UNIVERSITAT DE BARCELONA

Treball final de grau

GRAU DE MATEMÀTIQUES

Facultat de Matemàtiques i Informàtica
Universitat de Barcelona

Anàlisi i contextualització del *Traicté des Chiffres* de Blaise de Vigenère

---

Autor: Pau Cantal Rovira

Director: Dr. Carles Dorce i Polo
Realitzat a: Departament de Matemàtiques i Informàtica
Barcelona, 19 de gener de 2018

Abstract

In this work we give an analysis of how Blaise de Vigenère described the cipher that has been attributed to him. For that purpose, we study directly from the *Traicté des Chiffres*. We also explain the context of his work and show the evolution of cryptology as to understand how the autor came up with his cipher.

Resum

En aquest treball es fa una anàlisi de com Blaise de Vigenère va descriure a la seva obra el mètode de xifrat que li ha estat atribuït. Per tal de realitzar-ho, s'indaga directament del *Traicté des Chiffres*. També es posa en context l'obra de Vigenère, i es traça l'evolució que han sofert els mètodes de xifrat per tal d'entendre com l'autor va arribar a desenvolupar la seva xifra.

Agraïments

En primer lloc m'agradaria agrair profundament a la meva parella l'ajuda i consells que m'ha donat a l'hora de redactar aquest treball, i durant tota la carrera en general. Agraeixo també al meu tutor, Carles Dorce, qui em va proposar el tema i m'ha guiat al llarg del treball. Finalment, a la meva família, sense la qual no hagués arribat fins aquí.

Fent referència al físic i escriptor C. P. Snow, espero que aquest treball uneixi, una mica més, les dues cultures: la ciència i les humanitats.

Índex

1 Introducció **1**

1.1 Metodologia 2

2 Conceptes bàsics i nomenclatura **2**

3 Inicis de la criptografia **3**

4 Criptoanàlisi Àrab **5**

4.1 Context històric 5

4.2 Primeres referències 5

4.3 Desenvolupament de la criptoanàlisi 6

4.4 Altres criptògrafs àrabs 8

5 La criptografia a Occident **8**

5.1 Context històric 8

5.2 Giovanni Soro (m.1544) 10

5.3 François Viète (1540-1603) 11

6 Influències de Vigenère **12**

6.1 Leon Battista Alberti (1404-1472) 12

6.2 Johannes Trithemius (1462-1516) 14

6.3 Girolamo Cardano (1501-1576) 17

6.4 *La cifra del Sig. Giovan Battista Belaso* 18

6.5 Giambattista della Porta (1535-1615) 24

7 Blaise de Vigenère (1523-1596) **25**

7.1 Traicté des Chiffres 27

7.2 *Le chiffre indéchiffrable* 34

8 Conclusions **39**

1 Introducció

La Criptografia, del grec *Kryptós* (ocult) i *Grafé* (grafia o escriptura) és l'estudi dels mètodes de xifrat i desxifrat usats per tal d'assegurar que un missatge enviat pugui arribar al receptor sense que un tercer pugui obtenir el significat del missatge, encara que aquest l'intercepti. Molt lligat a aquest concepte es troba l'*esteganografia*, del grec *steganos* (cobert). Els mètodes esteganogràfics no xifren el missatge sinó que l'amaguen físicament per tal de que passi desapercebut als possibles interceptors i arribi segur al destinatari.

Al segle V aC, en *La Història* d'Heròdot, es troben relats sobre l'ús de tècniques esteganogràfiques. Heròdot relata com Grècia va guanyar la guerra contra l'exèrcit persa en la batalla de Salamina gràcies a Damaratos, un ciutadà grec expulsat de la seva terra i que vivia en territori persa. Aquest, en assebentar-se del que preparaven els perses, va enviar una tauleta de fusta a Grècia. En la tauleta hi va grabar el missatge i llavors el va cobrir amb cera, la qual amagava el text. En escalfar i retirar la cera els grecs van poder preveure l'atac de l'exèrcit persa. L'esteganografia amaga el text físicament, de manera que els interceptors no el puguin trobar, en canvi, una de les bases de la criptografia és que des del principi suposa que l'interceptor ha aconseguit el missatge però aleshores no el podrà entendre. Al segle XIX, l'holandès Auguste Kerckhoffs von Nieuwenhof (1835-1903), lingüista i criptògraf militar, en un article anomenat *La Cryptographie Militaire* publicat a *Le Journal des Sciences Militaires* estableix 6 principis que encara regeixen la criptografia. Kerckhoffs els enumera de la següent manera:

> 1º Le système doit être matériellement, sinon mathématiquement, indéchiffrable;
>
> 2º Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi;
>
> 3º La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants;
>
> 4º Il faut quìl soit applicable à la correspondance télégraphique;
>
> 5º Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes;
>
> 6º Enfin, il est nécessaire, vu les circonstances que en commandent l'apllication, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.(Kerckhoffs, 1883:12)

L'obra de Kerckhoffs va ser la més completa i precisa que s'havia escrit fins al moment, mostrant un complet i estricte coneixement de la criptografia. La criptografia, ja molt abans de Kerckhoffs, s'havia convertit en una ciència indispensable en molts camps del coneixement.

L'evolució dels mètodes de xifrat antics culminà amb l'obra de Blaise de Vigenère (1523-1596), el *Traicté des Chiffres, ou Secrètes Manières d'Escrire*. En aquest treball es traçarà la història de la criptografia des dels seus inicis i s'analitzarà l'obra de Vigenère tal i com la va presentar ell.

1.1 Metodologia

Al llarg del treball s'han consultat els llibres o articles que apareixen a la bibliografia. Tanmateix, l'obra principal del treball, el *Traicté des Chiffres*, i l'obra de Belaso, apareixen sovint citats en l'idioma en què foren escrits. D'aquesta manera, el lector més versat en l'italià i el francès podrà conèixer directament com aquests dos autors descrigueren els seus mètodes de xifrat. No obstant això, cada cita que apareix en aquest treball està comentada i explicada d'una manera actual i formal.

2 Conceptes bàsics i nomenclatura

Per tal d'usar una nomenclatura general i actual fixarem els conceptes que més endavant usarem a l'hora de referir-nos a un criptosistema determinat. Usarem la nomenclatura de [8]. Així doncs anomenarem *text en clar* o *text inicial* al text abans d'aplicar el mètode de xifrat i *text xifrat* o bé, tal com apareix usualment en la literatura, *criptograma* al text obtingut en aplicar el mètode de xifrat. Quan no hi hagi confusió simplement anomenarem *text* al text en clar. Anomenarem *alfabet* al conjunt de caràcters que poden formar el text en clar i *unitat de missatge* a la mínima part que constitueix el text. Les unitats de missatge poden constar d'una lletra, de dues (*dígraf*) o, en general, de k lletres (k-*grafs*).

Definició 2.1. Sigui U_i el conjunt de totes les possibles unitats de missatge del text inicial i U_x el conjunt de les unitats de missatge del text xifrat. Aleshores anomenarem *transformació xifradora* a una aplicació $f : U_i \longrightarrow U_x$ que sigui bijectiva. A l'aplicació inversa f^{-1} l'anomenarem *transformació desxifradora*. Imposem que f sigui bijectiva, perquè si no, dos textos diferents tindrien un mateix text xifrat i aleshores no podríem saber de quin text prové. S'anomena *criptosistema* al conjunt format per U_i, U_x i per la parella f, f^{-1}.

Existeixen dos tipus diferents de criptosistemes: els *clàssics* o de *clau privada o simètrica* i els de *clau asimètrica* o de *clau pública*. Per fer-nos-en una idea, en els mètodes clàssics existeix una *clau* del criptosistema i aquesta es manté en secret. En canvi, als mètodes de clau pública s'utilitza fonamentalment la teoria de nombres, com ara l'aritmètica modular i el fet que és possible saber si un número és primer o no a partir de tests de primalitat. Tot i així, és molt difícil poder descompondre un nombre gran en els seus factors. Els mètodes de clau pública sorgiren als anys 70 quan Whitfield Diffie i Martin Hellman van publicar la idea base d'aquests en un article anomenat *New Directions in Cryptography*. Aquesta idea permet intercanviar les claus d'un criptosistema de manera segura. Tanmateix, donades les característiques d'aquest treball només estudiarem el desenvolupament dels mètodes clàssics o de clau privada.

Els mètodes anomenats clàssics es poden dividir en dos grups: els de *substitució* i els de *transposició*.

Definició 2.2. S'anomenen xifrats per transposició als mètodes en què s'aplica una permutació a les unitats de missatge.

Per xifrar un text usant un algoritme de transposició format per k unitats de missatge tindríem $k!$ possibles maneres de xifrar-lo. En aquests mètodes la funció bijectiva f s'aplica sobre la posició de cada unitat de missatge.

Definició 2.3. Els mètodes de substitució consisteixen en reemplaçar les unitats de missatge per d'altres mitjançant un algorisme o mètode concret. Aquests es poden subdividir en *codis* o bé *xifres*. Als codis es canvia el significat de paraules senceres i a les xifres s'alteren les identitats de les unitats de missatge.

La diferència bàsica entre els xifrats per transposició i els xifrats per substitució rau en què en els primers no s'altera la identitat de les unitats de missatge, sinó només l'ordre. En canvi, en els segons, s'altera la identitat però no l'ordre. Una traducció més actual per als mètodes clàssics del 2n principi de Kerckhoffs seria que la fortalesa d'un criptosistema clàssic no ha de dependre de mantenir en secret l'algoritme emprat, sinó que només dependrà de mantenir en secret la clau.

Usualment als mètodes clàssics, el conjunt U_i i U_x seran el mateix i de la forma $\mathbf{Z}/N$, on N serà el nombre de lletres de les que compta un determinat alfabet, i les unitats de missatge seran les pròpies lletres de l'alfabet. Així, cada lletra quedarà representada per un nombre. Per exemple, en català tindríem $N = 26$ i la bijecció g entre el conjunt {0,1,2,...,25} i {a, b, c,..., z} vindria donada per $g(0) = a$, $g(1) = b$,..., $g(25) = z$.

També cal fer una distinció entre les anomenades xifres *monoalfabètiques* i les *polialfabètiques*. En les xifres monoalfabètiques un mateix alfabet és utilitzat per xifrar tot el text en clar. En canvi, en les xifres polialfabètiques s'utilitzen diversos alfabets per a xifrar les unitats de missatge. És a dir, cada unitat de missatge del text en clar podrà quedar xifrada per diferents unitats de missatge del text xifrat.

Als xifrats polialfabètics, sovint s'utilitzarà la notació $f_{k_i}(x_i) = y_i$ per indicar amb quina clau es xifra cada lletra. $k_0, k_1, ..., k_{n-1}$ denotarà la clau, i x_i, y_i per $i = 0, ..., n-1$ denotaran el text en clar i xifrat respectivament.

3 Inicis de la criptografia

Ja s'ha relatat que al segle V a.C, a *La Història d'Herodot*, es parla de mètodes esteganogràfics. Al segle I aC, a l'obra de Plutarc *Vida de Lisandre*, es descriu el que podria ser el primer instrument criptogràfic usat per a finalitats militars. Es tracta de l'escítala grega, un bastó de fusta amb un pergamí enrotllat al seu voltant a on s'hi havia escrit el missatge. Quan el pergamí es desenrotllava, quedaven una sèrie de lletres sense significat aparent. Per desxifrar el missatge, el receptor -que disposava d'una escítala amb el mateix diàmetre- només havia de tornar a enrotllar el pergamí al voltant del bastó per comprendre el text. Per tant, es tracta d'un sistema de transposició en què la longitud del diàmetre del bastó és el factor que canvia l'ordre de les lletres. Polibi, al segle II a.C., historiador igualment del món grec, descriu un mètode més elaborat que n'inspirarà de més moderns. Utilitzant l'alfabet llatí i la numeració actual i ajuntant les lletres i i j en una mateixa casella

per fer coincidir l'alfabet en una taula 5x5 [tal com fa Khan, 1996:83] el criptosistema és el següent:

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

Es substitueix cada lletra pels nombres de la seva columna i fila. En forma matricial, $a_{ij} = ij$ on $i, j = 0, 1, 2, 3, 4, 5$ i $A = (a_{ij})$ és la taula d'abans en forma de matriu on l'element $a_{11} = 0$ (no té rellevància).

Dins del món romà trobem un dels criptosistemes més coneguts. L'ús d'aquest criptosistema es troba narrat a *De Bello Gallico o La Guerra de les Gàl·lies* de Juli Cèsar (100 aC-44 aC). És, però, a través de l'obra de Suetoni (S.I-II), *La vida dels dotze Cèsars*, que ens arriba la informació sobre com era aquest criptosistema. Es tracta d'un sistema de substitució que desplaça les lletres de l'alfabet tres posicions endavant. En el llenguatge actual, i utilitzant l'alfabet en català, la funció és de la forma $f : \mathbf{Z}/25 \to \mathbf{Z}/25, f(x) = x + 3 \pmod{25}$. Sovint s'anomena "xifrat de Cèsar"al mateix mètode però en una visió més general, és a dir, utilitzant un alfabet de N lletres i considerant unitats de missatge d'una lletra. Aleshores tenim que $f : \mathbf{Z}/N \to \mathbf{Z}/N, f(x) = x + r \pmod{\text{N}}$ on $0 < r < N - 1$. Òbviament $f^{-1}(y) = y - r \pmod{\text{N}}$. En aquest xifrat, r és la clau del criptosistema. Notem que aquest és un criptosistema poc segur, ja que, en el cas de N=25, només hi ha 24 possibles claus. L'obra de Suetoni sembla exposar que l'ús de mètodes rudimentaris de xifrat era freqüent en l'època de Juli Cèsar, utilitzant també codis en què, per exemple, Sampsiceramus es referia a Pompeia.

No només en el continent europeu trobem exemples de l'ús de la criptografia. A la cultura índia, a l'obra més famosa de Vâtsyâyana (S. II dC), el *Kâma Sûtra*, s'hi troba anomenada l'art de l'escriptura secreta, mlecchita vikalpâ. En comentaris a aquest text es descriuen diferents mètodes basats en la sonoritat de les lletres. Per exemple, el *kautiliyam* consisteix en substituir lletres segons les seves similituds fonètiques (p.e. les vocals esdevenen consonants). (Kahn, 1996:74). A l'Antic Testament també s'hi troben paraules que s'han xifrat per substitució amb el que es coneix com "atbash". Aquesta xifra consisteix en substituir la primera lletra per l'última, la segona per la penúltima, etc. Es pot descriure com $f(x_i) = -x_i + (N + 1) \pmod{\text{N}}$. Molts altres xifrats s'han utilitzat al llarg de la història amb l'alfabet hebreu per la seva relació amb la Càbala jueva. Fent un salt en el temps, al Tibet també es té constància d'un mètode anomenat *rin-spungs* pel seu creador *Rin chen spungs pa* que va viure als voltants de l'any 1300 dC. L'ús de la criptografia sembla aparèixer en qualsevol cultura desenvolupada arreu del món, inspirat per la necessitat de privacitat tant a nivell oficial, militar com personal.

4 Criptoanàlisi Àrab

4.1 Context històric

Tret de casos molt puntuals, no es té constància d'estudis sobre criptoanàlisi en l'època romana o grega. La criptoanàlisi, com moltes d'altres ciències actuals, sorgirà al món àrab.

L'Islam sorgí al voltant de l'any 610 dC entorn de la ciutat de la Meca, quan al profeta Mahoma li van ser revelades les ensenyances que es convertirien en el sagrat Alcorà. Aquest llibre va ser escrit per Abû Bakr, primer califa de l'Islam i successor de Mahoma després de la seva mort, ocorreguda el 8 de març de l'any 632. Era responsabilitat dels califes estendre el missatge de Mahoma, i van ser els tres primers els que van recopilar els 114 capítols o sures que conté l'Alcorà. Quan va sorgir, l'Islam va topar amb les creences anteriors i els musulmans es van exiliar a Medina. Des d'allà seguiren en guerra contra els opositors de la Meca fins que els seguidors de Mahoma van conquerir la ciutat natal del seu profeta l'any 630. Des dels inicis de l'Islam fins ben bé el segle VIII, va tenir lloc un període de guerres i conquestes. El califat d'Abû Bakr durà només 2 anys i el seu successor, Umar ibn al-Khattâb (*c.*581-644), va ser qui acabà les conquestes de bona part de l'Imperi Persa i l'Imperi Bizantí. Aquests territoris s'expandien des de la Península Ibèrica a Occident, i fins a l'Índia, a l'Orient. Durant els dos califats següents hi hagué un període de revoltes que acabaren amb l'establiment del primer Califat Omeia, que donà lloc al Xiisme.

Quan el seu domini sobre els territoris es va consolidar, el món islàmic va gaudir d'una estabilitat i d'una pau que van afavorir el desenvolupament de tota mena d'arts i ciències. Durant l'edat d'or àrab, regnava la dinastia Abbàssida; el seu objectiu no era l'expansió territorial, sinó la construcció d'una societat més organitzada i pròspera. Traslladada la capital a Bagdad, l'any 815 el califa Al-Ma'mûn (786-833) va fundar la *Bayt al-Hikmah* o Casa de la Saviesa, que consistia en una biblioteca i un centre de traducció que importaria textos de totes les grans cultures que el món àrab havia conegut arran dels intercanvis comercials i culturals. Aquests textos, provinents de Grècia, Egipte i fins i tot l'Índia, van ser traduïts a l'àrab per diversos savis. D'aquesta manera, tot aquest coneixement va poder arribar als estudiosos àrabs.

4.2 Primeres referències

A l'any 855 l'erudit Abû Bakr Ahmad ben 'Alî ben Wahshiyya an-Nabatî, a la seva obra *Kîtab Shawq al-Mustahâm* (*El molt desitjat complert coneixement d'alfabets ocults*), on hi desxifrà diversos jeroglífics egipcis basant-se en l'escriptura copte, va incloure diversos mètodes de xifrat tradicionals per a usos "màgics" l'objectiu dels quals era desxifrar passatges de textos religiosos antics. L'ús i la importància de la criptografia queden plasmats en nombrosos manuals per a l'administració, com per exemple l'*Adab al-Kuttab*, del segle X, que conté un apartat dedicat a la

criptografia. El gran filòsof àrab Abû 'Abd al-Rahmân al-Khalîl ibn Ahmad ibn 'Amr ibn Tammâm al Farâhidi al-Zadï al Yahmadî (c. 718-791) va escriure el *Kitâb al-mu'ammâ* (*LLibre del Llenguatge Secret*), obra que no ha arribat fins als nostres dies. L'autor es va inspirar amb el desxiframent d'un missatge de l'emperador Bizantí, proesa que ell mateix havia dut a terme. En aquella època sovint els missatges s'escrivien d'una manera protocol·lària usant, per exemple, alabances a Déu o a l'emperador. Al-Khalîl aprofita aquest fet i escriu (KHAN, 1996:97):

"Em vaig dir a mi mateix, la carta ha de començar 'En nom de Déu' o alguna cosa semblant. Així que vaig resoldre les primeres lletres, i [la resposta] vingué a mi."

El fet que es descrigui que al-Khalîl va tardar un mes a desxifrar aquest missatge posa en evidència que en aquells moments encara no s'havia desenvolupat o, si més no, estès, l'ús de mètodes de criptoanàlisi.

4.3 Desenvolupament de la criptoanàlisi

Com va sorgir el primer mètode de criptoanàlisi (*Attargama* en àrab) o el que es coneixerà com *anàlisi de freqüències*? L'origen de l'anàlisi de freqüències es troba en un context religiós. Gran nombre d'erudits religiosos instal·lats a Kufa, Basra i Bagdad -a l'actual Iraq- intentaven fer un anàlisi cronològic de l'Alcorà i extreure'n el seu significat complet. Per tal de fer-ho, estudiaven el nombre d'aparicions de determinades paraules que estaven en ús en l'època del profeta Mahoma, tot fent anàlisis etimològics i gramaticals de les paraules i frases que hi apareixien. Així, si en un determinat capítol o sura s'hi trobava gran part d'aquestes, se li atribuïa un origen més proper a l'època de Mahoma. Classificaren les paraules segons si eren natives àrabs o bé si provenien de llengües estrangeres. Observaren que en les paraules àrabs certes lletres es repetien més sovint, i d'altres apareixien quasi sempre al costat de les mateixes, tot creant dígrafs. Per exemple, establiren que, en àrab, el dígraf *al* apareixia moltes vegades degut a l'article definit 'al-', i per tant, les lletres *alif*(a) i *lâm* (l) eren les lletres d'aparició més comuna en els textos; en canvi, la lletra *zâ'*(z) era la menys comuna.

L'any 1987, a l'Arxiu àrab Otomà d'Istanbul, s'hi va trobar el que segurament és el manuscrit més antic que ens ha arribat sobre l'art del criptoanàlisi. Aquest text es titula *Risâla fî Istikhrâj al-Kutub al-Mu'amâh* (*Sobre el desxiframent dels missatges xifrats*) i fou escrit pel pare de la filosofia àrab, Abû Yûsuf Ya'qûb ibn 'Ishâq as-Sabbâh al-Kindî (c.800-870), també conegut pel seu nom llatinitzat Alkindus. Al-Kindî no va destacar només com a filòsof; va escriure sobre astronomia, òptica, medicina, química, matemàtiques, criptografia i també sobre música. Formà part d'un grup de traductors que treballaven en obres sobre matemàtiques, ciència i filosofia grega, i es creu que va estar molt influenciat per aquestes. Al-Kindî començà l'*al-Mu'amâh* remarcant la importància que tenia al seu moment un tractat sobre criptoanàlisi tot dient:

> Entenc, que el vostre coneixement i comprensió sempre augmenti, el que m'ha ordenat d'escriure. Vol un llibre on s'hi descriguin els mètodes de criptoanàlisi

> per a cartes xifrades; un llibre que ha de ser clar i concís. Lloat sigui el Senyor que et donà un motiu per ajudar a la gent amb un dels més grans i negligits beneficis.[...] Us ho dic, que Déu us allargui la vida, i us millori la vostre situació, que el criptoanàlisi ofereix el millor dels avantatges, ja que molts filòsofs i científics antics usaven símbols a les seves obres. (Mrayati, Alam, Tayyan, 2003:119-120)

L'obra es divideix en diversos apartats, on es descriuen mètodes criptogràfics, tot separant-los segons si són xifrats de transposició o bé de substitució. Va introduir també la idea d'afegir caràcters nuls al xifrat per tal de dificultar la tasca als possibles atacants. En d'altres apartats explicà mètodes de criptoanàlisi segons la xifra que s'hagi usat. Al-Kindî descrigué la freqüència d'aparició de les lletres com:

> La lletra 'alif' és la més freqüent en l'àrab. Altres lletres són ordenades en ordre decreixent, segons la seva freqüència com segueix: l, m, h, w, y, n, r, f, t, b, k, d, [...]. Hem dit anteriorment que les vocals són més freqüents a totes les llengües, ja que són el subjecte bàsic del llenguatge, i altres fonemes apareixen amb elles.(Mrayati, Alam, Tayyan, 2003:166)

Seguidament, va fer una anàlisi exhaustiva sobre quines lletres poden aparèixer juntes i quines són les més freqüents. Va fer recomptes en taules de freqüències basant-se en set fulls escrits en àrab per tal de tenir una mostra representativa sobre quines lletres apareixien més assíduament. La idea bàsica de l'anàlisi de freqüències la descrigué amb claredat de la manera següent:

> Entre les maneres que usem a l'hora de criptoalanalitzar un criptograma si la llengua és coneguda, una és obtenir un text en clar prou llarg en aquella llengua, i comptar el nombre de vegades que apareix cada lletra. Marquem la més freqüent 'primera', la segona més freqüent 'segona', i la següent 'tercera', i així continuem fins a cobrir totes les lletres restants. Llavors tornem al missatge que volem desxifrar, i classifiquem els diversos símbols, cercant el més freqüent del criptograma i la fem correspondre amb la mateixa lletra que hem marcat 'primera' - al text en clar-; aleshores anem a la segona lletra i la fem correspondre amb la que hem marcat 'segona' i la propera 'tercera', fins a exhaurir tots els símbols que apareixen al criptograma per desxifrar.
>
> Podria passar a vegades que es trobin criptogrames curts, massa curts per contenir tots els símbols de l'alfabet, on l'ordre de la freqüència de les lletres no pugui ésser aplicat. En efecte l'ordre de la freqüència de les lletres pot ésser aplicat en textos llargs, on la falta de lletres en una part és compensada per l'abundància d'aquestes a una altra part. (Mrayati, Alam, Tayyan:124)

L'exposició del mètode de criptoanàlisi d'al-Kindî, actualment es coneix com *anàlisi de freqüències*. En qualsevol llengua és fàcil trobar les freqüències de cada lletra. Si disposem d'un missatge xifrat -per un criptosistema clàssic- i el volem desxifrar, en un primer intent comptaríem la freqüència de les lletres que apareixen al text xifrat. Al-Kindî anomenà "primera"a la lletra amb més aparicions dins el text, i "segona"a la següent lletra amb més aparicions, i així continuà. Aleshores, si x_0 és la xifra

amb més aparicions dins el text xifrat, podríem suposar que $f(y_0) = x_0$ on y_0 és la xifra més comuna en l'alfabet que s'ha usat. L'anàlisi que va fer al-Kindî anà més enllà de comptar les repeticions de cada lletra. Coneixent profundament les normes gramaticals i lèxico-gràfiques, estudià quins dígrafs, trígrafs, etc... apareixien amb més freqüència, i els va tabular. Per tant, era encara més possible desxifrar un text tenint en compte l'estructura de la llengua.

4.4 Altres criptògrafs àrabs

Als segles XIV i XV la sistematització de l'ús de la criptografia es fa palesa a la obra *Subh al-a 'sha*, de l'egipci Shihâb al -Dîn abu'l-'Abbâs Ahmad Ali Ahmad Abd Allâh al-Qalqashandî, acabada al 1412. El *Subh al-a'sha* és una enciclopèdia de 14 volums dirigida a la classe administrativa. En aquests s'hi inclou una secció dedicada a la criptografia, on l'autor exposa, de manera semblant els conceptes que al-Kindî ja havia introduït en l'*al-Mu'amâh*. Qalqashandî atribuí gran part del coneixement sobre criptografia que ell exposà a Tâj ad-Dîn Alî ibn ad-Duraihim Muhammad ath-Tha'âlibî al-Mausilî, qui visqué entre els anys 1312 i 1361. L'obra d'al-Qalqashandi és remarcable, ja que fins fa relativament poc es creia que era el primer text àrab en exposar els principis de l'anàlisi de freqüències. El fet que l'obra d'al-Kindî no es trobés fins l'any 1987 va fer creure que els orígens de la criptoanàlisis es trobaven al segle XV, lligats a la figura de Leon Battista Alberti.

5 La criptografia a Occident

5.1 Context històric

Com s'ha vist, entre els segles VIII i XIV es van escriure grans obres sobre l'ús de la criptografia i la criptoanàlisi al món àrab. L'obra d'al-Qalqashandî mostrà que per la classe administrativa era de vital importància la coneixença de mètodes per a xifrar i desxifrar missatges "ocults". No obstant això, en el continent europeu no va succeïr el mateix. Mentre que entre els àrabs van ser escrits molts textos sobre criptografia, no es té constància d'obres rellevants similars a Europa. Si bé l'ús de la criptografia es va mantenir de forma ininterrompuda, aquesta no va avançar durant aquest període. A l'epístola titulada *On the nullity of magic* escrita al segle XIII pel filòsof i científic franciscà Roger Bacon (c.1214-1294), es descriuen almenys sis mètodes de substitució i, un segle més tard, dins de *A treatise on the astrolabe* de Geoffrey Chaucer (c.1343-1400), hi apareixen diversos paràgrafs xifrats que constaten que, almenys entre els més erudits, la criptografia seguia essent utilitzada.

Durant l'Edat Mitjana l'Església i, en particular, els Estats Pontificis, tenien molt de poder i per tant és d'esperar trobar també als Arxius Vaticans que hi hagi documents que deixin constància de l'ús de codis i xifres: llistes de codis que daten aproximadament del 1326 donen exemples de quins codis s'utilitzaven. La majoria dels codis sorgien d'abreviacions o d'epítets de determinades entitats religioses o socials. Aquestes llistes es van utilitzar durant el conflicte entre güelfs i gibel·lins

-que s'estengué des d'Alemanya fins a Itàlia- i trobem que, per exemple, un codi per designar als gibel·lins era *egipcis* i els güelfs es convertien en *fills d'Israel*. Als Arxius Vaticans també s'hi troben alguns codis més moderns on, per exemple, la lletra A designava al rei, la D al Papa i S al mariscal. Aquests llistats donaran pas als nomenclàtors, que eren una barreja entre xifres (per substitució) i codis on s'utilitzaven els dos mètodes. Aquests nomenclàtors es van utilitzar posteriorment al llarg d'uns 450 anys. La *Gran Xifra* desenvolupada conjuntament per Antoine i Bonaventure Rossignol durant els regnats de Lluís XIII i Lluís XIV és potser la més coneguda usant nomenclàtors. A priori pot semblar que l'ús de codis és més segur que un xifrat per substitució, ja que una paraula pot ésser substituïda per qualsevol altra paraula, lletra, dígraf o, en general, k-graf. Tanmateix per utilitzar un xifrat només cal que l'emissor i el receptor es posin d'acord en la clau del xifrat, mentre que usant codis cal que tant l'emissor com el receptor coneguin el llistat de tots els mots codificats, els quals poden arribar a ser extremadament voluminosos.

El renaixement de la criptografia el trobem a la Península Itàlica. Un fet destacable és que també a aquesta Península és on hi tenen lloc un importants avenços matemàtics gràcies a personatges tals com Girolamo Cardano (1501-1576), Niccoló Fontana (c.1500-1557) i Ludovico Ferrari (1522-1565), coneguts per la resolució de les equacions de 3r i 4t grau; i prèviament degut a Leonardo de Pisa (c.1170-1240), popularment conegut com Fibonacci, que va introduir al *Liber Abaci* (1202), l'ús del sistema de numeració indo-aràbic. Connexions, com la de Fibonacci, amb la cultura àrab plantegen la hipòtesi de que les idees sobre la criptoanàlisi van ser introduïdes a través dels intercanvis culturals que s'establien amb aquesta cultura. Si bé això és possible, la versió més raonable és que es desenvolupés de forma paral·lela als països de l'Europa renaixentista i, per tal de mantenir avantatges sobre els altres territoris en una època convulsa, no es van fer públics els descobriments sobre l'anàlisi de freqüències.

En aquella època, l'actual Itàlia es trobava dividida en ciutats-estats independents, com per exemple Florència, Nàpols, Venècia i els Estats Pontificis al voltant de Roma. La constant amenaça que significaven els estats veïns convertia l'ús de missatges xifrats en quelcom gairebé imprescindible; així, es mantenien segures les comunicacions entre els estats aliats. D'aquesta manera, i a poc a poc, es creen les primeres oficines dedicades completament a la criptografia i també els primers criptògrafs d'ofici. Eren homes que es dedicaven exclusivament a xifrar i desxifrar missatges, tant de l'estat per qui treballaven com possibles missatges interceptats d'altres estats. També els ambaixadors disposaven d'un "secretari de xifres"per tal de poder transmetre d'una forma segura la informació convenient, i alhora per poder interpretar la que arribava, ja que la majoria de diplomàtics i polítics desconeixien el funcionament dels mètodes criptogràfics. L'oficina de xifres més famosa va ser la de Venècia, en especial durant el poder del Consell dels Deu -òrgan de govern que durà des del 1310 fins al 1797-. El Consell dels Deu (*Consiglio dei Dieci* en italià) s'encarregava de mantenir el control sobre la República de Venècia, tot evitant revoltes internes o intromissions de caire polític. Tot això ho feia en bona part mitjançant l'espionatge, i per tant, tot xifrant els seus propis missatges i desxifrant els missatges aliens.

5.2 Giovanni Soro (m.1544)

És dins el context descrit anteriorment quan apareix qui probablement és el primer gran criptoanalista d'Occident. Es tracta de Giovanni Soro que va viure al voltant de l'any 1506, data en què era el secretari de xifres de Venècia. La reputació de Soro com a criptoanalista no només es quedava a Venècia sinó que era reconegut a les altres ciutats-estat i fins i tot a altres països, com França o Espanya. Es desconeixen els detalls de la seva vida i només ens arriba informació de quan desenvolupava la seva funció com a criptògraf a través d'episodis que deixen constància de la seva brillant carrera. L'any 1526 el Papa Clement VII envià a Soro dos missatges xifrats que s'havien interceptat; el primer era entre l'emperador del Sacre Imperi Romanogermànic Carles V, amb els seus emissaris a Roma, mentre que el segon era entre el duc de Ferrara amb el seu ambaixador a Espanya. El Summe Pontífex volia que Soro els desxifrés. El criptoanalista va retornar els dos missatges desxifrats provocant l'admiració de la cúria papal. També és conegut que, en caure un missatge xifrat enviat pel Papa en mans dels florentins, aquest buscà consol en l'il·lustre secretari de xifres venecià tot enviant-li una còpia del missatge interceptat per assegurar la fortalesa del sistema emprat. Soro li respongué que no havia sigut capaç de desxifrar el missatge, tranquil·litzant així al Papa. Tanmateix, és bastant probable que Soro desxifrés el missatge però, per tal de mantenir l'avantatge que això suposava, no ho va comunicar. Als voltants de l'any 1500 escrigué una obra sobre com desxifrar xifres en llatí, italià, espanyol, i francès, però malauradament aquesta obra no ha arribat fins als nostres dies.

El 1542 Giovanni Soro treballava amb dos assistents més al palau del Dux, a Venècia. Quan un missatge era interceptat per la policia del Consell dels Deu, els tres criptògrafs eren tancats a la *Sala di Segret*, i fins que no es desxifrava el missatge no en sortien. L'ofici de criptògraf estava ben remunerat, i fins i tot es duien a terme exàmens per tal de formar-se com a tal. La criptografia passava de ser una "art oculta"a ser de vital importància per les comunicacions oficials dels països o ciutats-estats de la Itàlia renaixentista. Soro establí un xifrat usant varis nomenclàtors, on hi havia una xifra general i d'altres per a ús més específic. Si s'interceptava informació sobre el desxiframent d'algun d'aquests nomenclàtors, automàticament i en un breu període de temps aquests se substituïen per d'altres. A més a més, per tal d'augmentar la seguretat de les comunicacions cada ambaixador usava un nomenclàtor diferent. Després de la mort de Giovanni Soro, Pietro Partenio es convertí fou el principal criptògraf venecià. Partenio continuà creant nous nomenclàtors segons el mètode de Soro.

Es pot dir que durant el Renaixement totes les ciutats-estat disposaven d'un o més secretaris de xifres per a l'enviament de missatges escrits. Els ducs de Sforza, de la ciutat de Milà,per exemple, comptaven, entre d'altres, amb Cicco Simonetta (1410-1480). El 4 de Juliol de 1474 Simonetta escrigué tretze normes per a desxifrar xifrats monoalfabètics, que eren els més utilitzats al moment, i presentà maneres de desxifrar un text, encara que es conegués l'idioma en què estava escrit. Aquesta obra fou la primera dedicada completament i sense dubte a l'estudi de la criptografia.

5.3 François Viète (1540-1603)

Paral·lelament, França estava a punt de viure una època d'esplendor pel que fa al desenvolupament de les matemàtiques en general, gràcies a figures tan conegudes com René Descartes (1596-1650) o Blaise Pascal (1623-1662). Anteriorment, però, destacà un personatge que també va tenir un paper important tant en les matemàtiques (en el sentit més estricte) com en la criptografia. Es tracta de François Viète. Viète va començar els seus estudis a un claustre franciscà i, als 18 anys, estudià dret a la Universitat de Poitiers tal com havia fet el seu pare, Etienne Viète. Allà es va graduar com a Legum Baccalaureus (graduat en dret) l'any 1559. Un any després començà la seva carrera com a advocat a Fontenay-le-Comte. De forma esporàdica, també va treballar per a la reina Leonor de Portugal i França, i oferí serveis a Maria I d'Escòcia. Gràcies a la seva tasca destacada li va ser concedit un títol nobiliari. Al 1564 Viète passà a treballar per Antoinette d'Aubeterre, casada amb el noble Jean V de Parthenay, de la família Soubise. De Parthenay va ser acusat d'haver perdut la ciutat de Lion degut a la seva mala tasca com a comandant de l'exèrcit hugonot, durant el conflicte desencadenat per la reforma protestant. Viète havia de defensar a Jean de Parthenay de les acusacions en contra d'aquest. Degut a diversos conflictes causats pel casament de la filla d'Antoinette i Jean de Parthenay, aquests es van traslladar a La Rochelle juntament amb Viète. Al 1570 deixà de treballar per la família Soubise i va establir relacions amb la família reial a París, així com amb grans matemàtics de l'entorn. Un any més tard començà a editar dos llibres titulats *Canon Mathematicus* i *Universalium Inspectionum Liber Singularis*, que es van publicar el 1579. Acusat per simpatia envers la reforma protestant, Viète es retirà entre el 1583 i 1585 a la seva ciutat natal de Fontenay-le-Comte on va treballar quasi exclusivament en l'escriptura de la seva gran obra matemàtica, l'*Isagoge in Artem Analyticem* (*Introducció a l'Art Analítica*), que es publicà a Tours l'any 1591. En aquesta ciutat, on el rei Enric III hi havia traslladat la cort reial, Viète donà classes de matemàtiques i també treballà pel rei en tasques de criptoanàlisi. Viète va ser l'encarregat de desxifrar els missatges interceptats de la Lliga Catòlica, gran enemiga del rei. La Lliga Catòlica comptava amb el recolzament de Felip II d'Espanya, el Papa Sixte V i la reina consort de França Catalina de Mèdici, entre d'altres. Després de la mort d'Enric III, ocorreguda el 31 de juliol de 1589, Enric IV de Navarra el va succeir. El nou monarca nombrà a Viète un dels seus consellers privats. Durant aquesta època, Viète va aconseguir desxifrar els missatges enviats per Felip II d'Espanya, qui, cegat per la seva confiança en la dubtosa fortalesa dels seus xifrats, va arribar a acusar Viète de confabular-se amb el diable. Aquest fet presenta clarament la ineficàcia de les xifres monoalfabètiques enfront de la tècnica del criptoanàlisi, que s'havia anat estenent pels països del continent europeu. Després d'anar a París, on es va dedicar a complir tasques diplomàtiques i polítiques, Viète tornà a Fontenay-le-Comte on hi morí l'any 1603. A l'*Isagoge in Artem Analyticem* Viète va introduir l'àlgebra simbòlica usant vocals en majúscula per a les incògnites i consonants, també en majúscula, pels coeficients. Cal destacar que es coneix un mètode usat per Enric IV de Navarra, i que consisteix en assignar a cada lletra una combinació de números per tal d'evitar repeticions, i així tenir una major fortalesa a l'atac per anàlisi de freqüències. Aquest xifrat es complementava

amb tècniques esteganogràfiques i utilitzant codis.

6 Influències de Vigenère

Fins ara hem vist ràpidament l'evolució de la criptografia des dels seus suposats inicis, fins a veure com es va sistematitzar el seu aprenentatge, tot establint oficis pels anomenats *secretaris de xifres*, dels que tot sistema de poder mínimament competent disposava. Totes les obres i personatges que fins ara hem anomenat van tenir lloc en un determinat context històric, i en bona part ha estat aquest context el que ha permès fer un avanç en els sistemes de xifrat i desxifrat. Seria erroni intentar analitzar una obra sense tenir-ne en compte els seus precedents, tant els més immediats com els més llunyans. Si fins ara hem seguit aquest esquema per tal d'explicar l'evolució que ha sofert la criptografia, és necessari estudiar de quines fonts va treure el seu coneixement Vigenère i quines obres, i autors, van influir més directament en la composició del *Traicté des Chiffres*.

Als següents apartats s'estudiaran bàsicament cinc grans figures que fins ara no hem esmentat. S'intenta citar-los per ordre cronològic, tot i que molts d'ells visqueren durant pràcticament el mateix període de temps. Potser aquests no van influir directament en qüestions polítiques i militars, però sí van aportar coneixement al camp de la criptografia. Especialment són rellevants les seves aportacions pel que fa al desenvolupament dels primers xifrats polialfabètics. Fins al moment s'utilitzaven xifrats rudimentaris que sovint es tractaven de variacions de xifrats de Cèsar afegint paraules homòfones i codis per tal d'evitar repeticions de paraules, i així dificultar al desxifrador la seva tasca mitjançant l'anàlisi de freqüències. No obstant això, per context, l'interceptor podia arribar a deduir els codis i, tenint una idea del tema del que parlava el missatge, arribava a desxifrar-lo totalment. Durant aquest temps els criptoanalistes "guanyaven¨ la batalla als xifradors, encara que aquests afegissin variacions als seus mètodes de xifrat, que acabaven essent semblants els uns amb els altres.

6.1 Leon Battista Alberti (1404-1472)

Leon Battista Alberti va ser un exemple de l'ideal d'home renaixentista. Encara que és més conegut sobretot pels seus treballs de pintura i arquitectura, presents en esglésies i edificis florentins tals com l'església de Santa Maria Novella o el Palau de la família Rucellai, Alberti es destacà com a gran criptògraf. Fins fa relativament poc, aproximadament a finals dels anys 80, se'l considerava pioner en la descripció de l'anàlisi de freqüències. Alberti neix a Gènova fill d'un mercader benestant que fou desterrat de la Toscana. Alberti es va educar a Pàdua i més tard va anar a Bolonya a estudiar lleis a la universitat. Paral·lament també estudià pintura, escultura, matemàtiques i filosofia, i no abandonà tampoc l'escriptura, passió que mantingué des de la joventut. A la seva autobiografia es fa palès el seu interès per les matemàtiques i la filosofia quan digué:

> Jo, no podent estar lluny dels estudis, a l'edat de vint-i-quatre anys em vaig encarar a la filosofia i a la disciplina de les matemàtiques: de fet confiava poder-les cultivar en calma, veient que exercitava la inteligència i la memòria. (Cardini, Regoliosi:15)

Després de la mort del seu pare l'any 1421, Alberti va tenir problemes econòmics que, entre d'altres, el dugueren a ordenar-se sacerdot, i es traslladà a Roma per exercir la seva professió. El 1433 va començar a escriure els quatre volums del *Libri della famiglia*, obra escrita en la llengua vulgar italiana que plasma la societat de l'època, i que va acabar l'any 1441. Durant aquest període de religiositat, s'interessà per l'arquitectura del passat, i això el va dur a començar a exercir com a arquitecte pel Papa Nicolau V. La seva primera gran obra va ser la construcció de la façana del Palau dels Rucellai. L'any 1452 acabà d'escriure el que va ser el seu principal text sobre arquitectura: el *De Re aedificatoria*, publicat al 1485. Resulta ser un tractat sobre arquitectura basat en les obres de l'arquitecte i enginyer romà Vitruvi (S.I aC). També per ordre de la família Rucellai, l'any 1456 va dissenyar la façana de l'església de Santa Maria Novella. Alberti estudià profundament *Els Elements* d'Euclides. A la biblioteca de Sant Marc de Venècia es conserva un manuscrit de l'edició de Campanus de Novara (c.1220-1296) de *Els Elements*, amb anotacions del propi Alberti. De manera que no és d'estranyar el seu profund coneixement de la perspectiva i de la geometria en general. Es creu que els seus treballs sobre criptografia foren escrits degut a un encontre amb un tal Leonardo Dato, que treballava com a secretari papal. Dato preguntà a Alberti sobre el desxiframent d'uns missatges, i l'arquitecte va prometre ajudar-lo. Degut a aquest fet, el 1467 Alberti escrigué el *De componendis cifris*, un tractat de 25 pàgines sobre criptografia. Hi exposà un nou mètode per a xifrar, tot usant discs, i per primera vegada explicà l'anàlisi de freqüències a l'Oest.

Com que ja s'ha comentat amb detall en què consistia l'anàlisi de freqüències a través de l'obra d'Al-Kindi i al *De componendis cifris* no s'aporta cap idea nova, passarem directament a comentar en què consistia el xifrat que l'italià va anomenar "digne de reis¨ i el qual va qualificar "d' indesxifrable". Aquest xifrat per substitució es considera el precedent dels xifrats polialfabètics. Al *De componendis cifris* s'explica de la manera següent:

> Faig dos cercles concèntrics de coure. El primer, el més gran, s'anomena estacionari, el més petit s'anomena mòbil. El diàmetre de l'estacionari és, un novè més gran que el disc mòbil. Divideixo la circumferència de cada cercle entre 24 parts iguals. Aquestes parts s'anomenen caselles. A les diverses caselles del cercle més gran escric les lletres en majúscula, en vermell, ometent la H i la K [i la Y] perquè no són necessàries. (Kahn, 1996:127)

Alberti construeix dos cercles concèntrics de diferent diàmetre; el major és fix, i el menor és mòbil. A l'hora d'escriure les lletres dins de cada casella, al disc estacionari se segueix l'ordre alfabètic; s'hi inclouen també alguns nombres (1,2,3,4). En canvi, al disc mòbil l'alfabet apareix desordenat a l'atzar. Acordada una posició concreta dels dos discs, anomenada *clau* es xifra el missatge desitjat. Fins aquí es tracta d'un simple mètode per substitució, però Alberti va anar més enllà:

> Després d'escriure tres o quatre paraules, hauria de canviar la posició de l'índex a la nostra fórmula girant el cercle pertal de que l'índex k sigui, per exemple, sota la D [fa referència a un exemple previ on la clau era E-Z]. Així al meu missatge hauria d'escriure la lletra D, i en aquest punt, al text xifrat, k no significarà més B, sinó D, i totes les altres lletres al cim rebran nous significats. (KAHN, 1996:129)

Amb aquest paràgraf Alberti donà l'inici dels xifrats polialfabètics. Tot i que a priori els discs en si mateixos no formen un xifrat polialfabètic, l'ús que Alberti en va fer sí que consistia en usar diferents alfabets en un mateix xifrat. Canviant la posició dels discs cada certa mesura acordada, Alberti va aconseguir un xifrat polialfabètic. Al xifrat de Vigenère ja estarà implícit l'ús de varis alfabets. Alberti també descrigué com xifrar codis, sistema que fins ara no es tenia constància de que s'utilitzés. Malgrat els notables avenços que Alberti va descriure, el *De componendis cifris* no va tenir un impacte gaire extens dins l'àmbit criptogràfic del moment, i passà bastant desapercebut. Tanmateix, altres criptògrafs posteriors, com Vigenère, esvan influenciar de l'obra d'Alberti.

6.2 Johannes Trithemius (1462-1516)

Johannes Trithemius va néixer el 2 de febrer de 1462 a Trittenheim, Alemanya. En un primer moment es deia com el seu pare, Johannes von Heidenberg el qual morí un any després de que ell nasqués. Va passar a cuidar-lo la seva mare i un pare adoptiu que ridiculitzava les seves ganes d'aprendre. No obstant això, Trithemius aprengué d'amagat grec, llatí, i hebreu, i als 17 anys s'escapà de casa i va entrar a la Universitat de Heidelberg on, degut a la seva intel·ligència, li van pagar els estudis. En un dels seus viatges des de casa seva a la universitat, les dures condicions climàtiques de neu i fred l'obligaren a refugiar-se en una abadia benedictina de Spanheim. Arran d'aquest fet, al 1482 Trithemius hi entrà com a novici i un any i mig més tard fou escollit abat amb tan sols 21 anys. Trithemius va convertir l'abadia en un centre d'estudi. Durant aquest període escrigué vàries obres, la més important de les quals va ser el *Liber de scriptoribus ecclesiasticis*, on hi cita 963 autors diferents en referència a la teologia. El *Liber de scriptoribus ecclesiasticis* ésconsiderada la primera obra que incorpora una bibliografia detallada.

Trithemius professava una afició menys ortodoxa: l'ocultisme. Relacionat amb aquest fet, Trithemius escrigué una obra que generà polèmica; es tracta de *Steganographia. Hoc est: Ars per ocultam scripturamanimi sui voluntatem absentibus aperiendi certa* (*Esteganografia o l'art precís de descobrir la voluntat de l'ànima als que no hi són per mitjà de l'escriptura oculta*). L'obra ens arriba incompleta, ja que sols es conserven tres dels vuit volums que la formaven. Va ser inclosa a l'*Index librorum prohibitorum*, i per tant prohibida per l'Església Catòlica. L'obra està parcialment xifrada i no se sap amb certesa si el que pretenia Trithemius era escriure sobre criptografia o si era un tractat de màgia ocultisita. A aquella època, la criptografia estava fortament lligada a l'ocultisme i podria haver suposat un perill per la seva vida si l'Església ho hagués jutjat com a tal. Al segle XX, dos investigadors van desxifrar de forma independent els passatges de l'*Steganographia*. Primerament,

Thomas Ernst, estudiant de la Universitat de Pittsburgh, va publicar un extens escrit sobre el contingut de l'obra que, malauradament, va passar desapercebut. Al 1998 Jim Reeds, matemàtic dels laboratoris AT&T va publicar la seva troballa a la revista *Cryptologia* i es va emportar gran part del mèrit. Reeds descriu el contingut de l'*Steganographia* dient que "Aparentment el llibre explica com usar esperits per enviar missatges secrets a distància.[...] Gran part del llibre és dedicat a textos d'invocacions, mitjançant les quals s'obté la voluntat dels esperits."(Reeds, 1998:2). Explicà detalladament el procediment que va seguir per a desxifrar el text. A través d'altres obres de Trithemius se sap que professava un cert interès per l'estudi de la criptografia, i per tant és probable que es tractés d'un manual poc ortodox sobre el tema. L'acollida que va generar l'*Steganographia* no va ser bona, especialment per part de l'Església, ja que hi va veure allò que volia prohibir. Així, Trithemius va passar a ser molt popular a causa de l'atribució que se li va fer de poders "sobrenaturals¨ i guanyarà la mala fama d'ocultista. Per tal de dissimular el seu interès per l'ocultisme, escrigué, ara sí, una obra totalment dedicada a la criptografia, el nom complet de la qual és *Polygraphiae libri sex, Ioannis Trithemii abbatis Peapolitani, quondam Spanheimensis, ad Maximilianum Caesarem*, o *Sis llibres sobre Poligrafia, de Johannes Trithemius, Abat a Wurzburg, anteriorment a Spanheim, per l'emperador Maximilià*, més conegut simplement com *Polygraphia*. És la primera obra impresa dedicada totalment a l'estudi de la criptografia. Es publicà al juliol del 1518, es va reeditar en vàries ocasions i es va traduir fins i tot al francès. Tot i la seva tardana publicació, Trithemius la començà a escriure al voltant dels 46 anys d'edat. En destaca la rapidesa en què va escriure els 6 volums, ja que es calcula que va tardar una mitjana de només deu dies per esciure cada volum. La *Polygraphia*, tal com el seu nom complet indica, consta de 6 llibres (un total de 540 pàgines) escrits en llatí. Dels primers quatre es destaca l'*Ave Maria*. En aquest xifrat es posen per columnes les lletres de l'alfabet, 24 lletres en aquest cas, i al seu costat una columna de paraules que substituïen cada lletra. Trithemius va escollir les paraules de tal manera que, a l'escriure una paraula xifrada (cada lletra per una paraula), el significat fos coherent, i per tant es dissimulés el xifrat real. La gran aportació que va fer Trithemius és descrita al llibre cinquè: l'anomenada *tabula recta*, que va ser un precedent directe del xifrat de Vigenère. La tabula recta es construeix de la següent manera:

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

Es tracta, doncs, de a cada fila desplaçar l'alfabet una posició respecte de la fila anterior. Més formalment, a la fila i s'aplica un xifrat de Cèsar $f(x) = x + i \pmod{24}$ on $i = 0, 1, 2, ..., 23$. Trithemius utilitzà aquesta taula per xifrar cada lletra amb un alfabet diferent seguint l'ordre de la taula i començant de dalt cap a baix. Per exemple, per xifrar la paraula MARIA es considera l'ordre en què apareixen les lletres de la paraula i es xifra en concordança amb la fila que té el mateix ordre; per tant, si substituïm lletres per nombres tal com s'indica a l'inici de la memòria en l'apartat de *Conceptes bàsics i nomenclatura*, MARIA es xifraria com *mburf*, ja que la "M"és a la posició 0 i se li aplica $f(11) = 11+0 = 11 \pmod{24}$, que és la mateixa m; per la "A", que ocupa el lloc 1, s'usa $f(0) = 0+1 = 1 \pmod{24}$, que és la b, etc. Aquest mètode, a diferència del que proposava Alberti al *De componendis cifris*, utilitzava implícitament varis alfabets per un mateix xifrat, és a dir, és un xifrat polialfabètic. Com a avantatge respecte del mètode d'Alberti, destaca que s'usa un xifrat diferent per a cada lletra, mentre que l'italià proposava canviar d'alfabet a cada certa mesura estipulada prèviament. Notem també que Trithemius no usava cap clau, a diferència de tots els altres mètodes previs, sinó que la clau és inherent al propi sistema. Aquests xifrats, en general, s'anomenen de *clau progressiva*. Com a contrapartida destaca la rigidesa en què s'usà la tabula recta, ja que Trithemius només va proposar de xifrar les lletres fila per fila, i no aleatòriament seguint una clau com va fer posteriorment Vigènere. L'obra de Trithemius va influir enormement a molts criptògrafs posteriors. L'ús de la *tabula recta* va esdevenir comú, i va servir de base d'altres mètodes de xifrat.

A causa de la mala reputació que va adquirir degut a l'*Steganographia*, Trithemius va haver de marxar de l'abadia de Spanheim i va refugiar-se a la de Wurzburg, des

d'on escrigué la *Polygraphia*. Des d'allà escrigué altres obres i, fent una vida d'estudi humil, morí el 15 de desembre de l'any 1516.

6.3 Girolamo Cardano (1501-1576)

Girolamo Cardano ha passat a la història degut a la publicació de l'*Artis Magnae sive de regulis algebraicis* (*Gran Art de les regles de l'àlgebra*), al 1545. A aquesta obra hi apareix, per primera vegada la resolució de l'equació de tercer grau i de quart grau per radicals. La resolució de la çúbical·li va ser confiada per Niccolò Fontana (o Tartaglia), la qual cosa va generar una llarga disputa entre aquests i Ludovico Ferrari, brillant ajudant de Cardano. També destacà per haver realitzat els primers estudis al camp de les probabilitats al *Liber de ludo aleae*, publicat pòstumament el 1663. Va voler ésser recordat pels seus nombrosos escrits (131 llibres publicats en vida i 111 manuscrits) sobre una multitud de temes diversos.

Girolamo Cardano va néixer a Pavia, fill d'un advocat milanès. La seva vida ens arriba en bona part gràcies a la seva pròpia autobiografia, anomenada *De propia vita*. En aquesta obra Cardano relatà com la seva mare -de la qual no en parlà massa bé- volia avortar. També es descrigué de manera peculiar com una persona amb complicacions físiques que s'auto-lesionava pel "plaer que ve després d'un gran dolor"(Dorce, 2015:289). Els seus primers estudis foren a càrrec del seu pare com a ajudant seu. El 1520 començà a estudiar medicina a la Universitat de Pavia, i acabà els seus estudis com a doctor a la Universitat de Pàdua, ja que la primera va haver de tancar a causa de la guerra italiana coneguda com La Guerra dels Quatre Anys (1521-1526). El seu caràcter difícil el va fer enfrontar amb el Col·legi de Metges de Milà, els quals van rebutjar la seva sol·licitud d'admissió. Es va traslladar a la vila de Saccolongo, on exercí de metge, i al 1531 va casar-se amb Lucia Bandarini, amb la qual tingué tres fills. Va ser arran d'aquest període a Saccolongo que Cardano escrigué sobre probabilitats, ja que va tenir problemes amb el joc. Gràcies a l'ajuda d'amistats del seu pare, li va ser oferta una plaça per ensenyar matemàtiques a Milà. Allà també va exercir com a metge -il·legalment- i la seva fama com a tal cresqué. Gràcies a les pressions dels seus clients, Cardano va poder entrar al col·legi de Metges de Milà l'any 1539, i així abandonà la seva tasca com a professor de matemàtiques. No obstant això, no va deixar l'estudi d'aquestes, tal com demostren els seus nombrosos llibres.

Cardano no escrigué cap obra dedicada explícitament a la criptografia, sinó que els seus coneixements ens arriben a través de dues de les seves obres més populars: *De Subtilitate Rerum* i *De Rerum Varietate*. El primer va ser publicat al 1550 i el segon al 1559. Aquest últim sembla ser una continuació de l'anterior, que tractava sobre experiments de física i especulacions, intercalant anècdotes pel mig. Citant a l'historiador David Kahn (1996:144): "[En aquestes obres] Cardano va descriure els mètodes clàssics de l'antiguitat, va intentar donar una classificació que resultà en una auto-contradicció, va donar idees sobre com obrir secretament cartes, sobre com desxifrar-les, i desenvolupar tinta secreta i també va oferir alguns mètodes propis..."

Cardano va intentar idear un sistema en què el propi text en clar fos la clau de

la següent manera:

clau	S	I	C	S	I	C	E	S	I	C	E	R	G	O	E	L
text	s	i	c	e	r	g	o	e	l	e	m	e	n	t	i	s
xifrat	N	T	F	Z	C	L	T	Z	V	H	R	Y	V	I	P	E

Segurament Cardano va pensar poc aquest sistema que, encara que la idea fos bona, presentava vàries errades. La primera d'elles és que aquest mètode admetia vàries opcions de desxifrat, i la segona és que el receptor del missatge es trobava a la mateixa situació que un atacant a l'hora d'aconseguir la clau.

Aquest sistema de Cardano tenia greus deficiències, i per tant no va ser utilitzat posteriorment. En canvi, un mètode esteganogràfic que es descriu als seus dos llibres sí que va ésser popularment usat. Aquest mètode es coneix com la "reixa de Cardano". Consisteix en foradar, per exemple, una cartolina i escriure el missatge en aquests forats, que seran de diferent mida. D'aquesta manera un missatge aparentment innocent podia contenir un text ocult. El receptor havia de disposar d'una còpia de la cartolina per a poder desxifrar el missatge.

S'ha inclòs una petita descripció dels treballs de Cardano ja que, encara que no va fer grans progressos en l'àmbit de la criptografia, Vigenère el cita al *Traicté des Chiffres*, dient que ha llegit les seves obres, i per tant va estar influenciat, en poca o gran mesura, per aquestes.

6.4 *La cifra del Sig. Giovan Battista Belaso*

Si fins ara hem vist Alberti i Trithemius, que eren personatges molt coneguts en molts àmbits, i dels quals ens arriben nombroses cròniques i històries sobre les seves vides, no passa el mateix amb Giovan Battista Belaso[1]. Nascut al si d'una família noble de Brescia, Itàlia, Belaso es graduà en lleis a la Universitat de Pàdua al 1538. Se sap que va treballar pel cardenal Rodolfo Pio di Carpi. No es coneix l'any de la seva mort ni més detalls de la seva vida, tret que escrigué tres breus llibres sobre criptografia. El primer d'ells data de l'any 1553 i s'anomenava *La cifra del Sig. Giovan Battista Belaso.*. Al 1555 escrigué *Novi et singolari modi di cifrare*, una continuació del primer llibre. Al 1564 presentà el seu tercer llibre, titulat*Il vero modo di scrivere in cifra*, al qual es descriuen variacions dels mètodes explicats als dos primers llibres.

Segurament el més rellevant dels tres llibres escrits per Belaso és el primer. A *La cifra del Sig. Giovan Battista Belaso* hi descrigué un xifrat polialfabètic tot usant claus, dos elements que fins al moment no s'havien aplicat junts. Al títol, es fa palès l'orgull del seu autor per haver-la desenvolupat, dient que ningú no la podrà desxifrar sense tenir-ne la clau, i que és d'un ús molt senzill. Tal com està escrit:

> Laqual cifra, benche sia stampata, contiene in se questa maravigliosa bellezza, che tutto il mõdo potrà usarla,& nientedimeno, l'uno non potrà leggere quello

[1]Es troba escrit com Belaso o Bellaso

> che scriue l'altro; se non solamente quei che haueranno tra loro, un breuissimo contrasegno; come in questo medesimo foglio s'insegna, insieme cõ la sua dichiaratione, & col modo d'adoperarla.(Belaso, 1553:7)[2]

A les dues primeres pàgines del tractat Belaso remarcà la importància que té l'estudi de la criptografia. També descrigué els motius pels quals ha escrit aquest tractat. Seguidament continuà la descripció del seu mètode, començant per explicar com es pot escollir la clau del criptosistema:

> Bisogna hauere un contrasegno tra coloro che si scriuono. Il qual contrasegno hanno da essere alcune parole uolgari, ò latine, ò di qual si uoglia altra lingua, & possone essere poche parole ò molte, secondo che noi uogliamo.(Belaso:11)

Aquesta clau pot ser en l'idioma que es vulgui i de la llargada que es desitgi. Continuà dient:

> Pigliansi dipoi le parole che noi uogliamo scriuere, & si stendono sopra un foglio scriuendo un poco larghetto. Dipoi sopra ciascuna di quelle lettere, si mette una lettera del nostro contrasegno in questa forma. Sia per essempio il contrasegno questo uersetto. *Virtuti omnia parent.* Et sia quello che uogliamo scriuere, queste parole. *Larmata Turchesca partira a cinque di Luglio.* (Belaso:11)

Belaso explicà que s'ha d'escriure el text en clar, per a sobre col·locar-hi la clau escollida tantes vegades com faci falta, lletra sobre lletra. A l'exemple que posà la clau és *Virtuti omnia parent* i el text a xifrar *Larmata Turchesca partira a cinque di Luglio.* Seguidament mostrà com ho va fer:

> Metteranosi adunque sopra d'un folgio cosi disposti
>
> u i r t u t i o m n i a p a r e n t u i r t
> l a r m a t a t u r c h e s c a p a r t i r
>
> u t i o m n i a p a r e n t u i
> a a c i n q u e d i l u g l i o

> Que, come uedete, il modo e, che le parole del contrasegno si scriuono fun che durano. Et come ??? da capo,& cosi si farà di continuo, se ben uelisimo scriuere cento & mille fogli di carta, tenendo sempre un medesimo modo di metter di sopra lettera per lettera il contrasegno fin che dura. Et sia il contrasegno di poche ò di molte parole che non importa. Et sopra tutto auuertiscasi di disporle giustamente una per una & non prendere errore, che in questa ordinatione solamente, consiste tutta l'importanza.& sempre che si scriueranno le lettere larghe l'una dall'altra non si farà mai errore. (Belaso:11)

És a dir, explicà que no importa quantes paraules es vulguin xifrar que, si es fa de la manera que ell presentà, mai no hi haurà cap error. Remarcà la importància

[2]S'enumera la pàgina que consta a la versió digital, ja que el text original no està enumerat.

de no equivocar-se posant una lletra sobre l'altra, ja que en l'ordre recau tot el procediment. Al paràgraf següent, Belaso presentà la manera sobre com xifrar els missatges:

> [...]Dipoi per uoler cifrare si prende il foglio bianco doue uogliamo mettere la cifra damandare a chi scriuiamo, & si tiene la contracifra dauanti, cioè queste nostre undici coppie d'alfabeti cosi ordinati, con due lettere grosse dauanti à ciascuna coppia, & uasi al contrasegno & à quello che uogliamo scriuere, & cominciando dalla prima lettera del contrasegno si dice cosi u.l. & mirasi nella cifra, &primieramente si cerca tra le lettere grosse per trouare la lettera del contrasegno, cioe la V. che farà alla decima coppia, dipoi si camina dritto per largo à quella lettera, nell'Alfabeto doppio in lettere piccole, & trouasi la lettera che sta di sotto à quella del contrasegno, cioe la lettera di quello che noi uogliamo scriuere secreto, che farà la .l. & trouata, se sta disopra, si piglia in suo luogo quella che le sta di sotto. Et se sta di sotto si piglia quella che le sta disopra; mettédo sempre una per l'altra. Et cosi sopra il nostro folgio bianco metteremo detta lettera compagna di quella che noi in quello Alfabetominuto habbiamo trouata. (Belaso:11)

A aquestes línies, Belaso donà les pautes per a utilitzar el seu xifrat. No usava una tabula recta tal com feia Trithemius. Fa servir un alfabet de 22 lletres "ABCDEFGHILMNOPQRSTUXYZ"(l'italià del moment), i el divideix en grups de dues lletres que es posaven a l'esquerra en majúscules. Al costat dret s'hi posava, en dues files, l'alfabet dividit en dues parts, ABCDEFGHILM/NOPQRSTUXYZ, on, a la fila de dalt les lletres estaven ordenades alfabèticament, i a la de baix les lletres estan desordenades. Aquest desordre corresponia a desplaçar, mòdul 11, d_i posicions en la fila i, on $i = 1, ..., 11$. A aquest xifrat concret que descrigué Belaso $d_1 = 0$, $d_2 = 5$, $d_3 = 1$, $d_4 = 6$, $d_5 = 2$, $d_6 = 7$, $d_7 = 3$, $d_8 = 8$, $d_9 = 9$, $d_{10} = 4$ i $d_{11} = 10$. Notem que no aplicà el que semblava un xifrat de Cèsar d'una manera ordenada tal com feia Trithemius, sinó que a la primera fila no va desplaçar l'alfabet partit en dos, a la segona el desplaçà 5 posicions, a la tercera una, etc. Aparentment sembla que la disposició dels desplaçaments sigui aleatòria. D'aquesta disposició, que va servir per a xifrar el missatge, Belaso l'anomenà *contraxifra*. La manera per a fer correspondre la clau amb les lletres del text en clar és la següent: sigui s la llargada de la clau, aleshores la n-èssima lletra de la clau es correspondrà a la n-èssima lletra del text en clar mòdul s. Notem que el nombre sencer de cops que es repetirà la clau és $[N/s]$, on N és la llargada del text en clar. Així doncs, amb aquesta disposició, Belaso explicà, al paràgraf esmentat, com es substitueixen les lletres del text en clar per xifrar-les. Primerament es busca a la part esquerra de la contraxifra, on hi ha les lletres en majúscula, la lletra de la clau del criptosistema que està a sobre de la lletra en clar que volem xifrar. Un cop trobada, buscarem la lletra en clar en les dues files de la dreta. Si trobem que està a la fila de sota, al text xifrat la substituirem per la que té a dalt; i viceversa, si la lletra està a la fila de sobre, la xifrarem per la que té just a sota. Observem que clarament es tracta d'un mètode de substitució polialfabètic, ja que usà diversos alfabets segons la lletra de la clau que estava a sobre de la lletra a xifrar. A continuació explicà com xifrar la frase que havia posat com a exemple amb la clau VIRTUTI OMNIA

PARENT. Simultàniament explicà com el receptor desxifraria el missatge usant la mateixa contraxifra.

> Che nell'essempio che habbiamo posto, la lettera cercata è l. & sotto di lei sta la lettera .s. & cosi metteremo .s. nel foglio bianco, la quale .s. quando col medesimo contrasegno il nostro amico col medesimo ordine & con questa medesima cifra, decifrerà, la ritrouerà pure per .l. Dipoi si ritorna al contrasegno & alle lettere di quello che uogliamo scriuere, & pigliasi la seconda lettera dell'uno & dell'altro come facemmo della prima, & dicesi .i. .a. & fassi come della prima s'è fatto & cosi mettera detta lettera nel foglio bianco appresso all'altra che vi mettemmo, & haueremoui .sy. & cosi si torna poi allaterzadel contrasegno, & combinasi con quella di sotto, come si fece dell'altre, & diremo r r. & nella cifra troueremo la prima r. tra le lettere grosse, che farà alla ottaua coppia, & caminandosi all'incontro tra le minute à trouar l'altra r. si trouerà per sua compagna la lettera b. la qual metteremo nel foglio bianco appresso all'altre due & haueremo syb. Et cosi finalmente si uerrà facendo di tutte infino che uene sono. & haueremo per il sopradetto essempio queste lettere.
>
> *Sybouey ldanuofsz lpiincu pnshmlr nxoiznrd.* (Belaso:12)

La primera paraula a xifrar és ¨ Larmata", per tant buscarem primer la lletra ¨ l"a la contraxifra en les dues files corresponents a la lletra "V"de VIRTUTI. Com que la ¨ l"es troba a la fila de dalt la xifrarem per la lletra de sota que correspon a una "s". De la mateixa manera, quan el receptor vulgui desxifrar el missatge aquest buscarà la lletra "s"a la contraxifra i a sobre hi trobarà la lletra l·l", amb la qual cosa podrà recuperar el missatge xifrat. Per xifrar la següent lletra, la "a", haurem de mirar a les dues files de la lletra ¨ I". Seguint el mateix procediment substituirem la lletra "a"per la "y", que es troba just a sota. El mateix passarà per la "r"que es xifrarà com "b". Així seguirem fins a xifrar tot el text complet que quedarà com "Sybouey ldanuofsz lpiincu pnshmlr nxoiznrd". A continuació, Belaso explicà com el receptor pot desxifrar el missatge coneixent-ne la clau i la contraxifra. Assegurà que ningú que no conegui la clau no serà capaç de desxifrar el missatge, ja que una lletra del text xifrat representava múltiples lletres del text en clar.

> " Le qual lettere ò parole cosi cifrate, leggendosi dall'amico nostro col medesimo contrasegno, diranno. *Larmata Turchesca partira a cinque di Luglio.* Et senza il detto contrasegno non basterà tutto il mondo per uia naturale à leggerla mai. Perche come ben conoscono quei che piu ne fanno, in questa non si puo usare alcun'arte per ritrouarla, essendo che unamedesima lettera, hora significherà una lettera & hora un'altra, & ogni lettera puo significare .xi. lettere diuersamente. Come si uede nelle ultime lettere delle ultime lettere delle sopra dette parole, che **y z p u**, tutte significano .a. & si uede che tutte l'altre lettere uocali ò consonanti uengono sempre uariate, & se pure alcuna uolta uengono replicate è maggior cofusione di chi ¿uolesse? leggerla senza contracifra. (Belaso:12)

Belaso coneixia els mètodes de xifrat que s'usaven a la cúria romana, i per tant era conscient dels beneficis que implicava usar un xifrat polialfabètic. Explicà que

en aquest xifrat les lletres "y, z, p, u"totes representaven la lletra "a", fent inútil l'anàlisi de freqüències que s'usava per a desxifrar els missatges. Seguidament posà l'exemple de com s'havia de fer per a desxifrar el missatge que prèviament havia xifrat. El procediment era el mateix però a la inversa:

> [...]Il modo di leggerla è il medesimo che quello di scriuerla, che soprà le lettere cifrate si uien mettendo il contrasegno, & poi si cobina quella di sopra con quella disotto, & nella contra cifra si troua quella di sopra tra le lettere grosse, & quella di sotto tra le minute che le stano affronte, à puto come si fece nello scriuerla. L'essempio del leggerla è questo.
>
> u i r t u t i o m n i a p a r e n t u
> s y b o u e y l d a n u o f s z l p i
>
> i r t u t i o m n i a p a r e n t u i
> i n c u p n s h m l r n x o i z n r d
>
> Che leggendosi nel medesimo modo col quale fu scritta, dirà. L'armata Turchesca partirà à cinque di Luglio. (Belaso:12)

Veiem que la disposició de les paraules és la mateixa que al procés de xifrat. A la pàgina següent de *La cifra* de Belaso, hi apareix l'anomenada contraxifra, que va usar per a xifrar i desxifrar el text que es mostra a l'exemple. Es reprodueix a continuació:

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

Tal com s'ha descrit anteriorment, s'ha dividit l'alfabet en dues parts i al de sota s'ha aplicat un desplaçament de d_i posicions depenent de la fila. Finalment Belaso explicà que al text xifrat s'hi poden escriure les paraules conservant la seva separació (la qual cosa donaria cert avantatge a l'atacant), o bé es poden ometre les separacions.

> Questa cifra si puo scriuere con le parole spartite giustamente come quando scriuiamo in queste nostre lettere communi, si come habbiamo fatto nel sopra detto essempio. perche uenendo le ultime lettere tanto uariate, danno maggiore confusione à chi uolesse leggerla senza il contrasegno.Ma se pure alcuno uolesse scriuere continoato, puo farlo, come si fa in tutte l'altre cifre che hoggi usano i Principi. & ancora per piu comodità di chi ha da leggerla col contrasegno si puo scriuere una y, tra ogni parola, la quale y, nel decifrarla farà conoscere la diuisione delle parole. In questo modo.

u	i	r	t	u	t	i	o	m	n	i	a	p	a	r	e	n	t	u	i	r	t	u
l	a	r	m	a	t	a	y	t	u	r	c	h	e	s	c	a	y	p	a	r	t	i
t	i	o	m	n	i	a	p	a	r	e	n	t	u	i	r	t	u	t	i	o		
r	a	y	a	y	c	i	n	q	u	e	y	d	i	y	l	u	g	l	i	o		

& cosi verra cifrandosi tutta nel medesimo modo de la prima. (Belaso:12)

Al cas en què s'ometien els espais, Belaso proposà intercalar una *y* entre cada paraula per tal de facilitar la lectura al receptor del missatge xifrat. Belaso acabà l'explicació del seu mètode descrivint una manera de dividir en versos el text en clar per tal de que el criptògraf no s'equivoqui a l'hora de posar les lletres en correspondència amb la clau.

La xifra descrita per Giovan Battista Belaso suposà un salt qualitatiu respecte els mètodes de xifrat usats anteriorment. Aquest criptosistema polialfabètic es diferenciava del que proposava Trithemius, al qual no es construïa una tabula recta, sinó que el xifrat s'implementava de forma lleugerament diferent, tal com hem vist.

6.5 Giambattista della Porta (1535-1615)

Giambattista della Porta va combinar el que Belaso, Trithemius i Alberti ja havien fet separadament: l'ús de claus fàcilment canviables, el xifrat polialfabètic lletra per lletra, i l'ús d'alfabets mixtos (combinar codis dins d'una xifra) respectivament. Giambattista della Porta, també conegut per Giovanni della Porta, va néixer l'any 1535 a la ciutat de Vico Equensa, prop de Nàpols, fill de Nardo Antonio della Porta, qui valorava l'aprenentatge i li donà una bona educació. Des de ben petit, Porta i els seus germans van créixer envoltats d'amics del seu pare, els quals els van tutoritzar en diversos àmbits del coneixement. Aquest ambient influirà el recorregut del jove Porta, que personificà, talment com Alberti, l'ideal d'home renaixentista. Als 10 anys, Porta ja componia assajos en llatí i italià. Al 1558, amb tan sols 22 anys, va publicar la seva primera obra, *Magia naturalis*, una obra dedicada a curiositats científiques. Degut al seu interès per la "màgia de la naturalesa¨ crearà l'Accademia Secretorum Naturae, els membres de la qual es faran dir *otiosi* o *homes d'oci*. En aquest grup de persones aficionades als misteris de la ciència, es duien a terme experiments mesurables i, encara que poguessin a arribar ésser sorprenents, fàcilment reproduïbles. No obstant això, Porta va haver de declarar davant del Papa Pau V per defensar-se contra acusacions d'estar practicant ¨ ciències ocultes". També va exercir de vicepresident a l'Accademia dei Lincei o Acadèmia dels Linxs, a la que també hi pertanyia Galileo Galilei. Al 1563 publicà l'obra sobre criptografia anomenada *De Furtivis Literarum Notis*, i al 1586 el *De humana physiognomonia libri III*, un llibre que tractava de la relació de les característiques físiques entre humans i animals. Entre el 1586 i el 1609, escrigué vàries obres d'òptica, meteorologia, agricultura, mecànica, pneumàtica, astrologia i astronomia, i també comèdies teatrals. El *Magia naturalis* es va ampliar fins arribar als 20 volums, on es descrivien els experiments que duien a terme els *otiosi*. Entre aquests experiments hi compta l'explicació de com escriure dins d'un ou sense deixar rastre a la closca, utilitzant una tinta a base de pigments de plantes i alum. També s'hi descriu com escriure a la pell d'una persona sense que es vegi la tinta. El 4 de febrer de 1615, a l'avançada edat de 80 anys, Giambattista della Porta morí a la seva ciutat natal de Vico Equensa.

El *Furtivis Literarum Notis* va ser una de les obres més completes escrites fins

al moment. Porta no només es va centrar en les xifres que s'usaven a la seva època, sinó que també tracà l'evolució de la criptografia i descriu els mètodes usats des de l'Antiguitat. El principal historiador sobre criptografia, David Kahn, descriu el *Furtivis Literarum Notis* de la manera següent: "Fins i tot avui, quatre segles després, manté la seva frescor i encant, i -sorprenentment- la seva habilitat d'instruir. La seva gran qualitat és la seva perspectiva: Porta veia la criptologia completament"(Kahn, 1996:183). Al *Furtivis Literarum Notis* es descriuen tant xifrats antics com contemporanis, així com tècniques de criptoanàlisi juntament amb peculiaritats de les llengües que facilitaran l'anàlisi de freqüències. També s'hi descriu el que es coneix com ¨ la paraula probable", que es basa en aprofitar-se de saber quin és el tema del missatge per així poder-ne deduir les paraules que el formen, ja que depenent del tema, unes paraules són més freqüents que d'altres.

Porta donà una classificació, no molt diferent de l'actual, dels diferents mètodes de xifrat. Aquests es podien implementar o bé canviant de posició les lletres (transposició), o canviant la forma de les lletres usant símbols (substitució) o bé substituint-ne la identitat d'aquestes (substitució). L'obra de Porta contenia el primer criptosistema que xifrava dígrafs per un mateix símbol. Es tractava d'una taula que es mostra a la Figura 1, on a la línia de dalt i a la línia de la dreta s'hi posava l'alfabet -que en aquest cas constava de 20 lletres- i als espais del mig s'hi ubicaven els símbols que formaven el text xifrat. Els dígrafs es xifraven pel símbol que estigués a la intersecció de fila i columna de les dues lletres que el formaven. Matricialment, el dígraf ij es xifrarà com a_{ij}, on la matriu $A = (a_{ij})$ correspon a la matriu o taula que conté els símbols.

També s'hi descriuen discs semblants als usats per Alberti, que generaven un xifrat per substitució. A més a més, Porta explicà com transformar un xifrat usant un disc per un xifrat usant una taula, de manera que el xifrat fos el mateix però el mètode emprat fos diferent (tot i que formalment és el mateix). Referint-se als xifrats polialfabètics, donà consells sobre com escollir la clau. Porta optava per claus llargues i amb paraules poc rellevants, que no fossin d'ús comú.

Gràcies a la publicació de les obres de Trithemius i Belaso, i per a gran inconvenient dels criptoanalistes, els xifrats polialfabètics ja s'utilitzaven a l'època de Porta. Per això l'italià va descriure diversos exemples de com va arribar a trobar la clau d'una xifra polialfabètica, i com en va reconstruir la contraxifra. Les aportacions que va fer en aquest camp de la criptoanàlisi van passar desapercebudes, fins i tot per ell mateix, ja que no les hi donà rellevància. De manera independent, al segle XIX, Charles Babbage (1791-1871) i Friedrich Wilhelm Kasiski (1805-1881) utilitzaren els mateixos principis que Porta va intuir per a desxifrar les xifres polialfabètiques, concretament la xifra de Vigenère.

7 Blaise de Vigenère (1523-1596)

Vigenère és, probablement, un dels noms més coneguts dins del món de la criptografia, estretament lligat a la que ha passat a la història com la *chiffre indéchiffrable*, en francès, ¨ la xifra indesxifrable". Tanmateix, l'autoria d'aquesta obra és dub-

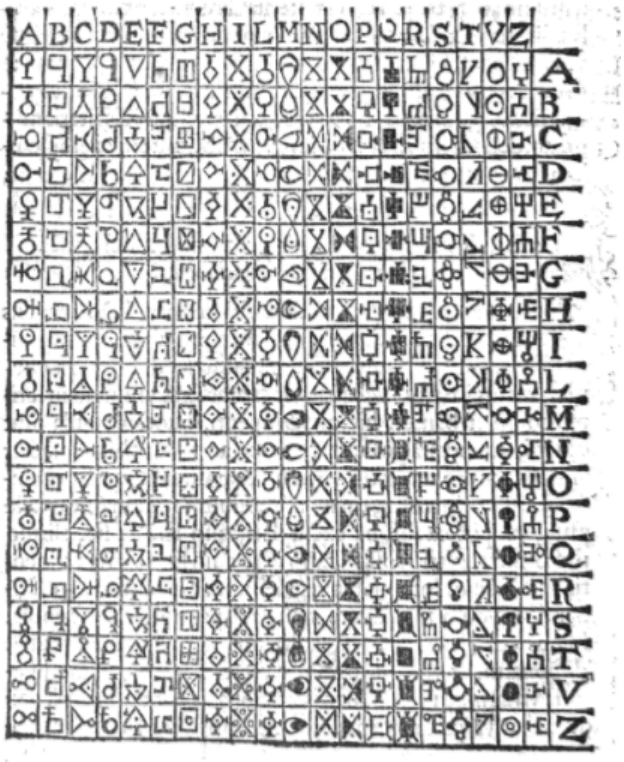

Figura 1: Taula dígrafs

tosa. Si bé Vigenère la va descriure i és gràcies a ell que es va popularitzar, els noms ja vistos de Porta i, sobre tot, de Belaso, també hi estan relacionats. Seria ingenu pensar que Vigenère va inventar-se aquest xifrat ell sol, tenint en compte que a la seva obra *Traicté des chiffres* cita diversos noms de criptògrafs anteriors a ell, incloent-hi Trithemius, Belaso, Porta i Cardano.

En contraposició al nombrós volum d'obres que escrigué, els detalls que ens arriben de la seva vida són relativament pocs. Blaise de Vigenère va néixer al poble de Saint Pourçain sur Sioule al 5 d'abril de 1523. El seu pare es va encarregar de donar-li una bona educació. Per aquest motiu, Vigenère es va traslladar a París, on hi va estudiar grec i hebreu. Al 1540, amb tan sols 17 anys, va abandonar els estudis i va passar a exercir com a diplomàtic a la cort francesa. Al cap de 5 anys, juntament amb el representant francès Louis Adhémar de Grignan, va ser enviat a la Dieta de Worms, una assemblea de prínceps del Sacre Imperi Romanogermànic encapçalada per l'emperador Carles V, instaurada el 1521. Aquesta va ser la major iniciació en la diplomàcia, i el va portar a viatjar per nombrosos països d'Europa. A l'edat de 24 anys, va entrar com a secretari al servei del Duc de Nevers (1516-1562). El Duc mantenia estrets vincles amb els reis francesos Francesc I i Enric II. Vigenère mantingué aquest càrrec fins a la mort del Duc. Esporàdicament, continuà exercint de diplomàtic a la cort, i al 1549, amb 26 anys, es traslladà a Roma per tal de complir una missió que durà 2 anys. Va ser durant aquest període que s'interessà profundament per la criptografia. Va llegir els llibres, anteriorment descrits, de Trithemius, Belaso, Cardano, Porta i fins i tot el manuscrit d'Alberti, que encara

no havia estat publicat. Vigenère digué:

> Au surplus ceux qui iusques icy en ont mis quelque chose dehors, entre les autres a esté l'abbé Tritheme; & Cardanincidemment par endroits; puis Baptiste Porte Neapolitain en un iuste volume à part, intitulé, *De furtiuis literarum notis*; où toutesfois ce à quoy il insiste le plus, est d'enseigner les moiens de dechiffrer sans alphabet; exercice certes d'un inestimable rompement de cerueau, & en fin un trauail tout inglorieux.(VIGENÈRE, 1587:12r).

Notem que pel que comentà de l'obra de Porta, Vigenère no era massa partidari ni d'ensenyar ni de desxifrar els missatges. Així doncs, Vigenère va estar clarament influït per les obres precedents. A més a més, també coneixia els mètodes de xifrat antics, tals com l'escítala grega i el xifrat de Cèsar, del qual en diu que "sovint usaven certes transposicions", (VIGENÈRE:11v). Observem que, amb la classificació actual, no és un xifrat de transposició tal com digué Vigenère, sinó que és de substitució. De la seva obra es dedueix que, durant l'estada a Roma, va tenir contacte amb criptògrafs papals, ja que n'explicà anècdotes. Va marxar de la cort francesa als 39 anys, i hi va tornar l'any 1566 com a secretari de l'ambaixada romana. Mantingué aquest càrrec fins el 1569. Finalment va ser nomenat secretari de cambra del rei Enric III de França (1551-1589). Un any més tard, amb 47 anys, Vigenère va demanar la seva jubilació. Donà la seva pensió de 1000 lliures anuals als pobres i mendicants de París. Se sap que es va casar amb una tal Marie Varé, més jove que ell. Des d'aquest moment Vigenère va dedicar el que li quedava de vida a escriure. Redactà una vintena de llibres, molts dels quals van passar bastant desapercebuts. Alguns d'ells són *La somptueuse et magnifique entrée du roi Henri III en la cité de Mantoue* publicat al 1576; *Les commentaires de César, des guerres de la Gaule. Mis en françois par Blaise de Vigenère, Secretaire de la Chambre du Roy. Avec quelques annotations dessus*, del 1582; *Les Décades que se trouvent de Tite-Live* (1583), *Traicté du Feu et du Sel*,publicat al 1608. Encara que molts llibres eren de caràcter històric, el *Traicté du Feu et du Sel* tracta d'alquímia, tema que juntament amb la Càbala jueva, Vigenère en va parlar al seu llibre sobre criptografia. Cal destacar també el *Traicté des Comètes ou étoiles chevelues*, del 1578, el qual va ajudar a desmitificar la creença que els cometes eren un càstig de Déu contra la humanitat. Indubtablement, l'obra més coneguda de Vigenère és el *Traicté des Chiffres, ou Secrètes Manières d'Escrire*, publicada al 1586. Blaise de Vigenère morí el 19 de febrer del 1596 a París, a causa d'un càncer a la gola. Les seves despulles es troben a l'església de Saint Étienne du Mont, a la mateixa ciutat.

7.1 Traicté des Chiffres

El *Traicté des Chiffres, ou Secriètes Manières d'Escrire* és una extensa obra, on s'hi detalla múltiples mètodes de xifrat. S'hi descriuen sistemes usats a l'Antiguitat i mètodes contemporanis a Vigenère. A l'obra també hi apareixen nous sistemes de xifrat basats en autors anteriors a ell. Pel que fa als que no són creats per ell mateix, Vigenère fou meticulós a l'hora d'atribuir-los a altres autors, així com a citar les seves obres. Així doncs, es pot confiar en les referències que apareixen a

l'obra. Tanmateix, gran part del *Traicté des Chiffres* està dedicat al comentari i a l'explicació de temes sobre Déu, la Càbala, el misticisme cristià, l'alquímia i la metafísica en general. Això és degut a que ell considerava que "totes les coses d'aquest món no són res més que una vertadera xifra"(VIGENÈRE:53r). Sovint, en fa una exposició llarga i tediosa que, pels interessats estrictament en temes criptogràfics, és totalment innecessària. D'aquesta manera, les quasi 700 pàgines quedaran substancialment reduïdes a la part en què parla de criptografia. Tampoc no és l'objectiu del present treball descriure tots els mètodes que apareixen a l'obra, ja que molts d'ells són repetitius i sense cap interès matemàtic rellevant. S'intentarà oferir una visió general del text, donant alguns exemples dels xifrats que es descriuen, i centrada en la xifra, posteriorment anomenada indesxifrable. Si bé no és indesxifrable, no va ser fins a principis del segle XIX que es va sistematitzar la manera de com desxifrar-la gràcies a l'obra de Kasiski *Die Geheimschriften und die Dechiffrierkunst* (*L'escriptura secreta i l'art del desxifrat*), publicada al 1863. El mètode que presentava Kasiski era bastant "artesanal¨ i actualment existeixen procediments més eficients, tals com utilitzar l'índex de coincidència i conceptes relacionats amb la teoria de la informació. Recordem que Vigenère, referint-se a la criptoanàlisi, escrigué que és un "trencament de cervell i un treball gens gloriós". Llegint aquesta frase no és d'estranyar que a l'obra no hi aparegui explicat cap mètode de criptoanàlisi. No obstant això, hi apareix un càlcul de les diverses formes en què es poden reordenar les lletres d'una paraula o d'una frase. A la pàgina 191v del *Traicté*, Vigenère donà el càlcul de les permutacions d'una possible frase de fins a 22 lletres (val a dir que el càlcul no és del tot precís). El *Traicté des Chiffres* és un text format bàsicament per mètodes de xifrat, temes que es poden anomenar metafísics i passatges de la història, amb anècdotes intercalades. Sovint, quan Vigenère parli de temes més filosòfics, ho ignorarem sense comentar-ho, ja que aquests hi abunden.

Vigenère començà l'obra abordant temes de filosofia grega i cabalista. Descrigué que hi ha dues maneres d'escriure: la d'ús ordinari i l'"oculta secreta"de la qual en digué:

> qu'on desguise d'infinies sortes, chacun selon sa fantasie, pour ne la rendre intelligible qu'entre soy & ses consçachans. Ce sont les chiffres, [...] auiord'huy non appropriez à autres effects que pour les affaires du monde, & les negociations & practiques, aussi bien des particuliers que des Princes.(VIGENÈRE:3v)

Exposà la seva visió, segons la qual antigament les xifres eren utilitzades per a transmetre el coneixement teològic. Seguidament dedicà l'obra a nobles francesos, i seguí amb el seu discurs filosòfic. A la pàgina 10v[3], reprengué el subjecte de les xifres i digué que l·l'usage en a esté de sort longuemain, voire apair presque de l'escriture, s'il n'est deuant". Considerava els jeroglífics com una forma de xifrat, així com altres formes d'escriptura orientals. A la següent pàgina, Vigenère descrigué alguns mètodes "vulgars"tals com l'escítala grega, l'autor de la qual digué que era Arquimedes de Siracusa. També va descriure, citant a Suetoni, el clàssic xifrat de Cèsar, és a dir, amb $r = 3$. A la pàgina 12r, hi apareix el paràgraf anteriorment citat sobre Trithemius, Cardano i Porta. De Trithemius afegí que "aquest ha estat,

[3]Es fa ús de la notació r (recto) i v (verso) per a referir-nos a la pàgina del tractat corresponent.

sincerament, el primer qui ha fet el camí als altres, almenys públicament; en dues grans i laborioses obres, un imprès, a saber, la Polygraphia, i [...] la Steganografia"(VIGENÈRE:12v). És obvi que Vigenère va estudiar les obres de l'abat, ja que les comentà i explicà amb detall, llibre per llibre.

A la pàgina 36r del tractat, Vigenère presentà la informació sobre el mètode de xifrat que va descriure vàries pàgines més endavant. Es tracta del mateix xifrat que hem descrit a *La cifra del Sig. Giovan Battista Belaso.* Vigenère considerà que Belaso va ser el primer en utilitzar aquest mètode. De Porta digué que també el va usar, encara que a la seva obra no es faci referència a Belaso sobre l'ús d'aquest xifrat.

> Premierement donques ie mettray le chiffre, que i'attribue quan à moy à un certain Belaso de la suitte du Cardinal de Carpi, pour auoir esté le premier de tous ceux dont i'ay eu cognosissance, qui le practiqua & mit en auant l'an 1549, que is fuz à Rome la premiere fois: Car le liure cy deuant allegué de Baptiste Porte, auquel il a inferé ce chiffre sans faire mention dont il le tenoit. (VIGENÈRE:36r)

Vigenère va fer una menció especial a l'aportació de Belaso en tant que va ser el primer en fer servir claus per a aquest mètode. També esmentà a Trithemius com a precursor de l'ús de taules, encara que en aquest cas siguin diferents. Tanmateix, afegí que "hi ha moltes taules a la Polygraphia de Tirthemius, però poques ben utilitzades."(VIGENÈRE:36v)

A aquesta mateixa pàgina, Vigenère deixà entreveure que va crear un sistema, actualment considerat d'autoclau, per tal que l'emissor i el receptor del missatge xifrat, només s'hagin de posar d'acord en una lletra. "[...]i'y ay, de mon invention puis-ie dire, amené l'artifice de faire dependre toutes les lettres l'une de l'autre, ainsi que par enchaisnement, ou liaison de maçonnerie; & ce par leur collocation & suiuances, selon que vous pourrez veoir cy apres". Aquest mètode consistia en usar el text en clar com a clau, però corregint els grans errors del sistema proposat per Cardano.

Al llarg de les pàgines següents, Vigenère exposà la seva visió segons la qual tots els xifrats provenen de la tradició mística jueva, on hi apareixien ocults. No és fins a la pàgina 45v que Vigenère no començà a parlar del xifrat de Belaso. Introduí la taula de la forma següent:

> DES CHIFFRES donques dont nous auons fait ceste premiere disgression& saillie, la premiere table en est telle, où il y a infinis coups à ruer;dont nou-nous contenterons d'en toucher icy les principaux traicts, sur lesquels la dexterité des bons esprits pourra forger plusieurs autres.

Es reprodueix la taula a continuació:

A	a	b	c	d	e	f	g	h	i	l
B	m	n	o	p	q	r	s	t	u	x
C	a	b	c	d	e	f	g	h	i	l
D	x	m	n	o	p	q	r	s	t	u
E	a	b	c	d	e	f	g	h	i	l
F	u	x	m	n	o	p	q	r	s	t
G	a	b	c	d	e	f	g	h	i	l
H	t	u	x	m	n	o	p	q	r	s
I	a	b	c	d	e	f	g	h	i	l
L	s	t	u	x	m	n	o	p	q	r
M	a	b	c	d	e	f	g	h	i	l
N	r	s	t	u	x	m	n	o	p	q
O	a	b	c	d	e	f	g	h	i	l
P	q	r	s	t	u	x	m	n	o	p
Q	a	b	c	d	e	f	g	h	i	l
R	p	q	r	s	t	u	x	m	n	o
S	a	b	c	d	e	f	g	h	i	l
T	o	p	q	r	s	t	u	x	m	n
V	a	b	c	d	e	f	g	h	i	l
X	n	o	p	q	r	s	t	u	x	m

Veiem que la taula és quasi idèntica a la que apareixia a *La cifra del Sig. Giovan Battista Belaso*. Les úniques diferències són que Vigenère utilitzà un alfabet de 20 lletres -ABCDEFGHILMNOPQRSTUX- i, seguint la mateixa notació que a la contraxifra de Belaso, en aquest cas $d_1 = 0$, $d_2 = 1$, $d_3 = 2$, $d_4 = 3$, $d_5 = 4$, $d_6 = 5$, $d_7 = 6$, $d_8 = 7$, $d_9 = 8$, $d_{10} = 9$. Notem que, a diferència de Belaso, Vigenère desplaçà les 10 files ordenadament, és a dir, $d_i = i - 1$, per a $i = 1, 2, ..., 10$. Així doncs, la manera de xifrar que va presentar és quasi idèntica a usar una tabula recta amb una determinada clau. Vigenère descrigué aquest sistema i, en una nota del lateral esquerre de la pàgina, hi trobem el nom que li dóna a la xifra: "revolució circular de commutacions d'alfabets". Recordem que es tractava d'un xifrat per substitució. Vigenère va fer la seva explicació, començant per recalcar la senzillesa i utilitat del mètode i comentà que era impossible que ningú pogués oblidar aquest alfabet. Descrigué la taula de la manera següent:

> [...] d'autant que tout gist au secret des clefs, qui dependent des lettres capitales marquees en teste à la main gauche des alphabets: Et se peuuent ces clefs varier en autant de sortes qu'on veult, presqu'en infiny, fust-ce pour escrire une mesme chose sans sortir hors du present chiffre, toutes differentes l'une de l'autre. (VIGENÈRE:46v)

La clau s'haurà de buscar a les lletres majúscules de l'esquerra, i pot ésser tan variada com es vulgui. A la mateixa pàgina, Vigenère explicà els motius pels quals

ha omès les dues lletres y i z a l'alfabet. El primer d'aquests és per a fer-les servir de "nul·les", és a dir, col·locar-les adequadament al text xifrat per tal de confondre a l'atacant. El receptor, que prèviament coneixerà els caràcters nuls del xifrat, simplement ignorarà tals lletres. Aquesta pràctica era comuna entre els xifrats de l'època de Vigenère, ja que introduint més caràcters d'una manera determinada, es podia dificultar l'anàlisi de freqüències. El segon motiu pel qual va ometre les dues lletres és menys precís: "per donar un significat secret diferent, que no té res a veure amb els caràcters, sinó al lloc on són"(VIGENÈRE:46v). El tercer motiu era per a distingir els mots entre ells en cas que s'ometin els espais al text xifrat. Les dues lletres es col·locaven entre les dues paraules, de tal manera que el desxifrador sabrà on és la separació. Notem que la y i la z utilitzades no estaran xifrades. Encara que ometre els espais sembli de sentit comú, rarament es feia. Tanmateix, quan aquesta pràctica es duia a terme, els desxifradors tenien molts més problemes a l'hora de desxifrar el text, encara que actualment no en suposi més. Vigenère ho remarcà quan es refereix a ometre els espais en blanc, on també aprofità per recalcar que aquesta xifra ja és indesxifrable per si sola:

> [...] est un grand soulagement pour le dechiffreur, auquel ceste confusion de dictions est un inutile surcrez de trauail, sans aucun fruit; car pour cela, le chiffre estant inuincible de soy, ceux qui en cuideroient venir à bout sans auoir communication du secret, mesmement des clefs, n'en auront pas meilleur marché. (VIGENÈRE:47r).

Vigenère tornà a divagar dient que les claus es poden agafar de versos amb un significat profund. Distingia l'escriptura vulgar de la xifrada, i de l'última en digué que pot ser escrita d'infinites maneres diferents, utilitzant "transposicions, commutacions, i símbols"(VIGENÈRE:47v).

Per fi Vigenère començà a descriure com s'utilitzava la contraxifra que va presentar a les pàgines anteriors tot posant un exemple per il·lustrar el mètode.

> Prenons donques le moien de ceste table; & que la clef du chiffre soit *Le iour obscur; & la nuit claire*: mais partons là en deux, pour faire voir la difference qu'il y aura, ne se seruant que de la moitié en ce premier; ouquel vous procederez en la sorte. Cherchez en la colonne des capitales, la lettre L, qui est la premiere de nostre clef, & voyez quelle lettre respond en son alphabet à celle de A, la premiere aussi du sujet; ce sera S. Poursuiuez ainsi de lettre en lettre tant que la clef se pourra estendre"(VIGENÈRE:47v-48r)

Vigenère agafà com a text en clar la frase *Au nom de l'eternel soit mon commencement*. La clau era *Le iour obscur; & la nuit claire* . Tanmateix, per a mostrar les diferències en utilitzar vàries claus, al primer exemple que posà només va fer servir la primera part de la clau. Per començar, busquem la primera lletra de la clau en la columna en majúscules de l'esquerra, en aquest cas la *L*. Seguidament, busquem la primera lletra del text en clar -la A- i la substituïm pel seu equivalent a la taula, en aquest cas la *s*. Vigenère, a diferència de Belaso, mostrà l'exemple complet:

> "Puis estant au bout vous la reitererez de nouueau: u de e, donne a: n de i, f: o de o, h: m de u, l: d de r, s: e de o, u: l de b, x: e de s, s : t de e, i: e de u, r: r

de r, c: n l de f [aquí s'entén que volia dir *n de l, f*]: e de e, o: l de i, r: s de o, c: o de u, b: i de r, n: t de o, d: m de b, a: o de s, l: n de c, c: c de u, p: o de r, l: m de l, e: mde e, c: c de i, s: n de o, g: e de u, p: e de r, t: m de o, g: e de b, q: n de s, i: t de e, i."(VIGENÈRE:48r)

Quan Vigenère deia ¨ u de e, donne a", es referia a que la lletra u del text en clar, xifrada usant la lletra e de la clau, es xifra com una a. Formalment, $f(u)_e = a$, o equivalentment, $f(18)_4 = 0$. Aquesta manera de xifrar ja està descrita a l'apartat de Belaso, així que no s'entrarà en més detalls. Vigenère continuà exposant maneres i trucs per tal de dificultar la tasca del desxifrador. Proposava posar quatre lletres al davant del text xifrat amb l'objectiu de confondre l'interceptor. Les quatre lletres són *drgq*(VIGENÈRE:48r). Continuà emfatitzant que, per tal de distingir les paraules entre si, s'han d'intercalar les lletres y i z com a separadors. Com a exemple de frase xifrada, Vigenère donà el següent:

Vostre cotexte sur ceste clef de, *Le iour obscur*, pour ce premier vers, *au nom de l'eternel soit mon commencement*, sera tel: *drgqsayfhlzsuyxsircforzobndyalczplecsgptgqiiy.*(VIGENÈRE:48r)

Aquest és el primer exemple que donà utilitzant una xifra polialfabètica. Tal com s'ha dit, Vigenère substituïa els espais entre paraules per les lletres y i z. Els tractats de criptografia ensenyaven tot posant exemples de l'ús de diversos mètodes. Així doncs, Vigenère continuà mostrant el mateix mètode però amb una clau diferent. El seu objectiu era emfatitzar l'ús de la clau i el canvi total que experimentava el xifrat si es variava. L'exemple era el següent:

Que si vous le voulez escrire par l'autre clef, *la nuit claire*, vous ferez de mesme, a de l, s: u de a, i: n de n, g: o de u, b: m de i, e: d de t, r: e de c, p: l de l, r: e de a, q: t de i, b: e de r, t: r de e, g: n de l, f: e de a, q: l de n, q: s de u, f: o de i, g: i de t, m: t de c, i: m de l, e: o de a, c: n de i, f: c de r, r: o de e, l: mde l, e: m de a, a: a de n, r: n deu, a: c de i, u: e de t, s: mde c, b: e de l, m: n de a,b: t de i, b. Premettez ces autres quatre lettres pour varier, car cela n'importe pas; puis qu'elles ne seruent de rien *fsbm*; & inferez les nulles à la fin des mots comme dessus.(VIGENÈRE:48r-48v)

Aquí Vigenère va utilitzar les quatre lletres *fsbm* per tal de confondre a l'interceptor de manera idèntica que al primer exemple. La frase quedà xifrada com *fsbmsiygbezrpyrqbtgfqqzfgmiyecfzreearausbmbb*. Vigenère tornà a recalcar que, canviant la clau del sistema, el xifrat es modifica completament encara que s'usi un mateix alfabet i contraxifra. Amb aquest sistema, l'únic que és necessari és mantenir la clau en secret. Si això es compleix, és impossible que ningú no pugui conjecturar res sobre el text en clar, encara que hi treballi persistentment (VIGENÈRE:48v). Evidentment, la impossibilitat que afirmava Vigenère no era certa.

Al text següent, Vigenère donà ¨ algunes regles generals sobre les claus".

Quãt ausdites clefs, il n'est pas possible ny necessaire nomplus d'en prescire ne limiter aucune reigle, attendu que cela depend de la volonté de chacun, qui se les

> peut forger à la fantasie d'infinies sortes. Les uns s'entredonnent certaine quantité de mots conuenuz entr'eux; le premier desquels doit seruir pour la presmiere depesche; le second pour la seconde; & ainsi du reste: il est bien vray que tant plus longue est la clef, tant plus sera malaisé le chiffre ?? descouurir; mais tãt plus difficile aussi & embrouillé tãt au chiffrer qu'au dechiffrer;(VIGENÈRE:48v)

Explicà que les claus poden ser curtes o llargues, a gust de cadascú. Hi havia qui s'intercanviava algunes paraules, de manera que la inicial servia per a la primera entrega d'un missatge, la segona per la propera, etc. S'ha de tenir en compte el context en què es feien servir aquests mètodes. Com ja s'ha vist amb altres personatges, sovint duien a terme funcions diplomàtiques en països o ciutats allunyades de les seves ambaixades. Era convenient haver-se posat d'acord amb les claus dels missatges entre emissor i receptor, ja que les distàncies podien ésser llargues. Sembla que Vigenère era partidari de no usar claus molt llargues, ja que dificultaven la manera de xifrar. No obstant això, era conscient que usar claus llargues també dificultava la feina del possible interceptor. Si s'utilitzaven claus molt curtes, aquestes s'havien d'anar repetint per xifrar el text en clar, i això proporcionaria certa periodicitat al text xifrat. La clau podria ésser utilitzada per al criptoanalista. Vigenère explicà que algunes persones empraven la frase d'algun poema com a clau, o utilitzaven el dia de la data en què s'enviava el missatge, com ara "quinze d'octubre"(VIGENÈRE:49r).

Vigenère explicà com es poden fer servir paraules del text xifrat com a clau. S'entén, però, que les paraules són en clar, ja que sinó es crearia el mateix problema que tingué Cardano. Vigenère també proposà usar com a clau les lletres nul·les que posava als exemples anteriors, així com les lletres que servien com a separador. Igualment descrigué com usar l'alfabet com a clau, començant per una lletra aleatòria i seguint, o no, l'ordre:

> [...]les autres y emploient le dernier mot qui precede l'escriture chiffree, ou l'une des lettres mises deuant en lieu de nulles, qui leur ser de clef par mesme moien; sur laquelle ayans chiffré tout le premier mot, il pourra seruir de clef au second; le secõd au tiers, & ainsi des autres; que s'il y a quelques interualles d'escriture commune, ils le continuent au chiffrement qui vient puis apres; ou bien le recommancent de nouueau[...]. D'autres poursuiuent & euacuent tout l'alphabet lettre apres autre, commançant à laquelle que bon leur semble, tant que la reuolution soit paracheuée; & puis recommancent circulairement, qui est une grande multiplication de labeur (VIGENÈRE:49r).

A continuació Vigenère presentà el seu mètode d'auto-clau:

> [...]si que ie m'artesterois plus volontiers à une seule lettre, dont de main en main partira successiuement tout le reste, cõme si elles venoient à naitre les unes des autres(VIGENÈRE:49r).

Aquest mètode consisteix en posar-se d'acord entre l'emissor i el receptor en una sola lletra. Aleshores, el desxifrador podrà usar la primera lletra com a clau. D'aquesta manera obtindrà una primera lletra del text en clar, que serveix de clau

per a desxifrar la següent lletra, i així successivament de forma recursiva. És a dir, si la clau consta de n dígits $\{k_0, k_1, ..., k_{n-1}\}$, on k_0 és conegut, la clau es calcularia de manera recursiva com $k_1 = f_{k_0}^{-1}(y_0)$, $k_2 = f_{k_1}^{-1}(y_1)$,..., $k_i = f_{k_{i-1}}^{-1}(y_{i-1})$ $\forall$ $i = 1, 2, ..., n-1$, on $\{y_0, y_1, ..., y_{n-1}\}$ denoten els dígits del text xifrat. Notem que per a conèixer $f^{-1}(y_0)$ només necessitem k_0, que ja coneixem. Aquesta manera recursiva de construir la clau està ben definida, i genera una única possible interpretació del text en clar. Vigenère explicà el mètode mitjançant un exemple, ja que considerà que és la manera més clara per entendre el sistema:

> [...] ou en chiffrant touiours la susequente par la precedente en ceste sorte sur la mesme sujet dessusdit; *Au nom de l'eternel*; dõt la clef soit *D*, nous dirons; a de d donne x; u de a, i: n de u, a: o de n, h: m de o, g: d de m, u: e de d, p: l de e,t: c de l, m: t de e, l: e de t, s: r de e, h: n de r, i: e de n, x: l de e, t. Tellement que par ceste voye prenant *D* pour clef, il y auroit *dxiahguptmlshixt.*(VIGENÈRE:49v)

A l'exemple que donà Vigenère, xifrà la frase *Au nom de l'eternel*. La lletra-clau és $k_0 = d$. Així doncs, $f_d(a) = x$, $f_a(u) = i$, $f_u(n) = a$,...,$f_e(l) = t$. El text xifrat és *xiahguptmlshixt*. Vigenère posà la lletra clau al principi del text xifrat per indicar-la al receptor. Per a desxifrar el missatge, el desxifrador ha de procedir al revés: "[...] x de d, faict a: i de a, u: a de u, n: h de n, o: g de o, m. & ainsi du reste"(VIGENÈRE:49v). És a dir, $f_d^{-1}(x) = a$, $f_a^{-1}(i) = u$, etc. Així es recuperava el text en clar, *au nom de l'eternel*. Vigenère afegí, una altra vegada, que es poden intercalar les lletres y i z com a separadors de paraules. Mitjançant un altre exemple, explicà una manera "més oculta"per a xifrar. Consistia en xifrar no usant la lletra precedent com a clau, sinó la posterior, de la manera següent:

> [...] a de d, qui est la clef, dira x: u de x, h: n de h, e: o de e, e: m de e, c: d de c, o: e de o, u: l de u, m: e de m, x: t de x, g: e de g, n: r de n, a: n de a, b: e de b, q: l de q, o. assemblez ce sera; *dxheecoumxgnabqo*. Pour le dechiffrer, x de d, fait a: h de x, u: e de h, n: e de e, o: c de e, m. (VIGENÈRE:49v)

Es té que la clau és $\{k_0, ..., k_{14}\}$=DXHEECOUMXGNABQ, és a dir, el text xifrat afegint la d al principi. Per a xifrar, el mètode es pot escriure com $f_{k_0}(x_0) = y_0 = k_1$,..., $f_{k_{n-1}}(x_{n-1}) = y_{n-1} = k_{n-1}$. En aquest cas tenim que $f_d(a) = x$, $f_x(u) = h$, $f_h(n) = e$, etc. Per a desxifrar s'utilitza el mateix procediment d'abans, ja que es coneix la primera lletra-clau $k_0 = d$. $f_d^{-1}(x) = a$, $f_h^{-1}(x) = u$,..., $f_q^{-1}(o) = l$. Tenim que $k_i = y_{i-1}$ per a $i = 1, ..., n-1$.

7.2 *Le chiffre indéchiffrable*

Fins ara s'ha presentat el mètode que explicà Belaso a *La cifra del Sig. Giovan Battista Belaso*, tal com ho va fer Vigenère. S'ha explicat com Vigenère donà exemples complets i parcials del sistema usant la contraxifra, i com col·locà les lletres amb un ordre diferent al de Belaso, segurament influenciat per la tabula recta de Trithemius (qui aplica un desplaçament de i posicions a la fila i). El que Vigenère exposà de nou són els diversos mètodes per obtenir claus. En particular,

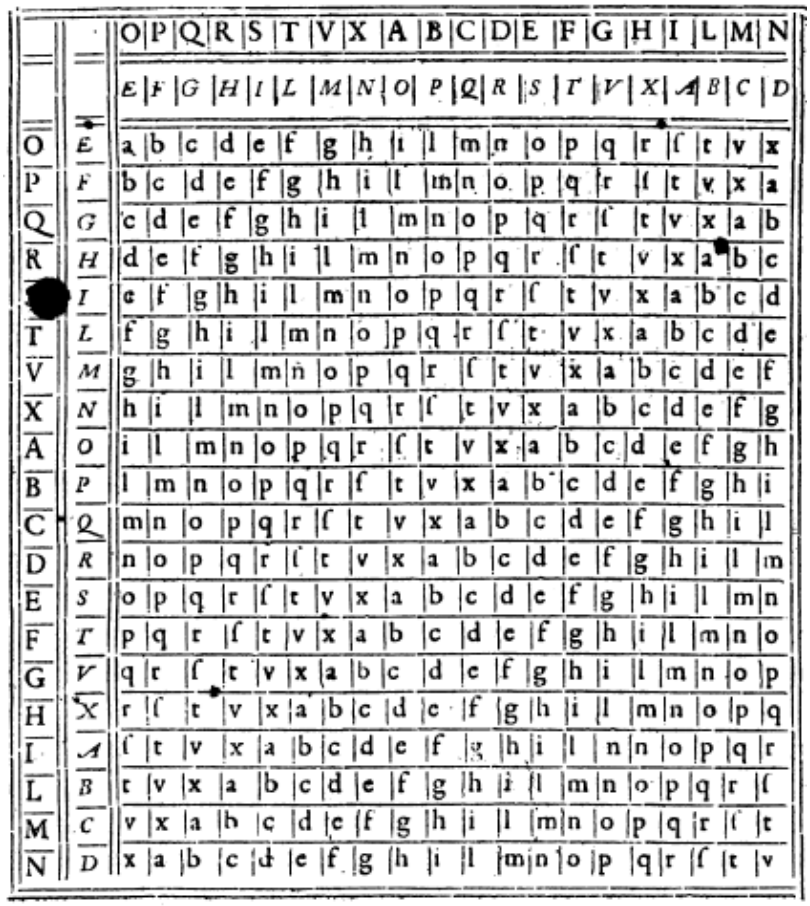

Figura 2: Taula usada per Vigenère

va solucionar els problemes del sistema d'auto-clau proposat per Cardano i n'oferí de diferents usant el mateix principi. En aquest apartat, es descriu el que ha passat a la història com a ¨ la xifra indesxifrable". Aquest nom es deu al fet que van passar gairebé dos segles abans no va ser desxifrada pels ja esmentats Babbage i Kasiski. Tanmateix, el mètode que ha passat a la història no és el que pretenia descriure Vigenère al *Traicté des Chiffres*. Tal com assenyala Charles J. Mendelsohn, "As given by Vigenère himself the cipher differs in important respects from the method just described"(Mendelsohn, 1940:108). A la Figura 2 es mostra la taula que apareix al Traicté i que Vigenère utilitzà per a explicar el seu xifrat.

El que es coneix com a xifrat de Vigenère és una millora de la tabula recta que emprà Trithemius. Usualment, consisteix en usar una taula com la que es reprodueix a continuació:

	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	X
A	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x
B	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	a
C	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	a	b
D	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	a	b	c
E	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	a	b	c	d
F	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	a	b	c	d	e
G	g	h	i	l	m	n	o	p	q	r	s	t	u	x	a	b	c	d	e	f
H	h	i	l	m	n	o	p	q	r	s	t	u	x	a	b	c	d	e	f	g
I	i	l	m	n	o	p	q	r	s	t	u	x	a	b	c	d	e	f	g	h
J	l	m	n	o	p	q	r	s	t	u	x	a	b	c	d	e	f	g	h	i
L	l	m	n	o	p	q	r	s	t	u	x	a	b	c	d	e	f	g	h	i
M	m	n	o	p	q	r	s	t	u	x	a	b	c	d	e	f	g	h	i	l
N	n	o	p	q	r	s	t	u	x	a	b	c	d	e	f	g	h	i	l	m
O	o	p	q	r	s	t	u	x	a	b	c	d	e	f	g	h	i	l	m	n
P	p	q	r	s	t	u	x	a	b	c	d	e	f	g	h	i	l	m	n	o
Q	q	r	s	t	u	x	a	b	c	d	e	f	g	h	i	l	m	n	o	p
R	r	s	t	u	x	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q
S	s	t	u	x	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r
T	t	u	x	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s
U	u	x	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t
X	x	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u

Observem que l'única diferència que hi ha entre aquesta taula i la que usava Trithemius és que a la primera hi ha una fila i una columna addicionals en majúscules, que serveixen per xifrar el text segons una clau. Sigui la clau $\{k_0, k_1, ..., k_{n-1}\}$, de llargada n, el text en clar $\{x_0, x_1, ..., x_{N-1}\}$, amb $n \leq N$. Aleshores $f(x_j) = x_j + k_i \pmod{20}$, on $i \equiv j \pmod{n}$, per a $j = 0, ..., N-1$. k_i representa l'equivalent numèric a una determinada lletra de la clau. Com que els alfabets en majúscules estan ordenats, k_j coincideix amb l'r_j del desplaçament de Cèsar. Com ja s'ha dit, aquest mètode difereix del que descrigué Vigenère, i no es tindrà que $k_j = r_j \pmod{20}$. Vegem com ho va descriure ell mateix; el presentà de la següent manera:

> Mais tout cecy se peut practiquer aussi bien, voire trop mieux, par la table encore suiuante, combien que tout reuienne presqu'à un, prenant les capitales trauersantes qui sont au front d'enhaut, pour le sens qu'on veut exprimer: & les perpendiculaires au costé gauche descendant en bas, au lieu de clefs.(Vigenère:49v)

A la taula que presentà Vigenère (a la Figura 2), les lletres en majúscula de la part de dalt en perpendicular s'utilitzen pel text en clar, i les de l'esquerra en vertical per a la clau. Una primera diferència amb la taula anterior és que hi ha dues files de lletres en majúscula, tant per la clau com pel text en clar. A més, aquestes estan desordenades. El fet que les lletres referents a la clau i al text en clar estiguin desordenades no permet formular el xifrat com abans. Per exemple, la lletra "E"ocupa la primera posició i, per això, no aplica cap desplaçament a

l'alfabet. En canvi, si s'utilitzés el mètode "estàndard", al xifrat corresponent a la fila "E"s'hi hauria d'aplicar un xifrat de Cèsar amb $r = 4$. Al paràgraf següent Vigenère explicà el motiu pel qual hi ha dues files en majúscula:

> I'en ay mis icy deux rengees; l'une de noir, l'autre de rouge, pour monstrer que les alphabets tant de l'escriture, que des clefs, se peuuent transposer & chãger en tant de sortes qu'on voudra; afin d'en oster la cognoissance à tous autres qu'à ses correspondans.(VIGENÈRE:49v)

Comentà que les dues files estan escrites en colors diferents -negre i vermell- per tal de distingir-les. No obstant això, a la còpia que s'utilitza per aquest treball no es distingeixen, ja que el text està escanejat en blanc i negre. La frase que marcà la principal diferència és la que indica que les dues files esmentades es poden intercanviar i transposar de la manera que es vulgui. Això es faria en un mateix xifrat. Aleshores, hi haurien diversos alfabets de xifrat per a una mateixa lletra de la clau, i diferents longituds de desplaçaments de tipus Cèsar per a cada lletra-clau. Per exemple, per a la lletra-clau "E"es podrien aplicar xifrats de Cèsar amb $r = 0$ (mirant la columna vertical de la dreta) i $r = 12$ (mirant la columna vertical de l'esquerra). Què passa si, en comptes de canviar les columnes referents a la clau, s'intercanvien les files referents al text en clar? Per fixar idees, considerem la lletra-clau "E"de la columna de la dreta i la lletra a xifrar "g"de la fila de sota. Busquem la intersecció de fila i columna i tenim que $f_E(g) = c$. Si utilitzem la fila de dalt per al text en clar tenim que $f_E(g) = q$. En ambdós casos hem usat la mateixa lletra-clau. Això resulta ser una "doble polialfabeticitat", ja que per una mateixa lletra-clau tenim diversos alfabets. Aleshores, fixant una columna per a les claus, cada lletra-clau té dos possibles alfabets.

L'avantatge principal d'intercanviar les files del text en clar és la següent: suposem que l'atacant ha descobert la longitud de la clau i sap que, per a k_j, $f_{k_j}(g) = c$. Si haguéssim utilitzat el xifrat de Vigenère estàndard, l'atacant automàticament sabria la clau r_j. En canvi, si hem utilitzat el xifrat que descrigué Vigenère, l'interceptor encara no podria conèixer la clau r_j. Aquesta és la principal fortalesa del mètode que exposà originàriament Vigenère.

Com que el xifrat que presentà Vigenère està intrínsecament lligat a la taula, i per tant al desordre de les files i columnes del text en clar i la clau, una formulació abstracta i més general no sembla la més adient, ja que no seria massa pràctica. El descriurem de forma matricial de la manera següent, usant l'alfabet de 20 lletres: sigui la matriu $A = (a_{ij})$, 22 x 22, formada pels elements de la figura 2. Denotem per $k_{j,t}$, $j = 2, ..., 21$, $t = 0, 1$, les lletres de la clau, i $x_{r,i}$, $i = 2, ..., 21$, $r = 0, 1$, les lletres de l'alfabet (no les del text en clar) en l'ordre que correspongui (és a dir, $k_{2,0} = O$, $k_{2,1} = E$, $x_{0,2} = O$, $x_{1,2} = E$,...). Aleshores $f_{k_{j,t},\, r}(x_{r,i}) = a_{ji}$. Per a desxifrar es té que $f^{-1}_{k_{j,t},\, r}(a_{ji}) = x_{r,i}$. Els subíndexs r i t indiquen quina columna i fila s'està usant per a la clau i per al text en clar. Notem que seran dues funcions diferents tant per a xifrar com per desxifrar, ja que es canvien els alfabets i sinó es tindria dos possibles valors per al desxiframent. La funció (més concretament, el subíndex r) indica quina fila per al text en clar s'està usant per a xifrar cada lletra. De cara als exemples, és més pràctic xifrar mirant la intersecció entre la clau i el

text en clar directament a la taula.

Per il·lustrar aquest nou mètode, Vigenère posà un exemple per mostrar com fer servir la taula:

> Pour chiffrer donques les mesmes mots, *au nom de l'eternel*, sur la clef *le iour obscur* procedez ainsi: *a* de l'alphabet transuersal marqué de *rouge* [correspon a la fila de sota], sevient rencontrer auec *l* du perpendiculaire en la chambre de *b*: u de e, sera q: n de i, n: o de o, s: m de u, a: d de r, m: e de o, i: l de b, c: e de s, o: t de c, n: e de u, q: r de r, c: n de l, o: e de e, a: l de i, l. Somme *bqnsami conqcoal*, & ainsi du reste. (VIGENÈRE:50r)

La clau és *le iour obscur*, i el text en clar, altre cop, *au nom de l'eternel*. Vigenère xifrà mirant la taula i buscant la intersecció entre la lletra-clau i la lletra clara. Per aquest exemple, Vigenère usà les files i columnes que estan a tocar de la tabula recta original. Així doncs, $f_{l,1}(a_1) = b$, $f_{e,1}(u_1) = q$,..., $f_{i,1}(l_1) = l$.

Vigenère finalitzà aquesta explicació dient que l'ús d'aquesta taula no era una idea seva, sinó que l'havia extreta de la *Polygraphia* de l'Abat Trithemius i d'altres autors que no especificà. Vigenère acabà remarcant els diversos usos i maneres de xifrar mitjançant la taula esmentada:

> si ont bien les beaux usages d'icelle; car i embrouille tout cela; & ceux qui se sont meslez de l'interpreter en une confusion d'orchemes, &infinité de reuolutions d'alphabets, laborieux & embrouillez ce qui se peut, & auec tout cela inutiles; de fort peu d'industrie au reste, & inuention; la où ceste table peut seruir pour tout.(VIGENÈRE:50r)

En aquestes pàgines que s'han citat i comentat, Vigenère explicà tot el que fa referència al seu xifrat més destacat. S'ha mostrat que el xifrat que ha passat a la història difereix del que va descriure el propi Vigenère. No és l'objectiu d'aquest treball comparar quin mètode és més robust a atacs, però sí mostrar-ne les diferències.

8 Conclusions

Aquest treball de final de grau presenta una breu descripció dels mètodes criptogràfics i esteganogràfics que s'han usat des dels seus suposats inicis, fins a l'obra de Blaise de Vigenère al segle XVI. La part principal ha consistit en establir i remarcar les diferències entre el xifrat estàndard de Vigenère i el que presentà ell mateix. S'ha donat informació sobre les influències que va rebre a l'hora de formular aquest xifrat, així com una anàlisi dels diversos mètodes que explicaren altres autors destacats.

Al llarg de la memòria s'ha intentat extreure la informació directament de les fonts originals. Gran part de la tasca realitzada ha consistit en recerca i consulta de material bibliogràfic. S'ha consultat una edició original escanejada del *Traicté des Chiffres, ou Secrietes Manières d'Escrire* (edició del 1587) i de *La cifra del Sig. Giovan Battista Belaso* (edició del 1553). També s'han consultat altres obres originals, tot i que l'idioma -llatí- en què estaven escrites n'ha impedit un estudi més profund. A partir d'aquests textos s'han traçat les principals explicacions que donaren els autors sobre els seus xifrats. En alguns casos aquests coincidien, però es presentaven de manera diferent.

Referències

[1] Vigenère, Blaise de. *Traicté des Chiffres, ou Secrièmes Manières d'Escrire*. París: 1587. Disponible a: https://books.google.es/

[2] Belaso, Giovani Battista. *La cifra del Sig. Giovan Battista Belaso*. Venècia, 1553. Disponible a: https://books.google.es/

[3] Belaso, Giovan Battista.*Il vero modo di scrivere in cifra*. Brescia, 1564. Disponible a: https://books.google.es/

[4] Porta, Giovani Battista della. *De furtivis literarum notis*. John Wolphius (ed.), 1591. Disponible a: https://books.google.es/

[5] Kahn, David.*The Codebreakers*. Rev Sub. New York: Scribner, 1996. ISBN 978-0-684-83130-5.

[6] Singh, Simon. *Los códigos secretos*. 1a ed. Madrid: Debate, 2000. ISBN 84-8306-278-X.

[7] Singh, Simon. *Histoire des codes secrets*. 1a ed. París: Jean-Claude Lattès, 1999. ISBN 978-2-253-15097-8.

[8] Juher, David. *Introducció a la criptografia*. 2a ed. Girona: Publicacions docents (Universitat de Girona), 2001. ISBN 84-8458-022-9.

[9] Galende Díaz, Juan Carlos. *Criptografía. Historia de la escritura cifrada*. 1a ed. Madrid: Complutense, 1995. ISBN 84-89365-29-6.

[10] Dorce Polo, Carlos. *Història de la matemàtica: des de Mesopotàmia fins al Renaixement*. 2a ed. Barcelona: Publicacions i Edicions de la Universitat de Barcelona, 2015. ISBN 978-84-475-4217-8.

[11] Dorce Polo, Carlos. *Història de la matemàtica: des del segle XVII fins a l'inici de l'època contemporània*. 1a ed. Barcelona: Publicacions i Edicions de la Universitat de Barcelona, 2014. ISBN 978-84-475-3799-0.

[12] Ycart, Bernard. Letter counting: a stem cell for Cryptology, Quantitative Linguistics, and Statistics. A:*Historiographia Linguistica*[arxiu pdf]. Berlín: E. F. K. Koerner, 2013. núm. 40. p. 303-329. [consulta:16/11/2017]. ISSN 0302-5160. Disponible a: https://arxiv.org/ftp/arxiv/papers/1211/1211.6847.pdf

[13] Adamson, Peter, "Al-Kindi", The Stanford Encyclopedia of Philosophy. Spring, ed 2015, Edward N. Zalta (ed.),[consulta:13/10/2017]. Disponible a: https://plato.stanford.edu/archives/spr2015/entries/al-kindi/

[14] Kerckhoffs, Auguste. *La cryptographie militaire* [arxiu pdf]. Journal des sciences militaires, Vol. IX, pp. 5-38, Gener 1883, pp. 161-191, Febrer 1883.[consulta: 6/10/2017] Disponible a: http://www.petitcolas.net/fabien/

[15] Azizi Abdelmalek, *La langue arabe, la Cryptographie et les Sciences mathématiques*[arxiu pdf]. Marroc: Faculté des Sciences, Université Mohammed I, 2010. Disponible a: https://www.researchgate.net/publication/235889389_La_langue_arabe_la_Cryptographie_et_les_Siences_mathematiques

[16] M. Mrayati, Y Meer Alam, M.H. At-Tayyan. *Arabic Origins of Cryptology.* Riad: KCFRIS & KACST, 2003. ISBN 9960-890-08-2.

[17] Reeds, Jim. *Solved: The Ciphers in Book III of Trithemius's Steganographia*[arxiu pdf]. New Jersey: AT&T Labs-Research, 1998. [consulta: 7/12/2017] Disponible a: http://profs.sci.univr.it/ giaco/download/Watermarking-Obfuscation/Trithemius.pdf

[18] Cardini, Roberto; Regoliosi, Mariangela. *Leon Battista Alberti. Autobiografia.* [consulta: 5/12/2017] Disponible a: https://www.academia.edu/35329863/Leon_Battista_Alberti_-_AUTOBIOGRAFIA

[19] Al-ahwal, Ayman; Farid, Sameh. *The effect of varying key length on a Vigenère cipher*[arxiu pdf]. IOSR Journal of Computer Engineering(IOSR-JCE). Vol. 17, 2, 2015. p. 18-23. ISSN: 2278-0661. [consulta: 27/12/17] Disponible a: https://www.academia.edu/26823898/The_Effect_Of_Varying_Key_Length_On_A_Vigen%C3%A8re_Cipher

[20] J. Mendelsohn, Charles. *Blaise de Vigenère and the Çhiffre Carré".*[en línia] Proceedings of the American Philosophical Society, Vol. 82, Nº2 (Mar. 22 1940). p. 103-129.[consulta: 27/12/2017] Disponible a: http://www.jstor.org/stable/985011