LE MACCHINE CIFRANTI: IL DISCO DI LEON BATTISTA ALBERTI

A metà del 1400 un grande matematico, latinista, letterato, musicista e architetto: Leon Battista Alberti attuò una vera analisi statistica della lingua e con un approccio totalmente scientifico analizzò l'uso delle vocali e delle consonanti e la frequenza delle lettere delle parole.

Grazie a quest'analisi comprese le inefficienze dei sistemi cifranti e allo scopo di renderli meno vulnerabili definì un codice polialfabetico.

Dunque in questa procedura si creano più alfabeti e più corrispondenze tra lettere

Leon Battista Alberti propone 3 metodi di cifratura, ma noi ne applichiamo solo 2.

Mittente e destinatario concordano una lettera minuscola, ad esempio k come chiave segreta.

ALFABETI DI PARTENZA :

1) 24 simboli ovvero le 20 lettere dell'alfabeto latino maiuscole, con la Z ed escluse le H,K, J, U (in latino equivalente a V) W, Y seguite dai numeri 1234: ABCDEFGILMNOPQRSTVXZ1234
2) 24 simboli ovvero le lettere minuscole con le 20 lettere latine classiche più h,k,y,& (quest'ultimo simbolo rappresenta la congiunzione et) in ordine casuale

   Quest'ultima regola, trascurata da molti successori dell' Alberti è fondamentale altrimenti si ha una semplice successione di Cifrari di Cesare.
3) Una chiave alfanumerica ovvero una lettera del secondo alfabeto (quindi non è un numero generico ma una lettera)

I numeri (1,2,3,4) verranno messi nel messaggio in chiaro e saranno considerati nulli.

Essendo un procedimento complesso prima applichiamo il procedimento in un caso particolare e poi proviamo a costruire l'algoritmo

ELEMENTI DI BASE:

1) Il primo alfabeto

A	B	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	2	3	4
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

2) Il secondo alfabeto

n	x	y	q	c	&	o	k	b	p	f	z	s	e	m	d	g	u	t	a	i	r	l	h
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

e la CORRISPONDENZA TRA LETTERE che ne deriva

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

3) La chiave: lettera k

Supponiamo di dover cifrare il seguente messaggio

INVIARE RINFORZI DOMANI

Come prima operazione il mittente elimina gli spazi tra le parole

INVIARERINFORZIDOMANI

Come seconda operazione il mittente inserisce a caso dei numeri tra le lettere

INV1IA2RERI4NFORZID3OMANI

Scriviamolo in una tabella

	I	N	V	1	I	A	2	R	E	R	I	4	N	F	O	R	Z	I	D	3	O	M	A	N	I

La cifratura comincia con una lettera B SCELTA A CASO da chi cifra

	I	N	V	1	I	A	2	R	E	R	I	4	N	F	O	R	Z	I	D	3	O	M	A	N	I
B																									

Dunque la lettera B non è UN ELEMENTO DI BASE, ma una seconda chiave indicata direttamente nel messaggio cifrato che appunto comincia con B scelta a caso

La lettera B occupa la posizione 2 e dunque si TRASLA IL SECONDO ALFABETO in modo che la chiave k vada ad occupare la posizione 2 (si è così creato IL NUOVO ALFABETO)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
o	k	b	p	f	z	s	e	m	d	g	u	t	a	i	r	l	h	n	x	y	q	c	&

E si costruisce la CORRISPONDENZA TRA LETTERE

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

Si poteva anche dire direttamente: si porta la chiave k sotto la B (lettera scelta come prima lettera del cifrato) ovvero si costruisce la seguente CORRISPONDENZA TRA LETTERE e poiché questa procedura dovremo applicarla più volte adotteremo questo spostamento diretto

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

dopodiché si cifrano (nella riga azzurra)alcune lettere con la NUOVA CORRISPONDENZA (nelle due righe verdi)

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

E poi si mette una maiuscola a caso (L) (TERZA CHIAVE)

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

E si ricomincia

Si porta la chiave k sotto la L (lettera scelta a caso) ovvero si costruisce la seguente

CORRISPONDENZA TRA LETTERE (nelle due righe verdi)

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

dopodiché si cifra un numero casuale di lettere con la NUOVA CORRISPONDENZA TRA LETTERE (nelle due righe verdi)

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

E poi si mette una maiuscola a caso (P) (QUARTA CHIAVE)

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

E si ricomincia

Si porta la chiave k sotto la P (lettera scelta a caso) ovvero si costruisce la seguente

CORRISPONDENZA TRA LETTERE (nelle due righe verdi)

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

Dopodiché si cifra un numero casuale di lettere con la

NUOVA CORRISPONDENZA TRA LETTERE (nelle due righe verdi)

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

E poi si mette una maiuscola a caso (Z) (QUINTA CHIAVE)

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

E poi si ricomincia

Si porta la chiave k sotto la Z (lettera scelta a caso) ovvero si costruisce la seguente CORRISPONDENZA TRA LETTERE (nelle due righe verdi)

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

Dopodiché si cifra un numero casuale di lettere con la NUOVA CORRISPONDENZA TRA LETTERE (nelle due righe verdi)

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

INV1IA2RERI4NFORZID3OMANI

diventa

primo)BeghyeoL

secondo)eiqeolpcafP

terzo)pmylZ

quarto)fhrsla

BeghyeoLeiqeolpcafPpmylZfhrsla

ALGORITMO

Inserimento casuale dei numeri del primo alfabeto nel messaggio da cifrare

Ripetizione fino ad esaurimento dei simboli del messaggio da cifrare della seguente procedura

“Scelta e scrittura nella cifratura di una maiuscola a caso

Costruzione di un nuovo alfabeto a partire dal secondo e mediante una traslazione

Costruzione di una relativa corrispondenza tra lettere

Cifratura di un numero di lettere a caso”