate chiavi si unisce una quarta, PHILIPPVS

. Kompare al la antaŭaj alfabetaj tabeloj, almenaŭ se oni rigardas rapide - kaj ne nur -, la aranĝo de ĉi tiu tabelo aperas malpli intuicia kaj ŝajnus sugesti uzon pli kompleksan. Unuloke, Bellaso preterflugas la ŝlosilvorton por formi la alfabetojn. Post SATURNO, IOVE, kaj MARTE, la leganto demandas kiun artifikon ĉi-foje li ekuzis. Se ja veras ke la tabelo, se bone interpretita, povas helpi, tamen estas necese reveni al la komencaj vortoj de la erudiciplena libreto, ĝis oni eltrovas ke al la tri menciitaj ŝlosilvortoj aldoniĝas kvaran, PHILIPPVS VENETIARVM DVX. En la antaŭe priskribitaj tabeloj,

VENETIARVM DVX. Nelle tavole di cui sopra, il riconoscimento della chiave che genera il sistema polialfabetico non è intuitivo come nelle tabelle precedenti. La disposizione delle lettere di VENETIARVM DVX e PHILIPPVS, che come negli altri casi non vengono - ovviamente - ripetute, è evidenziata in rosso:

la rekono de la ŝlosilvorto kiu generas la polialfabetan sistemon ne estas intuicia kiel en la antaŭaj tabeloj. La aranĝo de la literoj de VENETIARVM DVX kaj PHILIPPVS, kiu ne estas - kompreneble - ripetita kiel alikaze, estas rimarkigita ruĝe:

P	p**v**	p**e**	p**n**	p**t**	p**i**	p**a**	p**r**	p**m**	p**d**	p**x**	pb	pc	pf	pg	ph
	aa	ea	ia	oa	va	A	aa	ae	ai	ao	av	A	accio	altra	ancora
H															
I															
L															
V															
S															

. La comprensione di questo sistema polialfabetico necessita di un'analisi attenta e scrupolosa. Come vedremo, porterà alla luce alcune eccezioni, che lo rendono ancora più ostico. Abbiamo visto che a partire da PHILIPPVS e VENETIARVM DVX si generano i primi due alfabeti. Le rimanenti lettere, tuttavia, rimandano a due alfabeti differenti: quello di PHILIPPVS non conosce la lettera H e conosce invece X, Y e Z; quello di VENETIARVM DVX è l'alfabeto consueto delle tavole di Bellaso, comprensivo di H e di X ma privo di L, O, P, Q, S, Y e Z. Tornando di nuovo all'esempio della "ruote", possiamo vedere che l'alfabeto di VENETIARVM DVX "gira" e si comporta come nelle tabelle polialfabetiche utilizzate nei primi tre

. La kompreno de ĉi tiu polialfabeta sistemo necesas atentan kaj skrupulan analizon. Kiel ni vidos, ĝi prilumos kelkajn esceptojn, kiuj igas ĝin ankoraŭ pli kompleksa. Oni vidis ke de PHILIPPVS kaj VENETIARVM DVX generas la unuaj du alfabetoj. La restantaj literoj tamen resendas al du malsamaj alfabetoj: ĉi tiu de PHILIPPVS ne konas la literon H kaj konas anstataŭe X, Y, kaj Z; ĉi tiu de VENETIARVM DVX estas la sama alfabeto de la tabeloj de Bellaso, entenanta la literon H kaj X sed sen la literoj L, O, P, Q, S, Y, kaj Z. Revenante de nove al la ekzemplo de la "rado", oni povas vidi ke la alfabeto de VENETIARVM DVX "turniĝas" kaj agas kiel en la polialfabetaj tabeloj uzitaj en la unuaj tri metodoj, kiel oni povas observi

metodi, come può essere osservato dallo spostamento della lettera di V di VENETIARVM, che evidenzieremo in rosso:

ekde la movo de la litero V de VENETIARVM, kiu estas rimarkigita ruĝe:

P	pv	pe	pn	pt	pi	pa	pr	pm	pd	px	pb	pc	pf	pg	ph
	aa	ea	ia	oa	va	A	aa	ae	ai	ao	av	A	accio	altra	ancora

H	hh	hv	he	hn	ht	hi	ha	hr	hm	hd	hx	hb	hc	hf	hg
	ab	eb	ib	ob	vb	B	ba	be	bi	bo	bv	B	ben-che	che	che

I	ig	hh	iv	ie	in	it	ii	ia	ir	im	id	ix	ib	ic	if
	ac	ec	ic	oc	vc	C	ca	ce	ci	co	cv	Ch	cosa	como	della

L	lf	lg	lh	lv	le	ln	lt	li	la	lr	lm	ld	lx	lb	lc
	ad	ed	id	od	vd	D	da	de	di	do	dv	D	debba	detto	doppo

V	vc	vf	vg	vh	vv	ve	vn	vt	vi	va	vr	vm	vd	vx	vb
	ae	ee	ie	oe	ve	E	ea	ee	ei	eo	ev	E	esso	essen-do	essere

S	sb	sc	sf	sg	sh	sv	se	sn	st	si	sa	sr	sm	sd	sx
	af	ef	if	of	vf	F	fa	fe	fi	fo	fv	F	forsi	fvssi	finche

A	ax	ab	ac	af	ag	ah	av	ae	an	at	ai	aa	ar	am	ad
	ag	eg	ig	og	vg	G	ga	ge	gi	go	gv	G	gratia	grave	grato

B	bd	bx	bb	bc	bf	bg	bh	bv	be	bn	bt	bi	ba	br	bm
	ah	eh	ih	oh	vh	H	ha	he	hi	ho	hv	H	abia-mo	avvto	hanno

C	cm	cd	cx	cb	cc	cf	cg	ch	cv	ce	cn	ct	ci	ca	cr
	ai	ei	ii	oi	vi	I	ia	ie	ii	io	iv	I	impe-rio	impo	impe-roche

D	dr	dm	dd	dx	db	dc	df	dg	dh	dv	de	dn	dt	di	da
	al	el	il	ol	vl	L	la	le	li	lo	lv	L	leqva-li	liqva-li	lettera

E	ea	er	em	ed	ex	eb	ec	ef	eg	eh	ev	ee	en	et	Ei
	am	em	im	om	vm	M	ma	me	mi	mo	mv	M	molto	modo	mon-do

F	fi	fa	fr	fm	fd	fx	fb	fc	ff	fg	fh	fv	fe	fn	ft
	an	en	in	on	vn	N	na	ne	ni	no	nv	N	non	nostra	nella

G	gt	gi	ga	gr	gm	gd	gx	gb	gc	gf	gg	gh	gv	ge	gn
	ao	eo	io	oo	vo	O	oa	oe	oi	oo	ov	O	oltra	ogni	ogni-cosa

M	mn	mt	mi	ma	mr	mm	md	mx	mb	mc	mf	mg	mh	mv	me
	ap	ep	ip	op	vp	P	pa	pe	pi	po	pv	P	per	per	per-che

N	ne	nn	nt	ni	na	nr	nm	nd	nx	nb	nc	nf	ng	nh	nv
	aq	eq	iq	oq	vq	Q	st	st	st	st	qv	Q	qvali	qvella	qvesta

O	ov	oe	on	ot	oi	oa	or	om	od	ox	ob	oc	of	og	oh
	ar	er	ir	or	vr	R	ra	re	ri	ro	rv	R	qvan-to	qvan-do	qval-che

Q	qh	qv	qe	qn	qt	qi	qa	qr	qm	qd	qx	qb	qc	qf	qg
	as	es	is	os	vs	S	sa	se	si	so	sv	S	signor	signo-ria	scritto

R	rg	rh	rv	re	rn	rt	ri	ra	rr	rm	rd	rx	rb	rc	rf
	at	et	it	ot	vt	T	ta	te	ti	to	tv	T	scris-se	tvtto	tanto

T	tf	tg	th	tv	te	tn	tt	ti	ta	tr	tm	td	tx	tb	tc
	av	ev	iv	ov	vv	V	va	ve	vi	vo	vv	V	vostro	vero	vna

X	xc	xf	xg	xh	xv	xe	xn	xt	xi	xa	xr	xm	xd	xx	xb
	br	dr	gn	lt	nq	X	pr	rl	rp	rt	st	X	Vostra Sig.	le vo-stre let-tere	qvan-to pi pre-sto

Y	yb	yc	yf	yg	yh	yv	ye	yn	yt	yi	ya	yr	ym	yd	yx
	ch	fr	gr	mn	nt	Y	rc	rm	rs	sc	tr	Y	il Si-gnor Iddio	le cose pas-sano	me raco-mando

Z	zx	zb	zc	zf	zg	zh	zv	ze	zn	zt	zi	za	zr	zm	zd
	cr	gl	lm	nc	pn	Z	rd	rn	rt	sp	tr	Z	ha-biamo rece-vvte	have-mo spia-cer	fati-me rac-com.

. La peculiarità di questo sistema polialfabetico riposa nell'utilizzo di altri due alfabeti "intermedi", diversi dai precedenti per il fatto che conoscono X, Y e Z e con un certo stupore anche la lettera H, assente nell'alfabeto generato da PHILIPPVS. Sarà necessario evidenziare in colore rosso la loro posizione e le lettere di cui si compongono, fermo restando che in questo caso, assente una parola chiave che li genera, l'ordine è quello canonico A...Z.

. La karakterizaĵo de ĉi tiu polialfabeta sistemo troviĝas en la uzo de la aliaj du "mezaj" alfabetoj, neegalaj al antaŭaj tial ke ĉi tiuj konas X, Y kaj Z kaj surprize ankaŭ la literon H, neestanta en la alfabeto generita de PHILIPPVS. Do necesas rimarki ruĝe ilian aranĝon kaj la literojn kiuj ilin komponas, kaj tiukaze estas egale ke, se la ŝlosilvorto kiu generas ilin estas for, la ordo estas la kutima A....Z.

P	pv	pe	pn	pt	pi	pa	pr	pm	pd	px	pb	pc	pf	pg	ph
	aa	ea	ia	oa	va	A	aa	ae	ai	ao	av	A	accio	altra	ancora

H	hh	hv	he	hn	ht	hi	ha	hr	hm	hd	hx	hb	hc	hf	hg
	ab	eb	ib	ob	vb	B	ba	be	bi	bo	bv	B	ben-che	che	che

I	ig	hh	iv	ie	in	it	ii	ia	ir	im	id	ix	ib	ic	if
	ac	ec	ic	oc	vc	C	ca	ce	ci	co	cv	Ch	cosa	como	della

L	lf	lg	lh	lv	le	ln	lt	li	la	lr	lm	ld	lx	lb	lc
	ad	ed	id	od	vd	D	da	de	di	do	dv	D	debba	detto	doppo

V	vc	vf	vg	vh	vv	ve	vn	vt	vi	va	vr	vm	vd	vx	vb
	ae	ee	ie	oe	ve	**E**	ea	ee	ei	eo	ev	**E**	esso	essendo	essere

S	sb	sc	sf	sg	sh	sv	se	sn	st	si	sa	sr	sm	sd	sx
	af	ef	if	of	vf	**F**	fa	fe	fi	fo	fv	**F**	forsi	fvssi	finche

A	ax	ab	ac	af	ag	ah	av	ae	an	at	ai	aa	ar	am	ad
	ag	eg	ig	og	vg	**G**	ga	ge	gi	go	gv	**G**	gratia	grave	grato

B	bd	bx	bb	bc	bf	bg	bh	bv	be	bn	bt	bi	ba	br	bm
	ah	eh	ih	oh	vh	**H**	ha	he	hi	ho	hv	**H**	abiamo	avvto	hanno

C	cm	cd	cx	cb	cc	cf	cg	ch	cv	ce	cn	ct	ci	ca	cr
	ai	ei	ii	oi	vi	**I**	ia	ie	ii	io	iv	**I**	imperio	impo	imperoche

D	dr	dm	dd	dx	db	dc	df	dg	dh	dv	de	dn	dt	di	da
	al	el	il	ol	vl	**L**	la	le	li	lo	lv	**L**	leqvali	liqvali	lettera

E	ea	er	em	ed	ex	eb	ec	ef	eg	eh	ev	ee	en	et	Ei
	am	em	im	om	vm	**M**	ma	me	mi	mo	mv	**M**	molto	modo	mondo

F	fi	fa	fr	fm	fd	fx	fb	fc	ff	fg	fh	fv	fe	fn	ft
	an	en	in	on	vn	**N**	na	ne	ni	no	nv	**N**	non	nostra	nella

G	gt	gi	ga	gr	gm	gd	gx	gb	gc	gf	gg	gh	gv	ge	gn
	ao	eo	io	oo	vo	**O**	oa	oe	oi	oo	ov	**O**	oltra	ogni	ogni-cosa

M	mn	mt	mi	ma	mr	mm	md	mx	mb	mc	mf	mg	mh	mv	me
	ap	ep	ip	op	vp	**P**	pa	pe	pi	po	pv	**P**	per	per	per-che

N	ne	nn	nt	ni	na	nr	nm	nd	nx	nb	nc	nf	ng	nh	nv
	aq	eq	iq	oq	vq	**Q**	st	st	st	st	qv	**Q**	qvali	qvella	qvesta

O	ov	oe	on	ot	oi	oa	or	om	od	ox	ob	oc	of	og	oh
	ar	er	ir	or	vr	**R**	ra	re	ri	ro	rv	**R**	qvan-to	qvan-do	qval-che

Q	qh	qv	qe	qn	qt	qi	qa	qr	qm	qd	qx	qb	qc	qf	qg
	as	es	is	os	vs	**S**	sa	se	si	so	sv	**S**	signor	signo-ria	scritto

R	rg	rh	rv	re	rn	rt	ri	ra	rr	rm	rd	rx	rb	rc	rf
	at	et	it	ot	vt	**T**	ta	te	ti	to	tv	**T**	scris-se	tvtto	tanto

T	tf	tg	th	tv	te	tn	tt	ti	ta	tr	tm	td	tx	tb	tc
	av	ev	iv	ov	vv	**V**	va	ve	vi	vo	vv	**V**	vostro	vero	vna

X	xc	xf	xg	xh	xv	xe	xn	xt	xi	xa	xr	xm	xd	xx	xb
	br	dr	gn	lt	nq	**X**	pr	rl	rp	rt	st	**X**	Vostra Sig.	le vostre lettere	qvanto pi presto

Y	yb	yc	yf	yg	yh	yv	ye	yn	yt	yi	ya	yr	ym	yd	yx
	ch	fr	gr	mn	nt	**Y**	rc	rm	rs	sc	tr	**Y**	il Signor Iddio	le cose passano	me racomando

Z	zx	zb	zc	zf	zg	zh	zv	ze	zn	zt	zi	za	zr	zm	zd
	cr	gl	lm	nc	pn	**Z**	rd	rn	rt	sp	tr	**Z**	habiamo recevvte	havemo spiacer	fatime raccom.

. A questo punto possiamo immaginare di avere 4 ruote alfabetiche. Dal loro "movimento", sarà possibile comprendere meglio la disposizione finale della tabella. Bellaso scrive che *doi soli alfabeti si mutano mutando la cifra*. Disponiamo a guisa di strisce i 4 alfabeti e collochiamoli uno sopra l'altro, in questo modo:

. Nun oni povas imagi havi kvar alfabetajn radojn. De la ilia "movo" eblos kompreni pli bone la fina aranĝo de la tabelo. Bellaso skribas ke *doi soli alfabeti si mutano mutando la cifra*. Oni habas kiel linioj la kvar alfabetojn, kaj oni lokas ilin iu sur alia, ĉi tiel:

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

. Se confrontiamo la loro disposizione con la tabella polialfabetica

. Se oni komparas la ilian aranĝon kun la polialfabeta tabelo uzita

utilizzata per questo metodo di cifratura, possiamo vedere che la prima colonna VPAA è sufficiente per la formazione della prima riga della tabella. Nella prima casella superiore, infatti, l'incrocio fra la P dell'alfabeto di PHILIPPVS (seconda striscia) e la V dell'alfabeto di VENETIARUM DUX (prima striscia) genera la coppia PV evidenziata in rosso,

por ĉi tiu metodo, oni povas vidi ke la unua kolumno VPAA estas sufiĉa por formi la unuan linion de la tabelo. Fakte, en la unua supera ĉelo la kruciĝo inter la P de la PHILIPPVS alfabeto (dua linio) kaj la V de la VENETIARVM DUX alfabeto (unua linio) generas la paron PV, rimarkigita ruĝe,

P	**pv**	pe	pn	pt	pi	pa	pr	pm	pd	px	pb	pc	pf	pg	ph
	aa	ea	ia	oa	va	A	aa	ae	ai	ao	av	A	accio	altra	ancora

, mentre nella prima casella inferiore l'incontro fra la A del primo alfabeto intermedio e la A del secondo alfabeto intermedio generano la coppia AA, evidenziata in rosso nella tabella sottostante:

, dume en la unua suba ĉelo la kruciĝo inter la A de la unua meza alfabeto kaj la A de la dua generas la paron AA, rimarkigita ruĝe en la tuisuba tabelo:

P	pv	pe	pn	pt	pi	pa	pr	pm	pd	px	pb	pc	pf	pg	ph
	aa	ea	ia	oa	va	A	aa	ae	ai	ao	av	A	accio	altra	ancora

. Da questo esempio appare chiaro che il sistema polialfabetico è strutturato su coppie di lettere derivanti dalla corrispondenza fra le lettere delle prime due strisce alfabetiche e dalla corrispondenza fra le lettere delle altre due. È dunque necessario individuare quali di queste 4 strisce si "muovono" per generare il complesso sistema di tabelle del quarto metodo. Immaginiamo adesso che la prima striscia si muova come una ruota in senso inverso, per cui dalla prima lettera V si passi successivamente all'ultima, la H, e via via con la G, la F, ecc..., e che delle due strisce di alfabeti intermedi si muova soltanto l'ultima. Il risultato darà quindi luogo alle seguenti corrispondenze, che evidenzieremo in rosso:

. De ĉi tiu ekzemplo evidentas ke la polialfabeta sistemo strukturiĝas sur paroj da literoj, derivataj de la respondo inter la literoj de la unuaj alfabetaj linioj kaj de la respondo inter la literoj de la aliaj du. Kaj do necesas lokaligi kiuj linioj "moviĝas" por generi la kompleksan sistemon de tabeloj de la kvara metodo. Oni imagas nun ke la unua linio moviĝas kiel rado laŭ inversa senco, per kiu ekde la unua litero V oni pasas poste al la lasta, la H, kaj tiel plu kun la G, la F, ..., kaj ke de la du linioj de la mezaj alfabetoj moviĝas nur la lasta. La rezulto generos do la sekvantajn respondojn, kiujn oni rimarkigas ruĝe:

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

. Anche in questo caso, come nel precedente, dal confronto della prima colonna GPAB con la seconda tabella contrassegnata dalla lettera H possiamo verificare la correttezza del sistema pensato da Bellaso. Nella prima casella superiore, infatti, troviamo la coppia di lettere HH, mentre nella prima casella inferiore troviamo la coppia AB.

. Eĉ en tiu ĉi kazo, kiel en la antaŭa, ekde la komparo de la unua kolumno GPAB kun la dua tabelo markita per la litero H oni povas konstati la ĝustecon de la sistemo pripensita de Bellaso. En la unua supera ĉefo, fakte, oni eltrovas la paron de literoj HH, dume en la unua suba ĉefo oni eltrovas la paron AB.

H	hh	hv	he	hn	ht	hi	ha	hr	hm	hd	hx	hb	hc	hf	hg
	ab	eb	ib	ob	vb	B	ba	be	bi	bo	bv	B	ben-che	che	che

. Procedendo nella medesima direzione, si arriva alla definizione, almeno per la riga superiore di ogni singola tabella, di tutto il sistema polialfabetico congeniato per il quarto metodo. La riga inferiore, dal canto suo, data l'associazione dell'alfabeto generato da PHILIPPVS con i due alfabeti intermedi A...Z, si organizza con: l'accoppiamento delle vocali con la lettera associata (nel caso della seconda tabella qui sopra, contrassegnata dalla H, l'accoppiamento sarà con la B, appunto la seconda lettera dell'alfabeto A...Z); la lettera associata in sesta posizione (torna il motivo dell'intervallo di cinque posizioni, complice il fatto che le vocali dell'alfabeto latino sono appunto 5); il rovesciamento delle prime 5 caselle di coppie, ossia l'accoppiamento della lettera associata con le 5 vocali; di nuovo la lettera associata, da sola, in dodicesima posizione; tre parole

. Pluirante en la saman sencon, oni alvenas al la difino, almenaŭ por la supera linio de ĉiu unuopa ĉefo, de tuta polialfabeta sistemo elpensita por la kvara metodo. La suba linio, siavice, ĉar la alfabeto generita de PHILIPPVS rezultas asociita kun la du mezaj alfabetoj A...Z, organiziĝas tiele: la parigo de la vokaloj kun la litero asociita (en la kazo de la dua tabelo ĉi tie supre, markita per la H, la parigo estas kun la B, precize la dua litero de la alfabeto A...Z); la litero asociita en la sesa pozicio (revenas la motivo de la 5-pozicia intervalo, ankaŭ ĉar la vokaloj en la latina alfabeto estas precize kvin); la renversiĝo de la unuaj kvin ĉefoj de paroj, tio estas la parigo de la litero asociita kun la kvin vokaloj; de nove la litero asociita sole, en la dekdua pozicio; tri vortoj ordinare uzataj, kiuj havas kiel ĉeflitero la literon asociitan de la mezaj alfabetoj A...Z (ekzemple en la kazo

di uso comune, che abbiano come iniziale la lettera associata degli alfabeti intermedi A...Z (per es., nel caso della prima tabella associata alla lettera A, le tre parole sono accio, altra e ancora). Detto ciò, in verità il sistema "scricchiola" a causa di alcune eccezioni, che lo rendono poco funzionale alla possibilità di costruirlo dalle due parole chiave PHILIPPVS e VENETIARVM DUX. Evidenziamo in rosso le cosiddette eccezioni:

de la unua tabelo asociita al la litero A, la tri vortoj estas *accio*, *altra* kaj *ancora*). Tion dirite, vere la sistemo "knaras" pro kelkaj esceptoj, kiuj iĝas ĝin malbone funkcia por la eblo konstrui ekde la du ŝlosilvortoj PHILIPPVS kaj VENETIARVM DUX. Ni rimarkigu ruĝe la tiel nomatajn esceptojn:

P	pv	pe	pn	pt	pi	pa	pr	pm	pd	px	pb	pc	pf	pg	ph
	aa	ea	ia	oa	va	A	aa	ae	ai	ao	av	A	accio	altra	ancora

H	hh	hv	he	hn	ht	hi	ha	hr	hm	hd	hx	hb	hc	hf	hg
	ab	eb	ib	ob	vb	B	ba	be	bi	bo	bv	B	benche	che	che

I	ig	hh	iv	ie	in	it	ii	ia	ir	im	id	ix	ib	ic	if
	ac	ec	ic	oc	vc	C	ca	ce	ci	co	cv	**Ch**	cosa	como	**della**

L	lf	lg	lh	lv	le	ln	lt	li	la	lr	lm	ld	lx	lb	lc
	ad	ed	id	od	vd	D	da	de	di	do	dv	D	debba	detto	doppo

V	vc	vf	vg	vh	vv	ve	vn	vt	vi	va	vr	vm	vd	vx	vb
	ae	ee	ie	oe	ve	E	ea	ee	ei	eo	ev	E	esso	essendo	essere

S	sb	sc	sf	sg	sh	sv	se	sn	st	si	sa	sr	sm	sd	sx
	af	ef	if	of	vf	F	fa	fe	fi	fo	fv	F	forsi	fvssi	finche

A	ax	ab	ac	af	ag	ah	av	ae	an	at	ai	aa	ar	am	ad
	ag	eg	ig	og	vg	G	ga	ge	gi	go	gv	G	gratia	grave	grato

B	bd	bx	bb	bc	bf	bg	bh	bv	be	bn	bt	bi	ba	br	bm
	ah	eh	ih	oh	vh	H	ha	he	hi	ho	hv	H	abia-mo	avvto	hanno

C	cm	cd	cx	cb	cc	cf	cg	ch	cv	ce	cn	ct	ci	ca	cr
	ai	ei	ii	oi	vi	I	ia	ie	ii	io	iv	I	impe-rio	impo	impe-roche

D	dr	dm	dd	dx	db	dc	df	dg	dh	dv	de	dn	dt	di	da
	al	el	il	ol	vl	L	la	le	li	lo	lv	L	leqva-li	liqva-li	lettera

E	ea	er	em	ed	ex	eb	ec	ef	eg	eh	ev	ee	en	et	Ei
	am	em	im	om	vm	M	ma	me	mi	mo	mv	M	molto	modo	mon-do

F	fi	fa	fr	fm	fd	fx	fb	fc	ff	fg	fh	fv	fe	fn	ft
	an	en	in	on	vn	N	na	ne	ni	no	nv	N	non	nostra	nella

G	gt	gi	ga	gr	gm	gd	gx	gb	gc	gf	gg	gh	gv	ge	gn
	ao	eo	io	oo	vo	O	oa	oe	oi	oo	ov	O	oltra	ogni	ogni-cosa

M	mn	mt	mi	ma	mr	mm	md	mx	mb	mc	mf	mg	mh	mv	me
	ap	ep	ip	op	vp	P	pa	pe	pi	po	pv	P	per	per	per-che

N	ne	nn	nt	ni	na	nr	nm	nd	nx	nb	nc	nf	ng	nh	nv
	aq	eq	iq	oq	vq	Q	**st**	**st**	**st**	**st**	qv	Q	qvali	qvella	qvesta

O	ov	oe	on	ot	oi	oa	or	om	od	ox	ob	oc	of	og	oh
	ar	er	ir	or	vr	R	ra	re	ri	ro	rv	R	**qvan-to**	**qvan-do**	**qval-che**

Q	qh	qv	qe	qn	qt	qi	qa	qr	qm	qd	qx	qb	qc	qf	qg
	as	es	is	os	vs	S	sa	se	si	so	sv	S	signor	signo -ria	scritto

R	rg	rh	rv	re	rn	rt	ri	ra	rr	rm	rd	rx	rb	rc	rf
	at	et	it	ot	vt	T	ta	te	ti	to	tv	T	**scris- se**	tvtto	tanto

T	tf	tg	th	tv	te	tn	tt	ti	ta	tr	tm	td	tx	tb	tc
	av	ev	iv	ov	vv	V	va	ve	vi	vo	vv	V	vostro	vero	vna

X	xc	xf	xg	xh	xv	xe	xn	xt	xi	xa	xr	xm	xd	xx	xb
	br	**dr**	**gn**	**lt**	**nq**	X	**pr**	**rl**	**rp**	**rt**	**st**	X	Vostra Sig.	le vo- stre let- tere	qvan- to più pre- sto

Y	yb	yc	yf	yg	yh	yv	ye	yn	yt	yi	ya	yr	ym	yd	yx
	ch	**fr**	**gr**	**mn**	**nt**	Y	**rc**	**rm**	**rs**	**sc**	**tr**	Y	il Si- gnor Iddio	le cose pas- sano	me raco- mando

Z	zx	zb	zc	zf	zg	zh	zv	ze	zn	zt	zi	za	zr	zm	zd
	cr	**gl**	**lm**	**nc**	**pn**	Z	**rd**	**rn**	**rt**	**sp**	**tr**	Z	ha-biamo rece-vvte	have-mo spia-cer	fati-me rac-com.

. Aldilà della coppia *Ch* (in luogo di *C*) nella dodicesima casella della terza tavola contrassegnata dalla lettera I, e delle quattro coppie st della tavola contrassegnata da N, che prendono il posto di *qa, qe, qi, qo*, le altre eccezioni sono da registrare nei due *che* della seconda tavola (con lettera associata B), nella parola *della* in terza tavola (con lettera associata C), nei *quanto, quando, qualche* della tavola contrassegnata da O, nello *scrisse* della tavola R e nelle righe inferiori (a parte, si intende, le lettere associate) delle ultime tre tavole X, Y e Z, la struttura logica delle quali, ammesso che esista, pare lontana dall'umana comprensione per ciò che riguarda la loro disposizione, mentre trova più di un buon motivo nella necessità di cifrare coppie di consonanti, che altrimenti, a parte *st*, non sarebbero presenti nelle tavole. Nel caso delle *dittioni* e delle espressioni ritenute di uso comune, invece, una ragione deve essere individuata nel maggior numero, per es., di parole che inziano per *q* o per *s*. La medesima spiegazione potrebbe del resto essere utilizzata nel caso dei quattro st della tabella N, vista la frequenza della coppia di lettere sia nella lingua latina che in quella italiana. Per quanto riguarda la cifratura, vero rebus delle tavole del quinto metodo, Bellaso spiega che *se mira la consonante, compagnata con la vocale allo alfabeto secondo de maiuscole, et se scrive le due lettere che stanno sopra, et a cifrar doi consonanti, si mira nel fine della cifra se vi sono, et a cifrar una dittione, se mira nelle dittioni, et a cifrar una lettera sola, se scrive doi lettere de quelle che stanno sopra le lettere maiuscole de li doi alfabeti di meggio*. Vediamo quale esempio ci suggerisce l'autore. Immaginiamo che il messaggio da

. Krom la paro *Ch* (anstataŭ *C*) en la dekdua ĉelo de la tria tabelo markita per la litero I, kaj krom la kvar paroj *st* de la tabelo markita per N, kiuj okupas la lokojn de *qa*, *qe*, *qi*, *qo*, la aliaj esceptoj estas situigendaj en la du *che* de la dua tabelo (kun asociita litero B), en la vorto *della* en la tria tabelo (kun asociita litero C), en la vortoj *quanto*, *quando*, *qualche* en la tabelo markita per O, en la *scrisse* de la tabelo R, kaj en la subaj linioj (aparte, kompreneble, la asociitaj literoj) de la lastaj triaj tabuloj X, Y kaj Z, kies logika strukturo, se ĝi ekzistas, ŝajnas malproksima de la homa kompreno pri ilia aranĝo, dume ĝi trovas pli bonajn motivojn en la neceso ĉifri parojn da konsonantoj, kiuj alie, aparte *st*, ne ĉeestus en la tabeloj. Sed, en la kazo de la *dittioni* kaj de la esprimoj konsideritaj ordinare uzataj, la motivo devas esti determinata en la pli granda nombro, ekzemple, de vortoj kiuj komencas per *q* aŭ *s*. La sama klarigo povas esti eĉ uzita en la kazo de la kvar *st* de la tabelo N, pro la ofteco de la literoparo kaj en la latina kaj en la itala lingvo. Koncernante la ĉifradon, la vera rebuso de la tabeloj de la kvina metodo, Bellaso klarigas ke *se mira la consonante, compagnata con la vocale allo alfabeto secondo de maiuscole, et se scrive le due lettere che stanno sopra, et a cifrar doi consonanti, si mira nel fine della cifra se vi sono, et a cifrar una dittione, se mira nelle dittioni, et a cifrar una lettera sola, se scrive doi lettere de quelle che stanno sopra le lettere maiuscole de li doi alfabeti di meggio*. Oni vidas kiun ekzemplon la aŭtoro sugestas. Ni imagu ke la ĉifrenda mesaĝo estas

cifrare sia

le vostre lettere me sono state molto agrate

. La soluzione proposta da Bellaso, non senza un certo stupore, è il codice

. La solvo proponita de Bellaso, ne sen ia surprizo, estas la kodo

xxdaefqdfg nxrgum enaxorra

, dove *xx* sta per *le vostre lettere*, *da* per *lettera, ef* per *me, qd* per *so* e *fg* per *no*. E così via, sino a formare la frase della *minuta*. Tutto corretto, o quasi, perché Bellaso non ci rivela il motivo per cui, dopo aver cifrato l'espressione *le vostre lettere* con *xx*, debba rafforzare il concetto e cifrare *lettera* (che nel messaggio non compare) con *da*. Vezzi da cifratore professionista? Difficile affermarlo con certezza. Lasciamo all'autore l'onore di concludere: *le sette lettere infrascritte* [i sette metodi], *sono scritte fedelmente, secondo li precetti insegnati, nelle quali si contengono alcune belle, et curiose cose di sapere, et questo per dare occasione à valenti, et ingeniosi cifratori, di affaticarsi per caverle, massime à quelli liquali fanno professione di cavare ogni sorte de cifre. Il che se è la verità, come molti lo credono, non sarà loro difficile à cavar queste, sapendo tutti li precetti, con liquali sono scritte, essendo li modi di cifrare, se può dire numero infinito. Et doppoi che essi si saranno affaticati un'anno, ogni Principe potrà da me havere le dittioni, con le quali sono composti gli alfabeti, per poter leggere dette cifre, acciò conoscano essere scritte fedelmente, secondo li precetti insegnati.*

, kie *xx* kongruas al *le vostre lettere*, *da* kongruas al *lettera*, *ef* kongruas al *me*, *qd* kongruas al *so*, kaj *fg* kongruas al *no*. Kaj tiel plu, ĝis formi la frazon *minuta*. Ĉion korektite, aŭ preskaŭ, ĉar Bellaso ne klarigas la kaŭzon pro kiu, postkiam la esprimo *le vostre lettere* estis ĉifrita per *xx*, li devas plifortigi la koncepton kaj ĉifri *lettera* (kiu en la mesaĝo ne aperas) per *da*. Ĉu kaĵoloj de eksperta ĉifristo? Estas malsimple aserti ĝin certe. Ni lasas al la aŭtoro la honoron konkludi: *le sette lettere infrascritte* [la sep metodoj]*sono scritte fedelmente, secondo li precetti insegnati, nelle quali si contengono alcune belle, et curiose cose di sapere, et questo per dare occasione à valenti, et ingeniosi cifratori, di affaticarsi per caverle, massime à quelli liquali fanno professione di cavare ogni sorte de cifre. Il che se è la verità, come molti lo credono, non sarà loro difficile à cavar queste, sapendo tutti li precetti, con liquali sono scritte, essendo li modi di cifrare, se può dire numero infinito. Et doppoi che essi si saranno affaticati un'anno, ogni Principe potrà da me havere le dittioni, con le quali sono composti gli alfabeti, per poter leggere dette cifre, acciò conoscano essere scritte fedelmente, secondo li precetti insegnati.*

Note / Notoj

[1]Cfr. A. Petrucci, DBI.
[2]Cfr. A. Buonafalce, *Giovan Battista Bellaso e le sue cifre polialfabetiche*, Lerici 1997.
[3]Cfr. L. B. Alberti, *Dello scrivere in cifra*, a cura di A. Buonafalce, Galimberti, Torino 1994.
[4]*Traicté des chiffres ou Secrètes manières d' écrire*, 1586.
[5]*De Furtivis Literarum Notis*, 1563.
[6]Oni vidu A. Patrucci, DBI.
[7]Oni vidu A. Buonafalce, *Giovan Battista Bellaso e le sue cifre polialfabetiche*, Lerici 1997
[8]Oni vidu L. B. Alberti, *Dello scrivere in cifra*, a cura di A. Buonafalce, Galimberti, Torino 1994.
[9]*Traict des chiffres ou Secrtes manires d' crire*, 1586.
[10]*De Furtivis Literarum Notis*, 1563.
[11]Il riferimento va inteso limitatamente alla copia che ho avuto modo di consultare presso la Biblioteca dell'Università Cattolica del Sacro Cuore di Milano.
[12]Oni volas rilati nur al la kopio kiun mi konsultis ĉe la Biblioteko de la Katolika Universitato de la Sankta Koro de Milano.
[13]Anche in questo caso vale limitatamente al volume conservato presso la Biblioteca dell'Università Cattolica del Sacro Cuore di Milano.
[14]Ankaŭ en ĉi tiu kazo mi rilatas nur al la kopio ĉe la Biblioteko de la Katolika Universitato de la Sankta Koro de Milano.
[15]Bellaso lo chiama*quinto*perché viene esposto come corollario della terza variante del secondo metodo.
[16]Bellaso nomas lin *kvina* ĉar li estas prezentita kiel korolario de la tria varianto de la dua metodo.

A proposito dell'autore / Pri la aŭtoro

Indirizzo di riferimento / Kontaktadreso

Massimo Rizzardini
Università degli Studi di Milano, Italia
Facoltà di Lettere e Filosofia
Dipartimento di Filosofia
Via Festa del Perdono 7
20122 - Milano - Italia
Email / Retadreso: massimo.rizzardini@unimi.it.

Copyright