Interlingvistikaj Kajeroj

Articles | *Articoli* | *Artikoloj* 8 febbraio 2011

L'arte occulta della cifra: la crittografia moderna di Leon Battista Alberti

La kaŝita arto de la ĉifro: la moderna kriptografio de Leon Battista Alberti

Massimo Rizzardini

Tradukis Elena Marazzi

InKoj. Interlingvistikaj Kajeroj 2:1 (2011), 1–25 ISSN 2037-4550
http://riviste.unimi.it/index.php/inkoj/

ABSTRACT Attraverso l'analisi del cosiddetto sistema di cifratura polialfabetica, il saggio intende portare un ulteriore contributo alla questione storiografica che riguarda le origini della crittografia moderna. Composto fra il 1466 e il 1467, il *De componendis cyfris* di Leon Battista Alberti, emblema del genio rinascimentale, segna l'avvento del primo metodo razionale per l'oscuramento dei messaggi in chiaro e per la loro protezione dai tentativi illegittimi di decrittazione.

RESUMO Per la analizo de la tiel nomata polialfabeta ĉifradosistemo, la eseo intencas prezenti pluan kontribuon pri la historiografia demando rilatanta la originojn de la moderna kriptografio. Komponita inter 1466 kaj 1467, la *De componendis cyfris* de Leon Battista Alberti, emblemo de la renesanca genio, markas la alvenon de la unua racia metodo por la obskurigo de mesaĝoj kaj por sia protekto kontraŭ nelicaj provoj de elkodigo.

InKoj. Interlingvistikaj Kajeroj 2:1 (2011), 1–25 ISSN 2037-4550
http://riviste.unimi.it/index.php/inkoj/

Nel primo numero dell'*Emporio di utili cognizioni* del 1835 sono descritte otto diverse ricette per la preparazione degli inchiostri simpatici, "i cui caratteri appariscono alla luce" e stupiscono il destinatario del messaggio segreto, con tinte che vanno dal turchino al porporino, dal roseo al dorato [1]. Il fluido magico, che veniva presentato nella sezione dedicata alle arti e ai mestieri, ma che con ogni probabilità doveva essere impiegato con maggior frequenza nei giochi di prestigio o in attività ludiche, occultava i caratteri con il suo raffreddamento e li faceva riapparire non appena scaldato dal fuoco. L'Ottocento è ancora un secolo ingenuo e l'editoria popolare non perde una sola pagina per ricordarcelo. Una ricetta non dissimile, ma precedente di tre secoli, la si poteva leggere in uno dei libri di segreti per signore più diffusi del Rinascimento. La sua misteriosa autrice, Isabella Cortese, che lo mandò alle stampe nel 1561, donava ai suoi lettori avidi di *Secreti* – come l'opera era intitolata – *la ricetta per l'inchiostro che in quaranta dì sparisce e non si vede*:

En la antaŭa numero de la *Emporio di utili cognizioni*, eldonita en 1835, estas priskribitaj ok malsana recepto por pretigi nevideblaj inkoj, "kiuj literoj aperas per lumo" kaj mirigas la adresiton de la sekreta mesaĝo, kun tinkturoj kiuj estas intense lazuraj, purpuraj, rozaj kaj orkoloraj [2]. La sorĉa fluidaĵo, kiu estis prezentita en la sekcio dedicita al la artoj kaj metioj, sed kiu probable devis esti utiligita pli ofte en prestidigitaĵoj kai ludaktivadoj, kaŝis la literojn por sia malvarmigo kaj igis ilin reaperi tuj kiam varmigita per fajro. La deknaŭa jarcento estas ankoraŭ naiva jarcento kaj la popola eldonarto ne preterlasas pago memorigi al ni. Ne malsimilan rezepton, sed antaŭan tri jarcente, oni povis legi en unu el pli disvastiĝinta libro de sekretoj por damoj de la Renesanco. Ĝia mistera aŭtoro, Isabella Cortese, kiu lin eldonis 1561, donis al la siaj legantoj, avidaj de *Secreti* - kiel la verko estis titolita - *la rezepton por la inko kiu en kvardek tagoj malapenas kaj ne oni vidas*:

> piglia acqua forte da partire et in quella fa bollire la galla poi il vitriolo, poi mettigli tanto sale armoniaco quanto nell'acqua si potrà risolvere, e poi metti la gomma arabica dentro, e questo inchiostro farà l'effetto sopradetto. [3]

L'inchiostro di Cortese resistette più a lungo e il suo compendio di trucchi e bizzarrie conobbe la bellezza di una ventina di edizioni, comprese due in lingua tedesca e altrettante di recente pubblicazione. Nella seconda metà del Cinquecento fu un vero e proprio best seller e nella sola Venezia circolò con passione fra le delicate mani delle gentildonne e fra quelle callose degli artigiani. L'inchiostro poi era tema molto frequentato nella letteratura popolare e in quella dei manuali tecnici, che sostituivano su carta il tradizionale apprendistato in bottega. Eppure, molti anni prima, furono proprio

La inko de Cortese rezistis pli longe kaj sia kompendio de artifikoj kaj stangaĵoj akiris eĉ proksimume dudeko eldonoj, enkalkulitaj du eldonoj en la germana lingvo kaj samnobraj antaŭ ne longe eldonataj. En la dua duono de la dekseca jarcento ĝi estis vera furorverko kaj en la sola Venecio cirkulis fervorege en la delikataj manoj de la damoj kaj en tiuj kalaj de la metiistoj. La inko estis krome tre pridiskutata en la popola literaturo kai en tiu de specifaj manlibroj, kiuj antastaŭis papere la tradician metilernadon en butiko. Kaj tamen, multajn jarojn antaŭe, rezeptoj kiel tiu de la "dumtempa" inko iĝis

ricette come quella dell'inchiostro "a tempo" a diventare bersaglio di produzioni intellettuali dalla circolazione più elitaria. In uno di questi, il suo autore giudicava espedienti inefficaci (*inepta*) le scritture fatte con il latte, il succo di cipolla, acidi distillati e in generale tutti quegli stratagemmi per cui il messaggio oscurato veniva schiarito attraverso il ricorso a fonti di calore, raggi solari o acque di alchemica lavorazione. Lo stesso autore ricordava velocemente altre soluzioni tipiche dell'età rinascimentale e di epoche più remote, come quella dell'uomo rasato sul quale veniva scritto un messaggio in chiaro oscurato, di lì a poco, dalla ricrescita: in questo caso, più che un decrittatore, era necessario un barbiere. Se in tre secoli la crittografia popolare non aveva compiuto passi da gigante, va detto che all'epoca della Cortese lo strumento più utilizzato dai professionisti era chiamato nomenclatore e consisteva in un repertorio di nomi e parole con il codice corrispondente, che da un lato abbreviava il testo cifrato e dall'altro rendeva molto difficile l'intercettazione delle spie.

A Venezia, dove Cortese – ammesso che mai fosse esistita[4] - pubblicò il suo volume, a Firenze, a Milano e in molte altre città d'Italia i servizi segreti ricorrevano di frequente all'uso dei nomenclatori per trasmettere messaggi oscurati e proteggere il *secreto*. Il vero difetto di questi sistemi di cifratura, che si basavano costantemente sul principio della sostituzione monoalfabetica, era che aldilà dell'inserimento di segni *nulli* per dividere le parole o dell'utilizzo di più *omofoni* (lettere o segni di fantasia che identificano una lettera in chiaro: es. la *f*, la *g*, il 9 e il *k* possono, tutti quanti, criptare la *m*), una volta caduti nelle mani di esperti professionisti denunciavano limiti di protezione che nella prima modernità difficilmente erano compresi come tali. Limiti che non sfuggirono all'analisi dell'autore di cui si è riportata la severa critica alle "stramberie" del fantastico

mokceloj de intelektaj verkoj kiuj havis pli elitan disvastiĝon. En unu el ĉi tiuj la aŭtoro juĝis senefikajn artifikojn (*inepta*) la skribojn faritajn per lakto, soko de cepo, distilitaj acidoj kaj entute la artifikoj per kiuj la kaŝita mesaĝo estis heligita per varmofonto, sunradioj kaj akvoj distilitaj alkemie. La sama aŭtoro rapide memoris aliajn solvojn specifajn de la Renesanco kaj de pli foraj epokoj, kiel tiu de la razita viro, sur kiu oni scribi klare mesaĝon obskurigitan en mallonga tempo de la rekresko; tiukaze, oni necesis eĉ ne ĉifristo, sed barbiro. Se en tri jarcentoj la popola kriptografio ne plenumis gigantajn paŝojn, oni devas diri ke en la epoko de la Cortese la instrumento pli uzata de profesiuloj estis nomita nomenklatiro kaj konsistis en tabulo de nomoj kaj vortoj kun la asociitaj kodoj, kiuj de unu flanko mallongigis la ĉifritan mesaĝon, de la alia flanko igis malfacilan la interkapton de spionoj.

En Venecio, ke Cortese - supozante ke ŝi iam ekzistis - eldonis sian verkon, en Florenco, en Milano, kaj en moltaj aliaj urboj de Italujo, la sekretaj deĵoroj ofte ekuzis al la uzo de numenklatiroj por transdoni ĉifritajn mesaĝojn kaj protekti la *sekreton*. La vera defekto de tiuj metodoj de ĉifrado, kiuj bazis daŭre sur la principo de unualfabeta antastaŭigo, estis ke transe la enigo de *nulaj* signoj por dividi la vortojn kaj transe la uzo de pli *omofonoj* (literoj aŭ inventitaj signoj kiuj identici klaran literon, por ekzemplo *f*, *g*, *9* kaj *k* povas ĉiuj ĉifras *m*), se ĝi falis en manoj de spertaj profesiuloj elmontris protektadolimojn kiuj en la frua moderneco ne estis komprenitaj kiel tiaj. Limoj kiuj ne preterantentis al la analizo de la aŭtoro, kies estis raportita la severa kritiko al la "strangaĵoj" de mirindeco kaj al la solvoj naskitaj de la kunfuza popola praktiko. Tiu aŭtoro nomiĝis

e alle soluzioni nate dalla confusa pratica popolare. Quell'autore rispondeva al nome di Leon Battista Alberti e la sua fama lo precede oggi come lo precedeva un tempo. Fu in una passeggiata nei giardini vaticani con l'amico Leonardo Dati, allora segretario apostolico di papa Paolo II, che l'Alberti ebbe modo di conoscere, forse per la prima volta, l'intricato mondo delle corrispondenze segrete e dei messaggi cifrati. Non è l'inizio di un moderno romanzo di spionaggio, ma l'incipit del *De componendis cyfris* o *De cyfris*, opera composta verosimilmente fra il 1466 e il 1467[5], le cui ragioni sono ben espresse in questo rapido scambio di battute:

> "Tu, invero – disse guardandomi il Dati – da sempre impegnato a investigare le arti occulte e ad indagare nei misteri della natura, che pensi di questi, se possiamo chiamarli così, interpreti di cifre e rivelatori di segreti? Ti sei occupato forse della questione? Hai competenza in materia?"
> Io allora sorrisi e dissi: "È probabile che tu, come primo segretario del Pontefice, debba qualche volta servirti della scrittura cifrata nel trattare quegli affari politici che intendi mantenere nella massima segretezza".
> "È vero - rispose il Dati – e non mi spiacerebbe, in conformità del mio ruolo, potermela sbrigare da solo, senza dover ricorrere a un estraneo che sia esperto di linguaggi cifrati. Succede che talvolta vengano intercettati dalle spie e giungano sulle nostre scrivanie dei messaggi in cifra che ci pare meritino una certa attenzione. Se quindi hai scoperto qualcosa al riguardo, ti prego di farmene parte".[7]

Le fonti tacciono su un interesse dell'Alberti per la crittografia precedente alla sua conversazione con il Dati. Secondo Grayson[8] il *De cyfris* sarebbe stato composto con le *Institutiones Gramaticae* di Prisciano di Cesarea a portata di consultazione: lo testimonierebbero alcuni esempi particolari e altre osservazioni, come quella riguardante l'equivalenza di K e Q con la C velare, ecc.., ma è allo studioso di crittografia Augusto Buonafalce che si deve rendere merito di un attento esame storiografico e filologico[9]. Buonafalce si è occupato a lungo sia della cifra polialfabetica dell'Alberti che di quella, successiva, di Giovan Battista Bellaso[10], anch'egli operante nell'ambito vaticano ma con ogni probabilità all'oscuro del De cyfris. In effet-

Leon Battista Alberti, kaj sia famo antaŭas li hodiaŭ kiel tiam. En promeno en la vatikana ĝiardenoj kun la amiko Leonardo Dati, kiu estis tiam la apostola segretario de la papo Paolo II, Alberti ekkonis, eble unuafoje, la komplikan mondon de la sekretaj korespondajoj kaj ĉifritaj mesaĝoj. ĉi tiu ne estis la komenco de moderna spionromano, sed la komenca vorto de la *De componendis cyfris* aŭ *De cyfris*, verko komponita verŝajne inter 1466 kaj 1467[6], kies la motivoj estis bone diritaj en ĉi tiu interŝanĝo de frano:

La fontoj silentas pri intereso de Alberti por la kriptografio antaŭe al la interparolo kun Dati. Laŭ Greyson[12], la *De cyfris* estus kunmetita kun la *Institutiones Gramaticae* de Prisciano de Cesarea je dispono: tion atestus kelkaj specialaj ekzemploj kaj aliaj rimarkoj, kiel tiu koncernanta la samvalorecon de K kaj Q kun la velara C, k.t.p., sed oni ŝuldas al la fakulo de kriptografio Augusto Buonafalce la meriton de atenta historiografia kaj filologia ekzameno[13]. Buonafalce okupiĝis longe pri kaj la polialfabeta ĉifrado de Alberti kaj tiu sekva de Giovan Battista Bellaso[14], ankaŭ li aktiva en la vatikana kadro sed kiu havis verŝajne nenian scion de la *De cyfris*. Fakte la sorto de la verko estis pridiskutata kaj la polialfabeta ĉifrado de Al-

ti, la fortuna dell'opera fu controversa e la cifratura polialfabetica dell'Alberti ebbe destino di scarsa applicazione. Del 1518 è la pubblicazione (postuma) della *Polygraphiae libri sex* dell'abate Tritemio, già inventore e autore della *Steganographia*, che esponeva i risultati di un sistema di crittazione composto da ventiquattro alfabeti ordinati, ognuno scalato di un posto rispetto al precedente. Questo sistema rendeva più complesso e articolato il metodo noto come "sostituzione di Cesare", descritto da Svetonio[11], secondo cui la lettera dell'alfabeto oscuro era avanzata di tre posti rispetto a quello in chiaro, ma non garantiva un elevato livello di protezione e soprattutto era suscettibile di rapida decodificazione da parte di un analista esperto e avvezzo ai crittogrammi. Gli stessi limiti sono dell'*Opus novum* di Iacopo Silvestri, che sebbene introduca un disco cifrante simile a quello albertiano, come si vedrà più avanti, ricorre ad alfabeti ordinati e dunque non così "sicuri" come quelli disposti nel *De cyfris*.

Di Alberti non parlano né Cardano né Della Porta, che pur usa dischi cifranti nel suo *De furtivis literarum notis, vulgo de ziferis* (1563), ma è di cinque anni più tardi la traduzione e la prima edizione a stampa de *La cifera*, ovvero del *De componendis cyfris*, a cura di Cosimo Bartoli, a lungo indeciso se tenere nascosto e segreto il volumetto o pubblicarlo con le opere dell'Alberti. Sappiamo com'è andata, ma non sappiamo quale manoscritto avesse utilizzato (forse uno antecedente a quelli di cui si dispone oggi). Quasi certamente non lo lesse Blaise de Vigenère, l'alchimista e crittografo francese autore del noto *Traicté des Chiffres ou secrètes manières d'escrire* (1585) e di un meno noto *Traicté du feu et du sel*. Secondo Buonafalce non ci sono prove che ne avesse conoscenza di prima mano, ma ha l'onestà intellettuale di citare l'Alberti senza tuttavia riconoscerne i meriti[16]. E se non fosse stato il più grande divulgatore francese di

berti estis mal multe aplikita. En 1518 estis eldonita (postmorte) la *Polygraphie libri sex* de abato Tritemio, jam elpensisto kaj aŭtoro de la *Steganographia*, kiu prezentis la rezultojn de sistemo de ĉifrado komponita de dudek kvar ordaj alfabetoj, ĉiu movita de unua loko kompare al la antaŭo. Tiu sistemo igis malsimplan kaj pli aranĝitan la metodon konatan kiel "antastaŭigo de Cezaro", priskribita de Svetonio[15], laŭ kiu la litero de la sekreta alfabeto plueniris de tri lokoj kompare al la litero de la klara alfabeto, sed tio ne certigis altan nivelon de protekto kaj ĉefe povis esti rapide deĉifrebla de analizisto sperta kaj kutimigita al la kriptografioj. La samajn limojn havas la *Opus novum* de Iacopo Silvestri, kiu kvankam enigas ĉifrantan diskon similan al tiu de Alberti, kiel poste oni vidos, uzas ordajn alfabetojn kaj do ne tiom "sekuraj" kiel tiuj aranĝitaj en la *De cyfris*.

Pri Alberti parolas nek Kardano nek Della Porta, eĉ se kiu uzas ĉifrantajn diskojn en sua *De furtivis literarum notis, vulgo de ziferis* (1563), sed estis kvin jaroj pli poste la traduko kaj unua eldonado de *La cifera*, tio estas la *De componendis cyfris*, editoris Cosimo Bartoli, kiu estis longe sendecida krom teni sekretan kaj kaŝitan la volumo aŭ eldoni kun la verkoj de Alberti. Ni scias kiel ĝi igis, sede ni nescias kiun manuskripton li uzis (eble unu antaŭa al tiuj pri kiuj oni disponas hodiaŭ). Preskaŭ certe ilin ne legis Blaise de Vigenexre, la franca alkemiisto kaj kriptografisto aŭtoro de la fama *Traictex des Chiffres ou secrete maniere d'escrire* (1585) kaj de la malpli fama *Traictex du fue et du sel*. Laŭ Buonafalce ne estis pruvoj ke li havis rekte akiritan konon, sed li havas la intelektan honestecon de mencii Alberti, tamen sen agnoski liajn meritojn[17]. Kaj se li ne estis la pli eminenta franca vulgariganto de kriptografio en la dekseca jarcento, ĉi

crittografia nel Cinquecento, questo sarebbe soltanto un dettaglio di poco conto. Grande esperto di linguaggi cifrati, di idiomi artificiali e di improbabili alchimie linguistiche, ebbe morte per un cancro alla gola nel 1596 e la tavola che porta il suo nome, la più semplice dei cifrari polialfabetici, fu "vinta" solo tre secoli più tardi dal metodo Kasiski, come si chiamava il colonnello prussiano che elaborò un metodo crittoanalitico per l'attacco del cifrario di Vigenère e di simili sistemi di crittazione.

Riassumendo, la fama dell'Alberti architetto, urbanista e illustre esponente della Rinascenza offuscava, per usare le parole dello storico David Kahn, l'autore del fortunatissimo *The codebreakers*, i tre primati dell'Alberti crittografo: "la prima trattazione di decrittografia apparsa in occidente, l'invenzione della sostituzione polialfabetica e l'invenzione del codice cifrato"[18]. Sarebbe piaciuta questa definizione all'Alberti? Dichiarava l'autore del *De cyfris* che duplice è lo scopo del suo trattato: da un lato individuare gli strumenti per l'intercettazione dei messaggi altrui, dall'altro elaborare un sistema scritturale cifrato per la trasmissione dei messaggi propri. Fuori dal giudizio etico, l'operazione è nobile in entrambi i casi, ma se si considerano gli aspetti pratici, il secondo obiettivo non richiede solo uno sforzo intellettuale o uno spiccato talento per la decrittazione. È necessario che il sistema sia pensato ed elaborato con metodo e secondo un criterio che lo renda intelligibile sia per il mittente che per il destinatario e, di contro, inintelligibile per il resto del mondo. Un altro particolare, che ben si coniuga con il clima di spionaggio tipicamente rinascimentale, è rappresentato dal fatto che colui che cifra non ha più bisogno di essere coadiuvato da un esperto e si libera, di conseguenza, da una collaborazione professionale pur sempre suscettibile di ricatti, minacce e tradimenti. Procedendo con rigorosa acribia, l'Alberti individua le qualità necessarie perché un sistema

tiu estias nur malgrava detalo. Eminenta spertulo de ĉifritaj lingvoj, artifikaj idiomoj kaj malprobablaj lingua alkemioj, mortis pro gorĝiokancero en 1596 kaj la tabelo nomita per li, kiu estas la pli simpla de polialfabetaj ĉifraroj, estis venkita nur post tri jarcentoj de la Kasiskimetodo, kiel nomis la prusa kolonelo kiu elpensis kriptoanalizan metodon por ataki la ĉifraro de Vigenexre kaj similaj sistemoj de ĉifrado.

Resumante, la famo de Alberti kiel arkitekto, urboplanisto kaj eminenta elstarulo de la Renesanco vualis, citante la vortojn de la historiisto David Kahn, aŭtoro de la tute sukcesa *The codebreakers*, la tri rekordojn de Alberti kiel kriptografisto: "la unua traktado de deĉifrado aperita en okcidento, la invento de la polialfabeta antastaŭigo kaj la invento de la ĉifrita kodo"[19]. ĉi tiu difino plaĉus al Alberti? La aŭtore de la *De cyfris* deklaris ke la celo de sua traktado estis dutipa: unuflanke determini la strumentojn por kapti mesaĝojn de aliaj, aliflanke prilabori ĉifritan sistemon de skribado por sendi siajn mesaĝojn. Transe la etika juĝo, la verko estis nobela ambaŭkaze, sed se oni konsideras la praktikajn vidpunktojn la dua celo necesas ne nur intelektan streĉo aŭ evidentan talenton por deĉifrado. Oni necesas sistemon pripensitan kaj aranĝitan metode kaj laŭ kriterio ke igis lin kompreneblan de kaj la sendanto kaj la adresito, kaj tamen nekompreneblan de ceteroj. Kroma detalo, kiu bone konjuĝas kun la tipa atmosfero de spionado de la Renesanco, estis la fakto ke tiu, kiu ĉifras, ne pli necesas de esti helpita de spertulo kaj sekve li povas liberiĝi de profesia kunlaboro ebla de ĉantaĝoj, minacoj kaj perfidoj. Irante kun rigora detalemo, Alberti determinas la necesajn karakterizojn por ke ĉifrita sistemo povas komplete defini. La unua estas la firman kaj precizan norme con kiu lin subtenas, tiel ke la kompreno de la sendita mesaĝo - eks-

cifrato possa definirsi compiutamente. La prima è data dalla costante e precisa normatività che lo sorregge, di modo che la comprensione del messaggio trasmesso - a prescindere dalla sua lunghezza e dalla sua complessità – sia sempre possibile da parte di mittente e destinatario e risponda a criteri invariati sia per l'oscuramento dei dati che per la loro decrittazione. La seconda risponde invece al criterio della *novitas*: un sistema di cifratura deve essere del tutto nuovo (nel senso di nuova concezione) e del tutto sconosciuto. Sarà ciò sufficiente a proteggerlo dalle intercettazioni dei nemici, dei curiosi o delle persone direttamente coinvolte nel messaggio? Se la risposta fosse affermativa il *De cyfris* non sarebbe considerato, a ragione, il primo, vero studio di crittografia moderna, e l'Alberti non avrebbe esteso la sua indagine ai rapporti numerici che intercorrono fra le lettere alfabetiche. In altri termini, un sistema di cifratura che risponda ai criteri della scientificità deve trarre la sua origine da un'attenta disamina delle frequenze vocaliche e consonantiche.

klude de sia longeco kaj sia komplekseco - estas ĉiam ebla por kaj la sendanto kaj la adresito, kaj kongruas kriteriojn senŝanĝajn kaj laŭ la kaŝado de la elementoj kaj laŭ ĝiaj deĉifrado. La dua kongruas la kriterion de *novitas*: ĉifrita sistemo devas esti tute nova (intentante nova koncepto) kaj tute nekonata. Estos tio sufiĉa por protekti ĝin de la interkapto de malamikoj, scivoloj kaj personoj rekte implikitaj en la meŝago? Se la respondo estus jesa la *De cyfris* ne estus konsiderita rekte kiel la unua vera studo de moderna kriptografio, kaj Alberti ne plivastigus sian enketadon al la numeraj rilatoj kiuj estas inter la alfabetaj literoj. Alivorte, ĉifrita sistemo kiu kongruas sciencajn kriteriojn devas naskiĝi de atenta ekzameno de vokalaj kaj konsonantaj ofteco.

Accusandosi di prolissità - diciamo così – necessaria, l'Alberti spiega al lettore che il compito è noioso ma alla portata di tutti coloro che hanno la pazienza di aprire una o due pagine di un poeta o di un prosatore e raccogliere a mo' di elenco, ai margini del foglio, la serie delle vocali e delle consonati, prese separatamente. Questo primo esercizio serve a mostrare che sia nei testi poetici che in quelli in prosa – naturalmente si intende in latino - le vocali ricorrono molto più frequentemente di quanto si pensi, ma con una leggera differenza: nei primi le consonanti le superano per non più di un ottavo, nei secondi per non più di un terzo (es. 300 vocali e 400 consonanti). La O è quella che ricorre con minor frequenza e precede di poco la A e la V, più frequente nell'uso consonantico. Se le due vocali più ricorrenti sono dunque la I e la E, e se è vero che senza vocale non si dà sillaba, è bene, continua l'autore, procedere

Kvankam kulpigas sin pri necesa malkoncizo - por tiel diri - Alberti esplikas al la leganto ke la tasko estas teda sed ebla por tiuj kiuj havas la paciencon de malfermi unu aŭ du pagojn de poeto aŭ prozisto kaj listigi marĝene la serion de vokaloj kaj konsonantoj, aparte prenitaj. Tiu unua ekzerco utilas al montri ke kaj en poetaj kaj en prozaj testo - kompreneble en latina lingvo - la vokaloj aperas multe pli ofte ol oni supozas, sed kun malpeza diverseco: en la unuoj la konsonantoj superas ilin pri ne pli de okono, en la duoj ne pli de triono (ekzemple 300 vakaloj kaj 400 konsonantoj). La O estas la vokalo kiu aperas malpli ofte kaj antaŭiras malmulte la A kaj la V, kiu aperas pli ofte en la konsonanta ozo. Se la du vokaloj pli repetiĝantaj estas do la I kaj la E, kaj se estas vere ke sen vokalo oni havas neniun silabon, laŭ la aŭtoro estas bone efektivigi rigoran analizon de la silabaj renkontoj kaj atenti la vokalan aranĝon. Kun

a una rigorosa analisi degli incontri sillabici e prestare attenzione alla disposizione vocalica. Tavole di frequenza alla mano, l'Alberti registra che molto spesso alla A segue la U, qualche volta la O e nel caso del dittongo la E. Dopo la O non si trova la A, invece, e così via, senza stupirsi di una regola alla quale di norma non si pensa, ossia che qualsiasi vocale può trovarsi all'inizio o alla fine di una parola, ciò che non vale, invece, per le consonanti. E a proposito di queste, come non notare che la G ricorre pochissimo nella scrittura e che una sorte simile, in fondo, tocca alle sue "colleghe" F, B, C, L, Q e K, a dispetto delle usatissime e molto frequenti S, T e R. La posizione consonantica non è meno interessante.

Due sono le modalità di accorpamento: per *aggiunzione* quando da una o più consonanti, per aggiunta di una sola vocale, si genera una sillaba intera (es. *stat*); per *successione* quando una lettera è disgiunta dalla precedente, come nel caso di *ar-ma*. Infine, è opportuno ricordarsi che nella lingua latina non si dà mai un intervallo vocalico superiore alle quattro consonanti. Quanto riportato finora può considerarsi sufficiente per capire il nesso di queste tavole di frequenza con l'elaborazione di un metodo crittografico sicuro. Supponiamo infatti di entrare in possesso di un messaggio cifrato e di provare a decrittarlo. Alla luce delle frequenze di cui sopra e di alcune informazioni più immediate, quali il numero delle lettere dell'alfabeto (19 o 20 se è contemplata anche la Z anziché 21, poiché il segno V è sia vocalico che consonantico) e il possibile utilizzo, da parte di chi ha criptato il messaggio, dei segni nulli o di quelli omofoni (ossia che corrispondono alla medesima lettera), il nostro vantaggio – secondo l'Alberti – sarà quello di sapere che i segni più frequenti corrispondono alle vocali e che queste non distano l'una dall'altra per intervalli molto ampi. Dalle osservazioni sugli incontri consonantici di cui sopra e da altre frequenze piuttosto intuitive, come la

la tabuloj de ofteco en la mano, Alberti ke pli ofte la A antaŭiras la U-n, kelkfoje la O-n kaj en diftongo la E-n. Post la O oni ne trovas la A-n, kaj tiel plu, sen surpriziĝas de normo al kiu oni kutime ne pensas, tio estas ke ĉiuj vokaloj povas troviĝi al la komenco aŭ al la fino de vorto, kaj tio ne validas por konsonantoj. Koncerne ilin, kiel oni povas ne rimarki ke la G aperas tre malmulte en la skribado, kaj sama sorto okazas ankaŭ al la siaj kolegoj F, B, C, L Q kaj K, respekte la multe uzitaj kaj pli oftaj S, T kaj R. La konsonanta aranĝon ne estas malpli interesa.

Du estas la manieroj de kunigo: laŭ *aldono* kiam de unu kaj pli konsonantoj tuta silabo estiĝas per la aldonaĵo de unu vokalo (ekzemple *stat*); laŭ *sinsekvo* kaim literoj estas disigita de la antaŭa, kiel en la kazo de *ar-ma*. Finfine ĝi estas oportune memori ke en la latina lingvo oni havas neniam vokalan intervalon superan al kvar konsonantoj. Koncerne tion, kiu oni diras ĝis nun, oni povas konsideri ĝin sufiĉan por kompreni la konekson inter ĉi tiuj tabeloj de ofteco kaj la prilaboro de sekura ĉifrado. Ni eĉ supozu, ke ni trovas ĉifritan mesaĝon kaj provas ĝin deĉifri, laŭ la supremenciitaj oftecoj kaj kelkaj informojn pli tujaj, kiel la numero de la literoj de la alfabeto (19 aŭ 20 se estas konsiderita ankaŭ la Z sed 21, ĉar la signo V estas kaj vokala kaj konsonanta) kaj la ebla uzo, flanke de tiu kiu ĉifris la mesaĝon, de senrezultaj aŭ omofonaj signoj (estas tioj kiuj kongruas la saman literon), laŭ Alberti la nia avantaĝo estos la scion ke al oftaj signoj kongruas la vokalojn kaj ke tiuj ne distanciĝas reciproke pro larĝaj intervaloj. De la observadoj pri surmenciitaj konsonantaj renkontoj kaj de aliaj oftecoj sufiĉe intuiciaj, kiel la sinsekvo de du vokaloj en la sama silabo aŭ - tio okazas pli ofte - la konsonanto kiu intermetiĝas inter du vokaloj, ni akiras aliajn informojn

successione di due vocali nella stessa sillaba o – come accade molto spesso – della consonante che si frappone fra due vocali, abbiamo altre informazioni e sarà sufficiente disporre di buon intelletto e di un'innata predisposizione ai codici per procedere alla decrittazione del messaggio intercettato.

Immaginiamo ora di fare l'operazione inversa, ovvero di criptare una frase segreta che correrà il rischio di cadere in mani nemiche. Per prima cosa, non utilizzeremo un sistema di codificazione simile a quelli che abbiamo appena terminato di volgere in chiaro. Benché infatti lo studio delle frequenze ci abbia illuminato sui punti deboli dei codici tradizionali, è vero che il ricorso a qualche altro espediente migliorerebbe di poco il loro livello di protezione. Occorre dunque ripensare interamente la macchina crittografica, tenendo conto che per le vocali e le consonanti più ricorrenti, come nel caso della E e della R, è necessario poter disporre di un numero elevato di segni dissimili, così che la singola lettera sia associata, di volta in volta, a un carattere differente. Un altro accorgimento verrà dal trascurare le regole ortografiche, che rendono più prevedibile – al pari delle regole consonantiche – la struttura di una frase o delle singole parole. Ne consegue che sono assolutamente da evitare la geminata (per es. *arogans* in luogo di *arrogans*), la U dopo la Q, la H e così via, fino alla stipulazione dell'uso di parole prive di senso all'inizio o alla fine della frase o di parole prive di vocali. Nel sistema cosiddetto monoalfabetico si possono associare a un unico segno una o più lettere dell'alfabeto (per es. alla G la A e alla R la B nel caso di una sola lettera, ma anche alla N le coppie di *combinate* SC o RT), una o più sillabe o ancora una o più parole fino a un'intera frase (la lettera A per "pontefice" o la lettera R per "le truppe nemiche si spostano verso ovest"). Per confondere le carte si può anche invertire l'ordine scritturale, ponendo la prima lettera del messaggio in chiaro

kaj ĝi estos sufica havi efikan intelekton kaj kunnaskitan dispozicion por kodoj por iri al la deĉifro de la kapta mesaĝo.

Ni eĉ supozu fari la inversan operacion, tio estas ĉifri sekretan frazon, kiu riskas de fali en la malamikaj manoj. Antaŭe ni ne uzus sistemon de ĉifrado similan al tioj kiujn ni havas ĵus deĉifri. Kvankam la studo de oftecoj iluminis nin pri la malfortaĵojn de la tradiciaj kodoj, se oni ekuzus kelkajn aliajn artifikojn ilia nevelo de ŝirmo pliboniĝus iom. Oni devas do tute repripensi la kriptomaŝinon, considerante ke la vokaloj kaj la konsonantoj pli oftaj, kiel la E kaj la R, necesas ke oni povas disponi pri alta numero de malsimilaj signoj, kaj do la unuopa litero estas asociita ĉiufoje al malsimilaj signoj. Alia elturniĝo estos flankelasi ortografiajn normojn, kiuj igas - kiel la konsonantaj normoj - la strukturon de la fraso aŭ de la unuopaj vortoj pli antaŭvideblaj. El tio sekvas, ke oni devas absolute eviti la duobligon (ekzemple *arogans* anstataŭe *arrogans*), la U post la Q, la H kaj tiel plu, ĝis la kontraktado de sensencaj vortoj por uzi al la komenzo aŭ al la fino de la frazo, aŭ de vortoj sin vokaloj. En la tiel nomata monoalfabeta sistemo oni povas asocii sola signo kun unu kai pli literoj de la alfabeto (ekzemple la G kun la A kaj la R kun la B sed oni asocias solan literon, sed eĉ la N kun la paroj de *kuaranĝitoj*[20] SC aŭ RT), kun unu aŭ pli silaboj aŭ ankoraŭ kun unu aŭ pli vortoj ĝis kun kompleta frazo (la litero A povas signifi "pontifiko" aŭ la litero R "la malamikaj tropo formoviĝas al okcidento"). Por konfuzi la kartojn oni povas inversigi la skriban ordon, poni la unuan literon de la klara mesaĝon al la fino de la ĉifrita mesaĝo, la duo al la antaŭlasta loko kaj tiel plu, ĝis inversigi tute la ĉifritan frazon. Sammaniere oni povas inversigi la pozicio de la silaboj aŭ uzi kom-

all'ultimo posto del messaggio oscurato, la seconda al penultimo e così via, sino a invertire completamente la frase criptata. Allo stesso modo, è possibile invertire la posizione delle sillabe o utilizzare per la cifratura intere parole, come "libro" per indicare "flotta" o "campo" per indicare "pontefice". Meglio ancora, se si vuole restare entro il dominio delle convenzioni, può rappresentare il vecchio trucco di posizionare termini strategici per la comunicazione in oggetto disperdendoli all'interno di una comune lettera privata o di un messaggio apparentemente privo di ambiguità e doppie letture.

Dalla spiegazione che segue si possono comprendere senza difficoltà le ragioni che vogliono il *De cyfris* il primo manuale di crittografia moderna. Da due lamine di bronzo, scrive l'Alberti, si ottengano due dischi, l'uno (*fisso*) di diametro di un nono più grande dell'altro (*mobile*) ed entrambi divisi in ventiquattro sezioni di ampiezza uguale (*case*). In ciascuna di queste case del cerchio maggiore siano scritte, in colore rosso, le lettere maiuscole dell'alfabeto (A, B, C ... senza la H e la K, considerate dall'Alberti pleonastiche) per un totale di venti lettere (Z compresa). I quattro spazi vuoti che restano a disposizione servono invece per i primi quattro numeri, disposti in ordine crescente, così che alla fine tutte le ventiquattro case saranno contrassegnate da un carattere alfabetico o da un numero. Si prenda ora il cerchio minore e lo si divida secondo le stesse linee di demarcazione del primo. All'interno delle case mobili troveranno posto tutti i ventiquattro caratteri alfabetici di colore nero (la differenza fra rosso e nero non sembra avere significati particolari), ivi comprese - in luogo dei cardinali 1, 2, 3, 4 - le lettere H e K, assenti nel disco maggiore, nonché Y e &. L'ordine dei ventiquattro segni non sarà tuttavia quello alfabetico, ma risponderà al criterio della casualità, tale che alla A seguirà, per es., la G e alla G la Z, e così via. A questo punto, non resta che sovrapporre il disco minopletajn vortojn por ĉifri, kiel "libro" por indiki "floto" aŭ "kampo" por indiki "pontifiko". Ankoraŭ pli bona, se oni volas resti en la ordinara regado, estas la malnova artifiko de loki strategiajn vortojn por la tema komuniko per dismeti ilin en ordinara privata letero aŭ en mesaĝo ŝajne sen ambiguecoj kaj duoblaj legaĵoj.

De la sekvanta klarigo oni povas kompreni sen malfacilecoj la kaŭzojn pro kiuj la *De cyfris* estas la unua manlibro de moderna kriptografio. De du bronzaj lamenoj, skribas Alberti, oni akiras du diskojn, unu (*fiksa*) kun la diametro de unu naŭono pli granda ol la alia (*movebla*), kaj ambaŭ disaj en dudek kvar sekcioj de sama vasteco (*domoj*). En ĉiu sekcio de la pli granda disko oni devas skribi ruge la maiusklajn literojn de la alfabeto (A, B, C, ... sen la H kaj la K, kiuj Alberti konsideri pleonasmaj), ĝis entute dudek literoj (inkluzive la Z). La kvar malplenaj spacoj kiuj estas disponeblaj servas por la unuaj kvar numeroj, aranĝitaj en kreskanta ordo, tiel ke ĉiuj dudek kvar domoj estos markitaj de alfabeta literon aŭ numero. Nun oni devas preni la minoran diskon kaj ĝin disas laŭ la sama linioj de la unua. En la moveblaj domoj trovas lokon ĉiuj alfabetaj literoj, nigre skribitaj (la malsameco inter ruĝo kaj nigro ŝajnas malmulte grava), inkluzive, anstataŭe la kardinalaj numeroj 1, 2, 3, 4, la literoj H kaj K, neĉeestantoj en la unua disko, kaj ankaŭ la Y kaj la signo &. La ordo de la dudek kvar signoj ne estos tamen la alfabeta ordo, sed estos hazarda, tiel ke la G sekvas la A kaj la Z sekvas la G, kaj tiel plu. Kaj post tio oni devas nur meti la minoran diskon sur la pli granda kaj ilin kunligi per unua akso, tial ke la *fiksa* disko permesas la rotacion de la *movebla* kaj ke ĉiu domo en la unua disko kongruas

re a quello maggiore e collegarli attraverso un unico asse, di modo che quello chiamato *fisso* consenta la rotazione di quello chiamato *mobile* e che a una casa del primo corrisponda un'altra casa del secondo. La macchina crittografica così ottenuta, scrive l'Alberti, è la *formula*, ma non è sufficiente possederne un solo esemplare. È infatti necessario che sia il mittente che il destinatario possano disporne per criptare e successivamente decifrare il messaggio trasmesso, e soprattutto che i loro esemplari siano perfettamente identici (pena il fallimento della comunicazione e l'incapacità del destinatario di comprendere il testo oscurato).

alian domon en la dua. La kriptomaŝino tial akirita, Alberti skribas, estas la *formulo*, sed ne estas sufiĉe havi nur unuan modelon. ĝi estas necese ke kaj la sendanto kaj la adresito povas disponi de tiu por ĉifri kaj post deĉifri la senditan mesagon, kaj precipe ke iliaj modeloj estas tute samaj (alikaze oni havus la fiasko de la komunikado kaj la nekapableco de la adresito kompreni la ĉifritan tekston).

Un'altra condizione che deve essere soddisfatta, se non si vuole compromettere il buon esito della trasmissione in codice, è la scelta concordata di due indici o lettere chiave, l'uno tratto dal disco delle maiuscole e l'altro da quello minore. L'esempio spiegato dall'Alberti aiuta a comprendere questo passaggio. Immaginiamo di aver scelto come indice del disco mobile il *k* e di avergli fatto corrispondere, sul disco fisso delle maiuscole, la B. In fase di cifratura, quindi, la prima lettera da scrivere sarà la B (associata nella *formula* al *k*) così che il destinatario, ricevuta la missiva, comprenderà di dover ruotare la sua stessa e identica *formula* finché alla B non corrisponderà il *k*.

Alia kondiĉio plenuminda, se oni ne volas endanĝerigi la sukceson de la ĉifrita transigon, estas la antaŭfiksitan elekton de du *indicoj* aŭ ŝlosilliteroj, unu de la disko kun la ĉefliteroj kaj alia de la minora disko. La ekzemplo kiu Alberti klarigas helpas kompreni ĉi tiun transigon. Ni supozu elekti kiel indicon de la movebla disko la *k* kaj kongrui ĝin kun la *B* de la ĉeflitera disko. En ĉifradostadio do la unua litero skribinda estos la *B* (asociita al la *k* en la *formulo*) tial ke la adresito, post ricevi la leteron, komprenos ke li devas turni sian saman *formulon* ĝis la *B* kongruas la *k*.

A	**B**	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	2	3	4
x	**k**	v	s	a	i	e	n	t	d	o	h	b	p	g	z	c	y	r	&	q	f	m	l

A	B	C	D	E	F	G	I	L	M	N	O	P	Q	**R**	S	T	V	X	Z	1	2	3	4
h	b	p	g	z	c	y	r	&	q	f	m	l	x	**k**	v	s	a	i	e	n	t	d	o

Con l'inserimento della *R* maiuscola nella missiva, anche al desti-

Se oni enmetus la majuskla*R*-n en la letero, la adresito kompre-

natario sarà chiaro di dover ruotare la *k* (ossia l'indice concordato) fino alla sua corrispondenza con la *R* del disco maggiore. Le lettere maiuscole rappresentano quindi una sorta di codice nel codice: è attraverso il loro utilizzo che mittente e destinatario riescono a comunicare, all'interno della missiva, lo spostamento o la rotazione alfabetica che producono il cambiamento dell'ordine di cifratura. Un altro codice a sé è in un certo senso rappresentato dalle quattro case contrassegnate dai numeri. Se a un primo sguardo può sembrare che l'Alberti avesse predisposto l'eventualità di un codice alfanumerico (una scelta che invece farà, molti anni più tardi, l'ingegnere esoterista Abramo Colorni con la sua *Scotographia*), è bene sapere che le lettere associate alle caselle numeriche serviranno soltanto come segni nulli, privi di significato ed inseriti per dividere le parole che compongono il messaggio. Un esempio renderà tutto più chiaro. Immaginiamo di dover criptare il seguente messaggio:

nus ke li devas turni la *k* (tio estas la antaŭfiksitan indicon) ĝis li kongruas ĝin kun la *R* de la pli granda disko. La ĉefiteroj simbolas specon de kodo en la kodo: pere de ilia uzo la sendanto kaj la adresito povas komuniki, en la letero, la lokŝanĝon aŭ la alfabetan rotacion kiuj kaŭzas la ŝanĝon en la ordo de ĉifrado. Iasence alia kodo en si mem estas la kvar domoj markitaj per numeroj. Se ĉe unua rigardo oni povas kredi ke Alberti anatŭaranĝis eventualan liternumeran kodon (elekto kiu post multaj jaroj faros la inĝeniero esoteriista Abramo Colorni kun sia *Scotographia*), estas bone scii ke la literoj asociitaj al la numeraj ĉeloj servas nur kiel senrezultaj signoj, sensencaj kaj enmetitaj por disigi la vortojn kiuj komponas la mesaĝon. Ekzemplo klarigas ĉio. Oni supozas ke ni devas ĉifri la sekvantan mesaĝon:

LE TRUPPE SI SONO RITIRATE

E trasformiamolo secondo le regole prescritte dal sistema di cifratura albertiano (eliminazione delle doppie, inserimento dei segni nulli) fino a farlo diventare

Kaj ni transformas ĝin laŭ la normoj fiksitaj de la ĉifrosistemo de Alberti (la eliminado de la duopaj literoj, la enigo de la senrezultaj signoj) ĝis ni obtenas

LE1TRUPE2SI3SONO4RITIRATE

. Se si utilizzano come indici e come alfabeti quelli illustrati nelle tabelle di sopra, la prima chiave sarà la *B*, alla quale verrà associata la *k* dell'alfabeto oscuro. Dopo le prime quattro parole subentrerà il nuovo indice *R*, che corrispondendo ancora con il *k* genererà un nuovo alfabeto.

. Se oni uzas kiel indicoj kaj kiel alfabetaj tiuj indikitaj en la supre koncernataj tabeloj, la unua ŝlosilo estos la *B*-n, al kiu estos asociita la *k* de la malklara alfabeto. Post la kvar unuaj vortoj anstataŭas la nova indico *R*, kiu kongruas ankoraŭ la *k*-n kaj estigas novan alfabeton.

A	**B**	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	2	3	4
x	**k**	v	s	a	i	e	n	t	d	o	h	b	p	g	z	c	y	r	&	q	f	m	l
A	B	C	D	E	F	G	I	L	M	N	O	P	Q	**R**	S	T	V	X	Z	1	2	3	4
h	b	p	g	z	c	y	r	&	q	f	m	l	x	**k**	v	s	a	i	e	n	t	d	o

. Il crittogramma finale sarà dunque

. La fina kriptaĵo estos do

BtaqcgybafznmzhohlRkrsrkhsz

, come si può vedere nella tabella qui di seguito

, kiel oni povas vidi en la sekvantan tabelon

B	L	E	1	T	R	U	P	E	2	S	I	3	S	O	N	O	4	**R**	R	I	T	I	R	A	T	E
k	t	a	q	c	g	y	b	a	f	z	n	m	z	h	o	h	l	**k**	k	r	s	r	k	h	s	c

. Diverso è il caso di un indice concordato sul *disco fisso*, ad esempio la lettera *B*. Se ad essa si decide di associare la *q*

. Alia esta la kazo de indico antaŭfiksita sur la *fiksa* disko, ekzemple la litero *B*. Se oni decidas kongrui ĝin kun la *q*

A	**B**	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	2	3	4
&	**q**	f	m	l	x	k	v	s	a	i	e	n	t	d	o	h	b	p	g	z	c	y	r

si segnerà una *q* minuscola all'inizio della missiva così che il destinatario provvederà a ruotare e ad allineare le ventiquattro case nell'ordine corretto. Dal momento che, in questo caso, l'inserimento della maiuscola per la variazione del codice non è più possibile, il destinatario verrà avvisato del nuovo sistema di cifratura dalla corrispondenza di una lettera minuscola, detta *numerale*, con una delle

oni markos minusklan *q*-n ĉe la komenco de la litero tiel ke la adresito turnos kaj vicigas la dudek kvar ĉefoj en la rekta ordo. ĉar en ĉi tiu kazo la enigo de la majuskla litero por modifi la kodon estas neebla, oni informos la adresiton pri la nova ĉifrosistemo de la respondo de minuskla litero, nomita *numeralo*, kun unu el la kvar numeraj ĉeloj. Kaj post tio estas sufiĉe turni ĝis la antaŭfiksita indico

quattro caselle numeriche. A questo punto, sarà sufficiente ruotare fino all'indice concordato *B* la lettera numerale di cui sopra e procedere a cifrare o a decrittare secondo il nuovo ordine. Immaginiamo, dopo quattro parole, di voler mutare il codice. Si inserisca a questo punto nella frase da oscurare la lettera *c*, che come si può vedere corrisponde al numero 2

B la surmenciitan numeralan literon kaj pluiri ĉifri aŭ deĉifri laŭ la nova ordo. Ni imagas voli ke, post kvar vortoj, la kodo ŝanĝiĝas. Oni enmetas kaj post tio en la ĉifrinda frazo la literon *c*-n, kiu kiel oni vidas kongruas la numeron 2

A	B	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	**2**	3	4
&	q	f	m	l	x	k	v	s	a	i	e	n	t	d	o	h	b	p	g	z	**c**	y	r

. Da questo "codice nel codice" il destinatario comprenderà che la scelta del nuovo indice del disco *mobile* è la *c*, da associare allo stipulato indice *B* del disco *fisso*. Con la rotazione della *formula* si otterrà un nuovo ordine alfabetico

. De ĉi tiu "kodo en la kodo" la adresito komprenos ke la elekto de la nova indico de la *movebla* disko estas la *c*, kiu estas asociinda al la antaŭfiksita indico *B* de la *fiksa* disko. Per la rotacio de la *formula* oni akiros novan alfabetan ordon

A	**B**	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	2	3	4
z	**c**	y	r	&	q	f	m	l	x	k	v	s	a	i	e	n	t	d	o	h	b	p	g

, che d'ora in avanti sostituirà quello precedente. In questo caso si potrà disporre delle lettere maiuscole da inserire come segni nulli o ricorrere ad accorgimenti di depistaggio stipulati fra mittente e destinatario prima della trasmissione in codice (ma l'elenco sarebbe talmente lungo che persino l'Alberti decide di risparmiare il lettore da un'ulteriore prolissità). Proviamo a fare un esempio con la frase che abbiamo utilizzato con l'altro metodo, ovvero

, kiu ekde nun anstataŭos tion antaŭan. ĉiukaze oni povos disponi de la majusklaj literoj por enigi ilin kiel senrezultajn signojn aŭ ekuzi al artifikoj de devojigo aranĝitaj inter la sendanto kaj la adresito antaŭe la ĉifrita transigo (sed la listo estus tiom longa ke eĉ Alberti elektas ŝpari pluan multvortecon al la legantoj). Ni elprovas fari ekzemplon per la frazo kiun ni uzis kun alia metodo, tio estas

LE TRUPPE SI SONO RITIRATE

. In questo caso, dal momento che le *numerali* sono necessarie a

. ĉiukaze, ĉar la *numeraloj* estas necesaj por signi la ŝanĝon de al-

segnalare il cambio d'alfabeto, accorperemo il messaggio in questo modo, con la consueta eliminazione delle doppie:

fabeto, ni grupigas la mesaĝon tiel, kun la kutima eliminado de la duobloj.

LETRUPESISONORITIRATE

Se dunque si utilizzerà l'indice concordato *B* associato con q e dopo la quarta parola si passerà alla corrispondenza di *c* con *B*, secondo il seguente schema polialfabetico

Se do oni uzos la antaŭfiksitan indicon *B* asociitan kun *q*, kaj post la kvara vorto oni transiros al la kongrueco de *c* kaj *B*, laŭ la sekvanta polialfabeta skemo

A	**B**	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	**2**	3	4
&	**q**	f	m	l	x	k	v	s	a	i	e	n	t	d	o	h	b	p	g	z	**c**	y	r
A	**B**	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	2	3	4
z	**c**	y	r	&	q	f	m	l	x	k	v	s	a	i	e	n	t	d	o	h	b	p	g

. Il crittogramma finale sarà

. La fina kriptogramo estos

qslhdbnlovoeiecimnmizn&

, come risulta dalle corrispondenze indicate dalla tabella qui di seguito

, kiel oni povas vidi de la kongruecoj indikitaj en la tabelo poste

B	L	E	T	R	U	P	E	S	I	S	O	N	O	**B**	R	I	T	I	R	A	T	E
q	s	l	h	d	b	n	l	o	v	o	e	i	e	**c**	i	m	n	m	i	z	n	&

. È piuttosto sulle lettere *numerali*, come sono appunto denominate le minuscole di volta in volta associate a una casella numerica

. Plivere, sur la literoj *numeralaj*, kiel estas ĝuste nomitaj la minusklaj ĉiufoje asociitaj al numera ĉelo sur la disko de la maiuskloj,

sulla ruota delle maiuscole, che poggiano le possibilità di un ulteriore codice (non propriamente alfanumerico) per la cifratura di ben trecentotrentasei frasi. Seguiamo l'Alberti nel suo esempio e stabiliamo che le lettere p, s, f e k corrispondano alle caselle numeriche 1, 2, 3 e 4, come nella tabella sottostante.

1	2	3	4
p	s	f	k

. Con questa disposizione, se si procede per coppie, si possono creare 16 abbinamenti per altrettante locuzioni. Se in una tabella concordata di frasi da sottoporre a cifratura si vuole, per esempio, cifrare la frase con codice 13, sarà sufficiente indicare nella missiva oscurata i caratteri combinati pf, che corrispondendo al numero 13 indicheranno la frase associata e per il destinatario non vi sarà alcuna difficoltà, consultando la tavola o addirittura ricordandolo a memoria, a decrittare la sigla e a capire a quale frase in chiaro si riferisce il testo oscuro. Se la tavola contempla un numero maggiore di frasi e si vuole criptare, supponiamo, quella recante il codice 123, si indicherà il codice *psf* e il destinatario procederà, a sua volta, a trovare la frase in chiaro corrispondente. Se ancora le possibilità a disposizione non fossero sufficienti, si può estendere la tavola sino a 336 frasi in chiaro e, per esempio, criptare quella con codice 3124 con la sigla alfabetica *fpsk*. La tavola dovrà essere composta nel modo che segue, tale che si troveranno disposte in serie tutte le possibili associazioni numerali e le frasi convenzionalmente associate a queste.

bazi$\hat{g}$as la ebloj de plua kodo (ne propre alfanumera kodo) per $\hat{c}$ifri e$\hat{c}$ tricent tridek ses frazojn. Ni sekvas Alberti en sia ekzemplo kaj decidas ke la literoj p, s, f kaj k kongruas la numeraj $\hat{c}$efoj 1, 2, 3 kaj 4, kiel en la suba tabelo.

. Per $\hat{c}$i tiu aran$\hat{g}$o, se oni pluiras por paroj, oni povas krei dek ses parigojn por samnombraj lokucioj. Se en antaŭfiksita tabelo de $\hat{c}$ifrindaj frazoj oni volas ekzemple $\hat{c}$ifri la frazon kun kodo 13, estos sufi$\hat{c}$e indiki en la $\hat{c}$ifrita letero la aran$\hat{g}$itaj signoj *pf*, kiuj, $\hat{c}$ar ili kongruas la numeron 13, indikos la asociitan frazon kaj por la adresito estos nenia malfacila$\hat{j}$o, se li konsultas la tabelon aŭ li e$\hat{c}$ memorigas $\hat{g}$in, de$\hat{c}$ifri la siglon kaj kompreni la frazon al kiu la $\hat{c}$ifrita teksto rilatas. Se la tabelo konsideras pli grandan numeron de frazoj kaj oni volas $\hat{c}$ifri, ni supozu, tion kiu havas la kodo 123, oni indikos la kodon *psf* kaj la adresito pluiros siavice trovi la kongruan klaran frazon. Se ankoraŭ la ebloj je dispono ne estas sufi$\hat{c}$aj, oni povas plivastigi la tabelon $\hat{g}$is 336 klaraj frazoj kaj ekzemple $\hat{c}$ifri tion kiu havas la kodon 3124 kun la alfabeta siglo *fpsk*. La tabelo devos esti kombinita sekva maniere, tiel ke trovi$\hat{g}$os $\hat{c}$iuj eblaj numeraj kunigoj, kaj la frazoj konvencie asociitaj kun ili, aran$\hat{g}$itaj serie.

11	131	311	431

12	132	312	432
13	133	313	433
14	134	314	434

21	141	321	441
22	142	322	442
23	143	323	443
24	144	324	444

31	211	331	1111
32	212	332	1112
33	213	333	1113
34	214	334	1114

41	221	341	1121
42	222	342	1122
43	223	343	1123
44	224	344	1124

111	231	411	1131
112	231	412	1132
113	233	413	1133
114	234	414	1134

121	241	421	1141
122	242	422	1142
123	243	423	1143
124	244	424	1144

1211	1331	2111	2231
1212	1332	2112	2232

1213	1333	2113	2233
1214	1334	2114	2234

1221	1341	2121	2241
1222	1342	2122	2242
1223	1343	2123	2243
1224	1344	2124	2244

1231	1411	2131	2311
1232	1412	2132	2312
1233	1413	2133	2313
1234	1414	2134	2314

1241	1421	2141	2321
1242	1422	2142	2322
1243	1423	2143	2323
1244	1424	2144	2324

1311	1431	2211	2331
1312	1432	2212	2332
1313	1433	2213	2333
1314	1434	2214	2334

1321	1441	2221	2341
1322	1442	2222	2342
1323	1443	2223	2343
1324	1444	2224	2344

2411	3131	3311	3431
2412	3132	3312	3432
2413	3133	3313	3433

2414	3134	3314	3434

2421	3141	3321	3441
2422	3142	3322	3442
2423	3143	3323	3443
2424	3144	3324	3444

2431	3211	3331	4111
2432	3212	3332	4112
2433	3213	3333	4113
2434	3214	3334	4114

2441	3221	3341	4121
2442	3222	3342	4122
2443	3223	3343	4123
2444	3224	3344	4124

3111	3231	3411	4131
3112	3232	3412	4132
3113	3233	3413	4133
3114	3234	3414	4134

3121	3241	3421	4141
3122	3242	3422	4142
3123	3243	3423	4143
3124	3244	3424	4144

4211	4331
4212	4332
4213	4333
4214	4334

4221	4341
4222	4342
4223	4343
4224	4344

4231	4411
4232	4412
4233	4413
4234	4414

4241	4421
4242	4422
4243	4423
4244	4424

4311	4431
4312	4432
4313	4433
4314	4434

4321	4441
4322	4442
4323	4443
4324	4444

. Dal momento che la consultazione rischia di non essere poi così immediata, nel *De cyfris* l'Alberti suggerisce di tenere sia presso il mittente che presso il destinatario, oltre a questa tavola, un'altra che rechi – in ordine alfabetico – le frasi convenzionali (per es., sotto la

. Ĉar la konsultado riskas ne esti tiom tuja, en la *De cyfris* Alberti konsilas teni kaj ĉe la sendanto kaj ĉe la adresito, krom ĉi tiu tabelo, alian tabelon kiu indikas - en alfabeta ordo - la konvenciajn frazojn (ekzemple sub la P estus la frazoj kiuj rilatas la proviantadon, sub

A le frasi che riguardano l'annona, sotto la E le frasi che riguardano l'esercito e così via). Alla fine di ogni frase la tavola indicherà, inoltre, il numero corrispondente, così che nella fase di cifratura sia più immediata la ricerca della cifra da trasmettere nel codice delle minuscole.

. Come ha avuto modo di spiegare il sopracitato Augusto Buonafalce, l'utilizzo del disco cifrante non è prerogativa albertiana, benché vi avesse fatto ricorso nei *Trivia senatoria*, scritti pochi anni prima del *De cyfris*. Non è certo che l'Alberti conoscesse Raimondo Lullo (ma è tuttavia molto verosimile) e non è il caso di ricordare l'incisività che ebbe l'applicazione delle sue regole ai vari campi del sapere fra l'età rinascimentale e quella barocca. Piuttosto, riprendendo Buonafalce, l'ipotesi più affascinante sembra rimandare all'influenza del coevo Giovanni Fontana[21], autore dell'opera di mnemotecnica Secretum de Thesauro, nelle cui pagine un apparecchio molto simile al disco dell'Alberti, composto di cerchi concentrici recanti le lettere alfabetiche, serve a ottenere meccanicamente brevi espressioni. Benché né l'autore né l'opera palesino intenzioni di cifratura o decrittazione, il testo è interamente cifrato e il meccanismo di Fontana ricorda molto da vicino quello albertiano, che forse – tuttavia – non ebbe modo di conoscere la sua opera. Il Secretum era stato trascritto quasi interamente in cifra, a partire dal testo latino in chiaro, probabilmente intorno al 1420, grazie all'operato di copisti che lo riempirono di errori e imperfezioni. Fontana aveva individuato nell'alfabeto latino alcuni gruppi di lettere che potevano essere riunite sulla base di criteri geometrici anziché sull'analogia fonetica. Vocali e consonanti potevano essere ridotte a due soli segni e alle loro combinazioni: il circolo "O" e la linea, sempre presente tranne che nella vocale *i*. Il primo gruppo era appunto quello delle vocali, dove la i svolgeva funzione mediana da copula mundi (a, e, i,

la A estus tiuj kiuj rilatas la armeon, kaj tiel plu). Je la fino de ĉiu frazo la tabelo indikos krome la kongruan numeron, tiel ke dum la ĉifrado la serĉado de la ĉifro sendinda per la minuskla kodo estas pli tuja.

. Kiel povis espliki supremenciita Augusto Buonafalce, la uzo de la ĉifranta disko ne estas prerogativo de Alberti, kvankam li ekuzis en la *Trivia senatoria*, skribita pli frue ol la *De cyfris*. Ne estas certe ke Alberti konis Raimondo Lullo (sed ĝi estas tre verŝajna) kaj ne estas konvene memori la efikecon kiun la aplikadon de siaj normoj havis en la variaj fakoj de la scio inter la Renesanco kaj la Baroko. Plivere, kongruante kun Buonafalce, la pli ĉarma hipotezo ŝajnas resendi al la influo de la samtempulo Giovanni Fontana[23], aŭtoro de la memorateknika verko *Secretum de Thesauro*, en kies paĝoj aparato pli simila al la disko de Alberti, kiu konsistas el samcentraj cirkloj kun la alfabetaj literoj, servas akiri aŭtomate mallongajn esprimojn. Kvankam nek la aŭtoro nek la verko malkaŝas intencojn de ĉifrado aŭ deĉifrado, la teksto estas tute ĉifrita kaj la mekanismo de Fontana memoras pli multe tion de Alberti, kiu eble tamen ne povis koni lian verkon. La *Secretum* estis transskribita per ĉifro preskau tute, kaj deiris de la klara latina teksto, verŝajne ĉirkaŭ 1420, per la agado de kopiistoj kiuj plenigis ĝin de erarojn kaj neperfektaĵojn. Fontana trovis en la latina alfabeto kelkajn grupojn de literoj kiuj povis esti rekunigitaj surbaze de geometria kriteriojn antastaŭ ol fonetika analogio. Vokaloj kaj konsonantoj povis esti reduktitaj al du solaj signoj kaj al iliaj aranĝoj: la cirklo "O" kaj la linio, ĉiam ĉeestas krom en la *i*. La unua grupo estis ĝuste tiu de la vokaloj, kie la *i* havis la meza tasko de *copula mundi* (a, e, i, o, u) kaj tial eble ĝi estis simboligita de la pura signo, la cirklo. Kiam maldekstre al ĝi oni aldonis linion, proksimume akirante signon kiel ĉi tiu,

o, u) e per questo probabilmente era rappresentata dal segno puro, il circolo. Quando alla sua sinistra veniva aggiunta una linea, più o meno in un segno come questo, -o, allora la *i* si tramutava in *a*. Se il segno veniva applicato a destra, in questo modo, o-, allora si otteneva una u e così via, lungo un alfabeto simbolico che si organizzava in altri gruppi, come quello rappresentato da *c*, *h* e *k*, o ancora da *b*, *d*, e *l*. Con questo alfabeto *secreto* i copisti tradussero il *Secretum*, che del resto titolava in chiaro gli intenti di oscura segretezza del suo autore, i quali non avrebbero resistito alla decrittazione dello studioso Eugenio Battisti e, due secoli prima (forse nel 1721), di Carolus Lisca*secreto*[22]. Benché si sia molto insistito su un presunto legame fra Fontana e Alberti, è altresì da rimarcare la profonda differenza fra la straordinaria officina del fantastico che anima le macchine cifranti del primo e il rigore dimostrativo che accompagna l'analisi del secondo, dopo Leonardo forse l'incarnazione più nobile dell'idea quattrocentesca di uomo universale. Di lui vale la pena ricordare, come ha fatto David Kahn, ciò che scrisse John Addington Symonds:

-o, tiam la *i* transŝanĝis en *a*. Se la signo estis aldonita dekstre, tiele, -o-, tiam oni obtenis *u* kaj tiel plu, laŭ simbola alfabeto kiu organiziĝis en aliaj grupoj, kiel tiu, kiu estis reprezentita de *c*, *h* kaj *k*, aŭ ec *b*, *d*, kaj*l*. Per ĉi tiu *secreto* alfabeto la kopiistoj tradukis la *Secretum*, kiu cetere montris klare la celojn de malklara sekreteco de sia aŭtoro, celoj kiu ne rezistos la deĉifrado de la spertulo Eugenio Battisti kaj, du jarojn antaŭe, de Carolus Liska[24]. Kvankam oni multe insistis pri ligon inter Fontana kaj Alberti, same estas rimarkinda la profunda diferenco inter la eksterordinata uzino de la mirindeco kiu animas la ĉifrantajn maŝinojn de la unua kaj la demonstracia rigoro kiu akompanas la analizon de la dua, kiu post Leonardo estas eble la pli nobla enkarniĝo de la dekkvinjarcenta ideo de universala viro. Pri li estas tute peninde memori, kiel fasis David Kahn, tion kiu John Addington Symonds skribis:

> quell'uomo di multiforme ingegno venne al mondo troppo presto per il perfetto esercizio delle sue singolari facoltà. Lo si consideri dal punto di vista dell'arte, della scienza o della letteratura, egli occupa di volta in volta il posto del precursore, del pioniere, dell'antesignano. Sempre originale e sempre fertile l'Alberti intravide terre in cui non ebbe il privilegio di mettere piede, lasciando dietro di sé il ricordo di una grandezza dalle molte facce ma dai contorni incerti, invece che un solido monumento.[25]

Note / Notoj

[1]*Emporio di utili cognizioni*, Pomba, Torino 1835, I, pp. 244-245.
[2]*Emporio di utili condizioni*, Pomba, Torino 1835, I, pp.244-245.
[3]*I Secreti de la Signora Isabella Cortese*, in Venetia, appresso Giovanni Bariletto, MDLXI, lib. II, cap. VII, c. 16 b.
[4]Cfr. M. Rizzardini, "*Lo strano caso della Signora Isabella Cortese, professoressa di secreti*", Philosophia, II, 1/2010, pp. 45-84.
[5]Secondo il biografo G. Mancini (*Vita di Leon Battista Alberti*, Carnesecchi, Firenze 1911), la famosa passeggiata non può essere avvenuta prima del 1466 e non oltre il 17 agosto 1467, giorno del titolo vescovile conferito al Dati. Questo significa che l'Alberti produsse il suo rivoluzionario metodo crittografico polialfabetico nello spazio di un anno e mezzo al massimo.
[6]Laŭ la biografo G. Mancini (*Vita di Leon Battista Alberti*, Carnesecchi, Firenze 1911), la fama promeno ne povis okazi antaŭe 1466 kaj ne post la 17 agosto 1467, tago en kiu la episkopa titolo estis atribuita al Dati. Ĉi tiu signifas ke Alberti produktis suan revolucian kriptografian polialfabetan metodon en maksimume unua kaj duona jaro
[7]Leon Battista Alberti, *Dello scrivere in cifra*, premessa di D. Kahn, introduz. di A. Buonafalce, Galimberti, Torino 1994, p. 4.
[8]Leon Battista Alberti, *La prima grammatica della lingua volgare*, a cura di C. Grayson, Commissione per i testi di lingua, Bologna 1964, pag. xxxvii.
[9]Cfr. A. Buonafalce, *Leon Battista Alberti e l'invenzione della cifra polialfabetica*, introduz. di P. Preto, pubblicaz. stampata dall'autore.
[10]Cfr. M. Rizzardini, "Saturno, Giove, Marte e Filippo: le quattro chiavi del Codice Bellaso / Saturno, Jupitero, Marto kaj Filippo: la kvar ŝlosiloj de la Kodo de Bellaso", *Inkoj*, vol. I, n. 2.
[11]*De vita duodecim Caesarum libri VIII*, cap. 56.
[12]Leon Battista Alberti, *La prima grammatica della lingua volgare*, editoris C. Grayson, Commissione per i testi di lingua, Bologna 1964, p. xxxvii.
[13]Onividu A. Buonafalce, *Leon Battista Alberti e l'invenzione della cifra polialfabetica*, enkonduko de P. Preto, eldono presita de la aŭtoro.
[14]Onividu M. Rizzardini, "Saturno, Giove, Marte e Filippo: le quattro chiavi del Codice Bellaso / Saturno, Jupitero, Marto kaj Filippo: la kvar ŝlosiloj de la Kodo de Bellaso", *Inkoj*, vol. I, n. 2.
[15]*De vita duodecim Caesarum libri VIII*, cap. 56.
[16]Cfr. A. Buonafalce, op. cit., p. 14.
[17]Onividu A. Buonafalce, *cita verko*, p. 14
[18]D. Kahn, *La guerra dei codici. La storia dei codici segreti*, Mondadori, Milano 1967, pp. 75-80.
[19]D. Kahn, *La guerra dei codici. La storia dei codici segreti*, Mondadori, Milano 1967, pp. 75-80.
[20]Alberti nomas *kunaranĝitoj* tiuj konsonantok kiuj kutime sekvis unu la alian en pli oftaj silabaj renkontoj.
[21]Cfr. E. Battisti, G. Saccaro Battisti, *Le macchine cifranti di Giovanni Fontana*, Arcadia, Milano 1984.
[22]Ivi, p. 142.
[23]Onividu E. Battisti, G. Saccaro Battisti, *Le macchine cifranti di Giovanni Fontana*, Arcadia, Milano 1984.
[24]Tie, p. 142.
[25]D. Kahn, op. cit., p. 80.

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