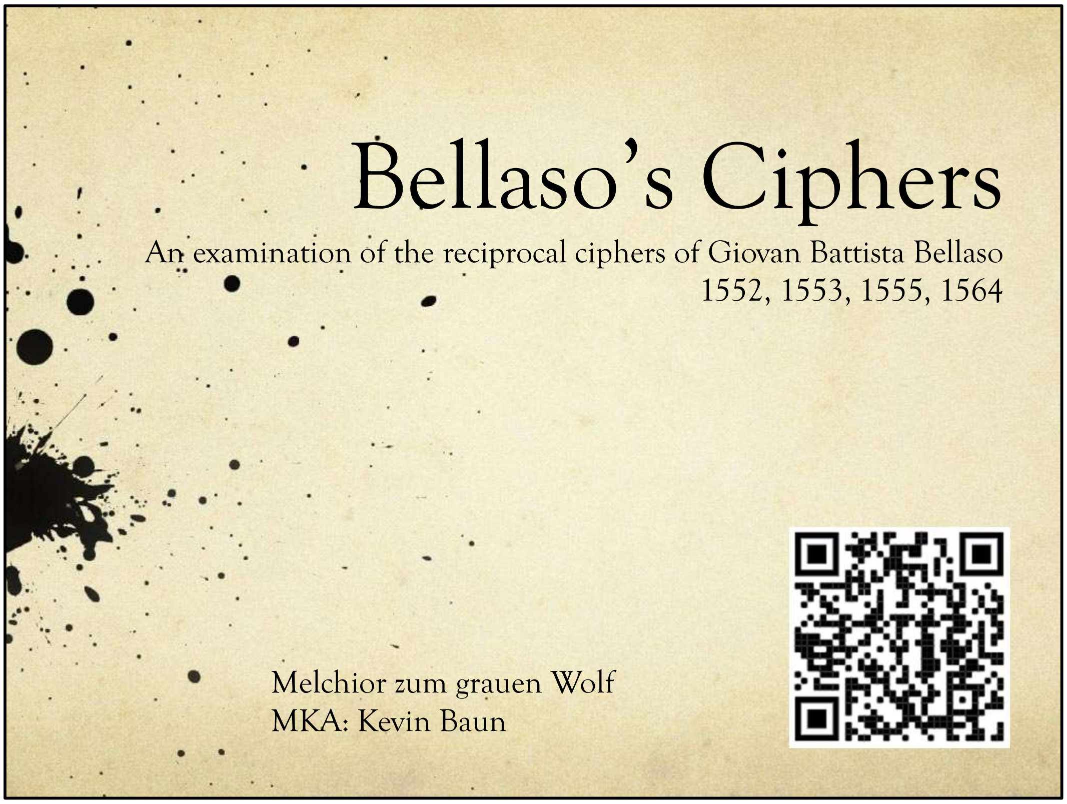


Bellaso's Ciphers

An examination of the reciprocal ciphers of Giovan Battista Bellaso
1552, 1553, 1555, 1564

Melchior zum grauen Wolf
MKA: Kevin Baun

Greetings and thank you for your interest in period cryptography.

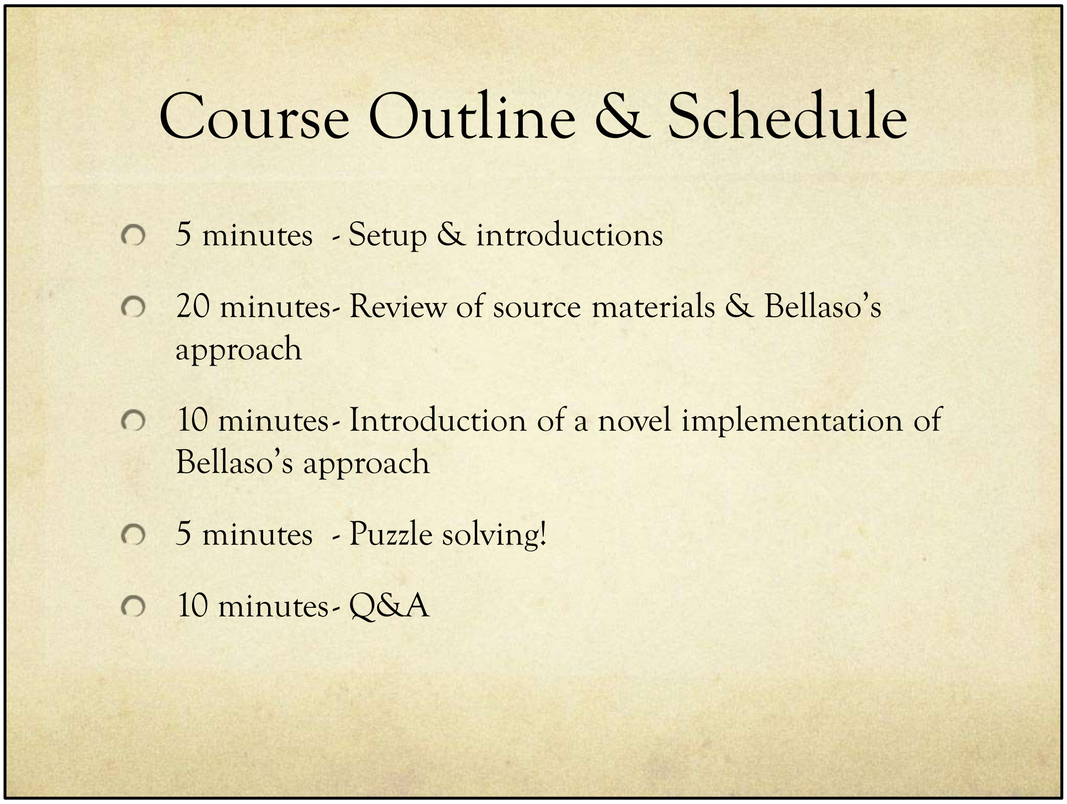
This class is intended to be a practical introduction to the work of Giovan Battista Bellaso. There is much material that we will not be covering in this presentation. For example: we will not be going into his life (little is known), work as a secretary and cryptographer for Cardinal Duranti (Brescia), from where he was dispatched to the Roman Curia. We will also not be discussing his apparent “concerns” about the work of G.B. Della Porta, much of which bears a STRONG resemblance to his own from several years prior. We will not go into depth for how Vigenère is given credit for the keyed rotational tablu even though he himself gives credit to Bellaso. Nope! Not going to talk about that stuff! ;-)

The objective of this class is to provide the information you need to know to work through some of Bellaso’s reciprocal ciphers. I hope that you find this introduction to be informative as well as enjoyable. I do not claim any degree of expertise on this specific subject. I’m sure that questions will be asked that I do not have an immediate answer for. Please feel free to contact me with any questions or comments that you may have and I will do my best to help you find an answer.

Programming note: This content is largely scripted, as I have a tendency to ramble, though I will not be reading off of the slides. This isn’t a death by PowerPoint presentation. There are only about 20 slides of content anyway. The rest is just pretty pictures. Following the link in the QR code seen here will take you to a site where you may download this presentation with the full class notes.

Contact information

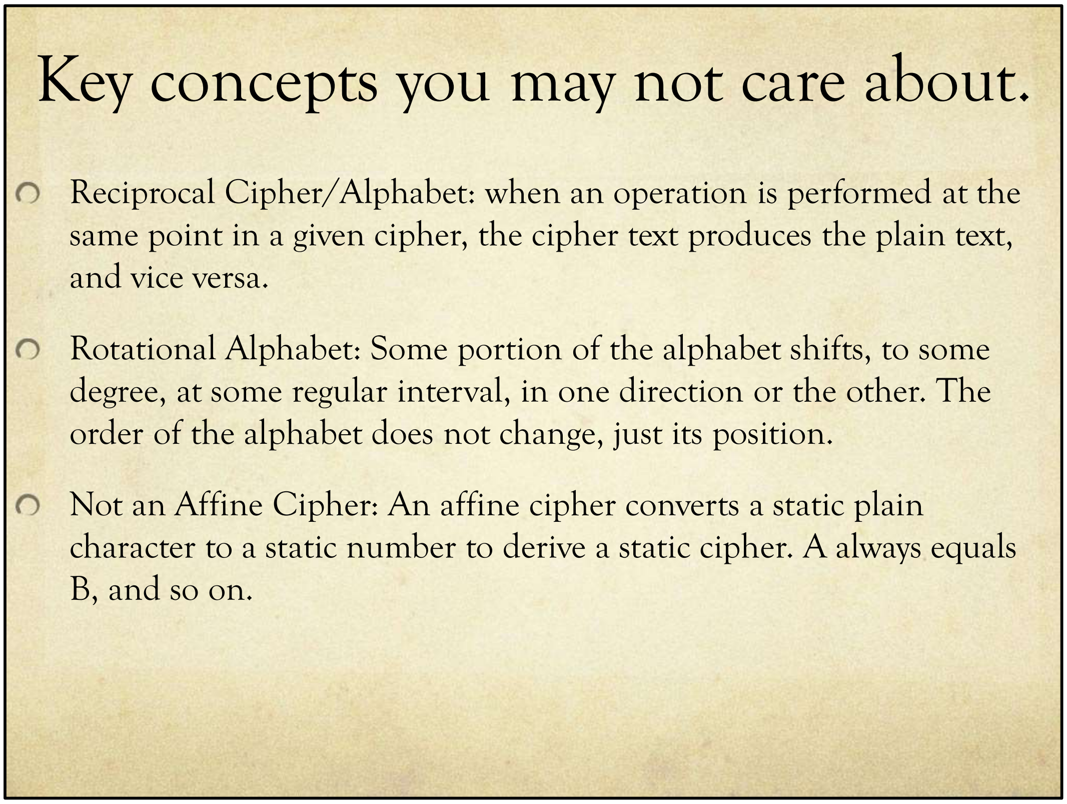
Melchior zum grauen Wolf, OP
melchior@houseblueheron.com
https://crypto.houseblueheron.com



Course Outline & Schedule

- 5 minutes - Setup & introductions
- 20 minutes- Review of source materials & Bellaso's approach
- 10 minutes- Introduction of a novel implementation of Bellaso's approach
- 5 minutes - Puzzle solving!
- 10 minutes- Q&A

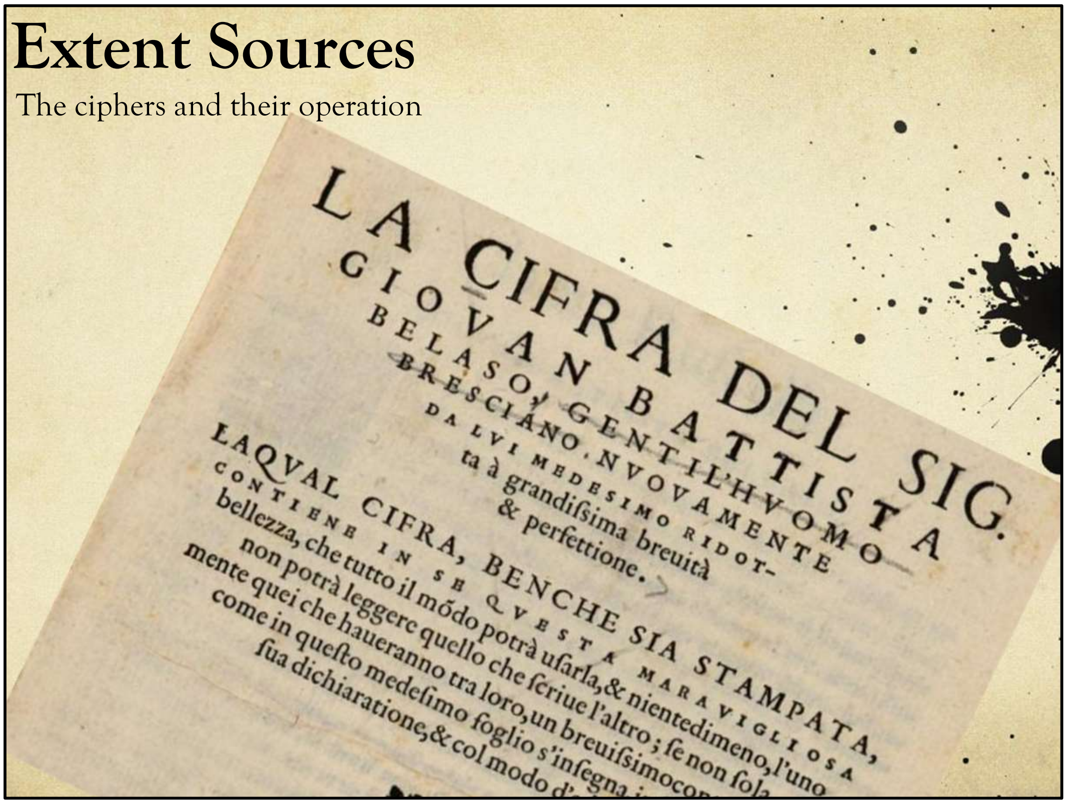
This class should take approximately 30-40 minutes. Assuming a standard 50 minute class this will allow you about 10 minutes of 'free time' for discussion. If you have a specific question about what we're talking about on a given slide then I encourage you to ask. I will offer a moment at the end of each slide to do so. General musings and discussion are welcome but I ask that you save those items for the end of the presentation at the Q&A.



Key concepts you may not care about.

- Reciprocal Cipher/Alphabet: when an operation is performed at the same point in a given cipher, the cipher text produces the plain text, and vice versa.
- Rotational Alphabet: Some portion of the alphabet shifts, to some degree, at some regular interval, in one direction or the other. The order of the alphabet does not change, just its position.
- Not an Affine Cipher: An affine cipher converts a static plain character to a static number to derive a static cipher. A always equals B, and so on.

These are some key concepts that we need everyone to be aware of before we begin to dive into the ciphers themselves. The first two concepts are essential to understanding the ciphers we are going to be addressing. Please ask questions if there is anything about this that is unclear. The final concept is not as important to understanding how to use Bellaso’s encryption but it is a very important distinction to make.



Extent Sources

The ciphers and their operation

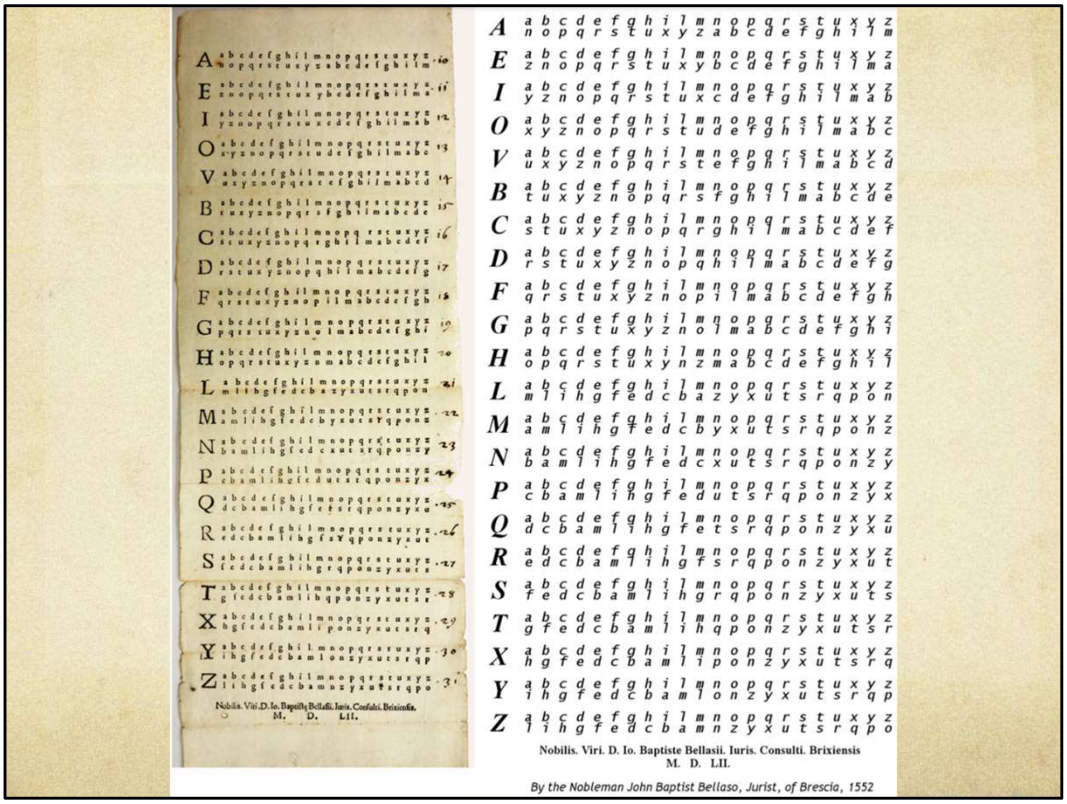
LA CIFRA DEL SIG.
GIOVAN BATTISTA
BELASO, GENTIL'HVOMO
BRESCIANO, NVOVAMENTE
DA LVI MEDESIMO RIDOT-
ta à grandiſsima breuità
& perfettione.

LAQVAL CIFRA, BENCHE SIA STAMPATA,
CONTIENE IN SE QVESTA MARAVIGLIOSA
bellezza, che tutto il mõdo potrà uſarla,& nientedimeno,l'uno
non potrà leggere quello che ſcriue l'altro; ſe non ſola
mente quei che haueranno tra loro,un breuiſsimocon
come in queſto medeſimo foglio s'inſegna
ſua dichiaratione,& col modo d'

We're going to start by looking at the existing period materials. We are fortunate that these works have all been scanned in and are available online for free. Direct links to the source material are available in the slide deck. Bellaso presents more than a handful of variations on reciprocal ciphers. It would be impractical to attempt to cover them all in the available time so I will be focusing on those ciphers that most directly build on each other through his publications. My intent is to show a progression, an evolution, of the reciprocal cipher through Bellaso's work.

References

Google Books: Retrieved 25 Feb 2022:
https://books.google.com/books?id=GbZRAAAAcAAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false



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

Nobilis. Viri. D. Io. Baptiste Bellasii. Iuris. Consulti. Brixiensis
M. D. LII.

By the Nobleman John Baptist Bellaso, Jurist, of Brescia, 1552

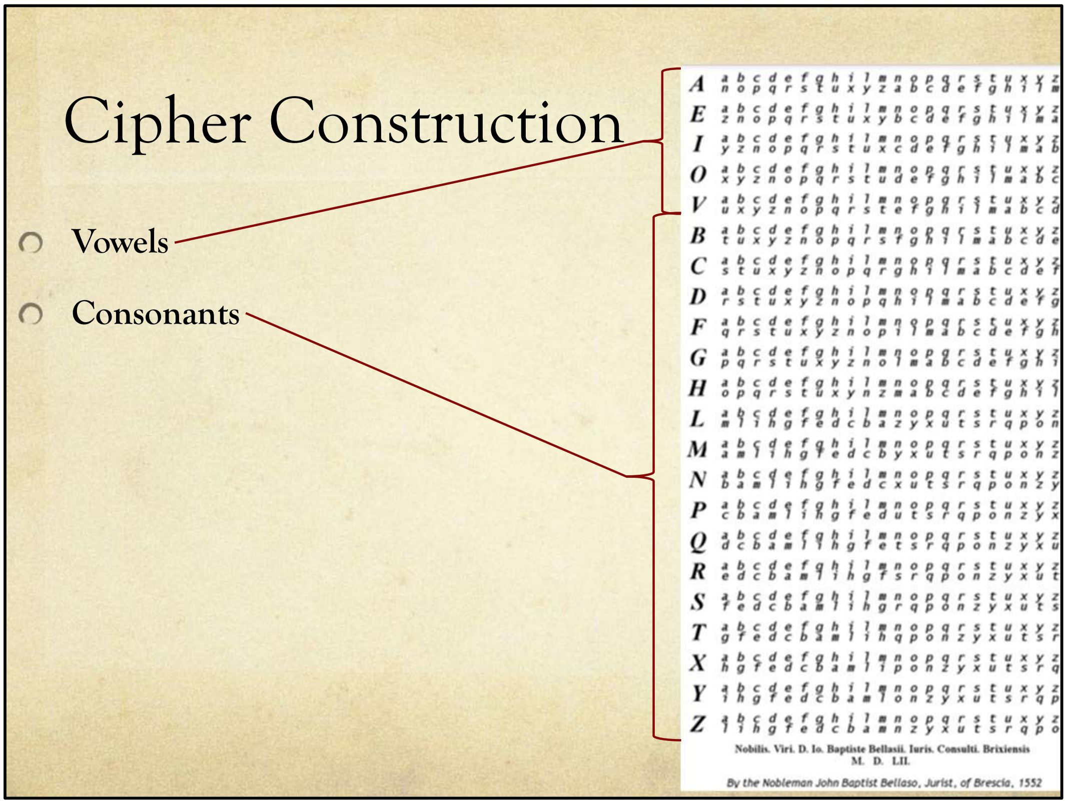
In 2018 a researcher, Paolo Bonavoglia, discovered this 1552 leaflet, presented without instruction or explanation, in the state archives in Venice. This previously unknown document presents 22 alphabet ciphers and is clearly marked as being Bellaso's work (see the footnote). You will notice that each alphabet is identified by a letter and that they are presented with the vowels preceding the consonants. While no instruction is provided with this document to indicate its intended operation we can see the fundamental operation in Bellaso's later publication of which all reciprocal ciphers employ the same basic mechanism of substitution, so a similar approach may be safely assumed here. I will be spending a little extra time here to describe the process as it is foundational to future ciphers.

To encipher a text we utilize a key word, DOG. Using the D cipher we would encipher 'CAT' with sequential alphabets starting with D such that (D)C=>T, (F)A=>Q, (G)T=>E or CAT == TQE. The key is then repeated for the length of the intended message by resetting the initial index for each subsequent word using the next character in the countersign (you can think of this as the password). I will detail this process on the next slide.

Make note of the split cipher text in the second line of each cipher. That line is split in half after the eleventh position such that each half of the enciphered text rotates independently. Notice, for the A cipher the pairing of m=z and n=a, then note the inward shift of each half of the cipher alphabet throughout the remainder of the set. Actually, let's take a quick closer look at how these alphabets are constructed.

References

Bonavoglia, P. (2019) Bellaso's 1552 cipher recovered in Venice, Cryptologia, 43:6, 459-465, DOI: 10.1080/01611194.2019.1596181



Cipher Construction

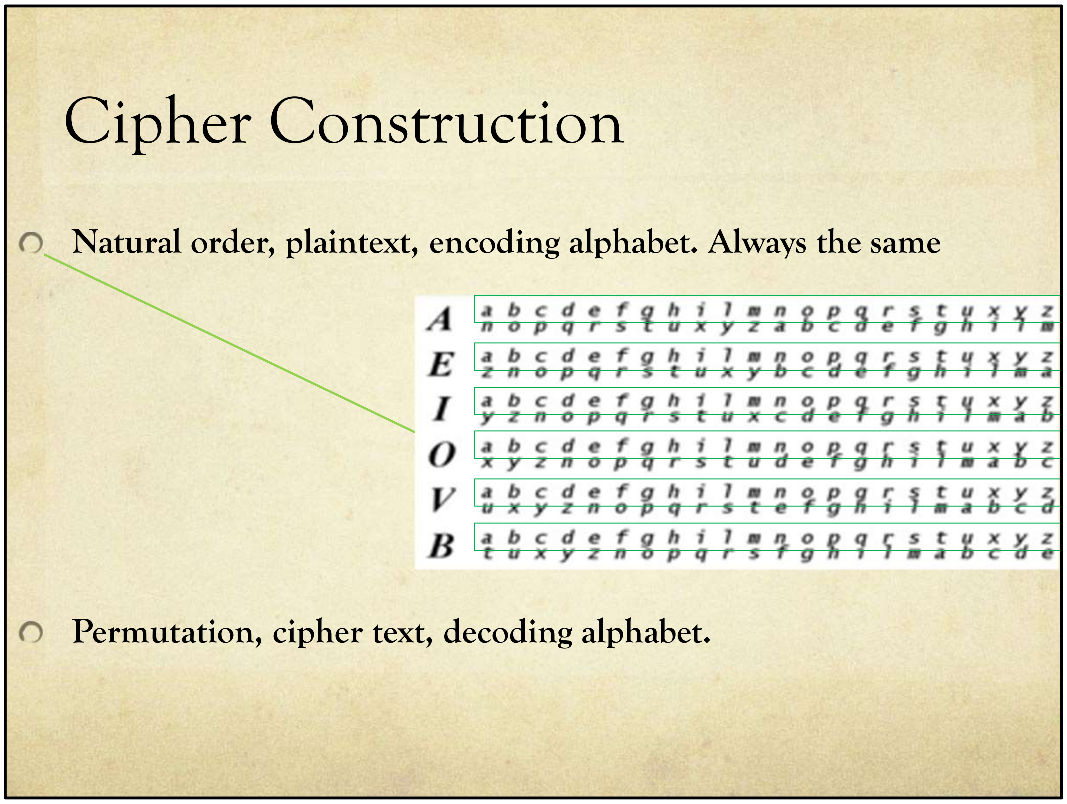
- Vowels
- Consonants

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

Nobilis. Viri. D. Io. Baptiste Bellasii. Iuris. Consulti. Brixiensis
M. D. LII.

By the Nobleman John Baptist Bellaso, Jurist, of Brescia, 1552

Here we see the construction of the cipher alphabets. Notice that the vowels are addressed first and followed by the consonants.



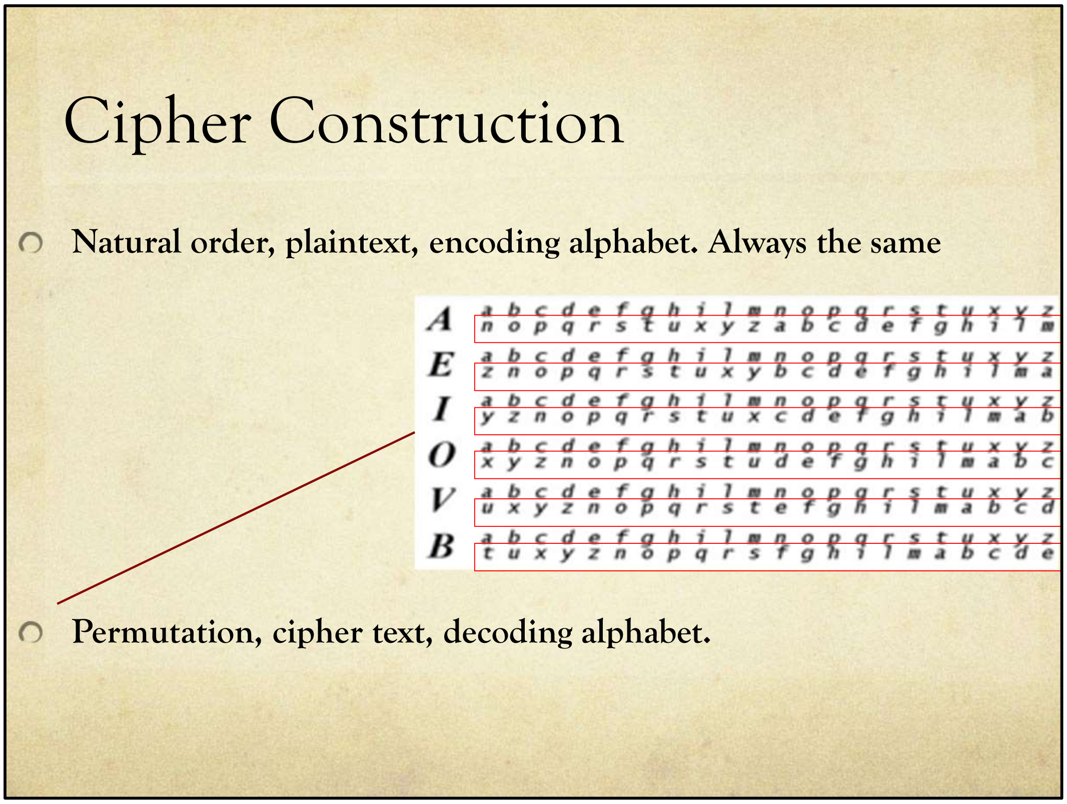
Cipher Construction

- Natural order, plaintext, encoding alphabet. Always the same

A	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	n	o	p	q	r	s	t	u	x	y	z	a	b	c	d	e	f	g	h	i	l	m
E	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	z	n	o	p	q	r	s	t	u	x	y	b	c	d	e	f	g	h	i	l	m	a
I	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	y	z	n	o	p	q	r	s	t	u	x	c	d	e	f	g	h	i	l	m	a	b
O	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	x	y	z	n	o	p	q	r	s	t	u	d	e	f	g	h	i	l	m	a	b	c
V	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	u	x	y	z	n	o	p	q	r	s	t	e	f	g	h	i	l	m	a	b	c	d
B	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	t	u	x	y	z	n	o	p	q	r	s	f	g	h	i	l	m	a	b	c	d	e

- Permutation, cipher text, decoding alphabet.

Each cipher alphabet has a pair or letter sets. The first, top, set of characters appears in natural order every time and does not change.



Cipher Construction

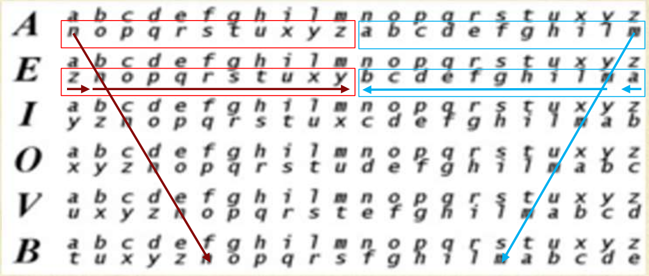
- Natural order, plaintext, encoding alphabet. Always the same

A	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	n	o	p	q	r	s	t	u	x	y	z	a	b	c	d	e	f	g	h	i	l	m
E	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	z	n	o	p	q	r	s	t	u	x	y	b	c	d	e	f	g	h	i	l	m	a
I	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	y	z	n	o	p	q	r	s	t	u	x	c	d	e	f	g	h	i	l	m	a	b
O	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	x	y	z	n	o	p	q	r	s	t	u	d	e	f	g	h	i	l	m	a	b	c
V	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	u	x	y	z	n	o	p	q	r	s	t	e	f	g	h	i	l	m	a	b	c	d
B	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	t	u	x	y	z	n	o	p	q	r	s	f	g	h	i	l	m	a	b	c	d	e

- Permutation, cipher text, decoding alphabet.

The second set of characters rotates by a position for each subsequent cipher alphabet.

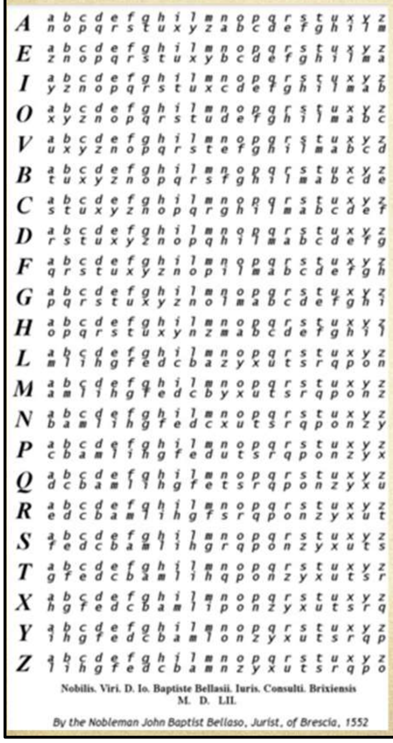
Cipher Text Construction



A	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	n	o	p	q	r	s	t	u	x	y	z	a	b	c	d	e	f	g	h	i	l	m
E	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	z	n	o	p	q	r	s	t	u	x	y	b	c	d	e	f	g	h	i	l	m	a
I	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	y	z	n	o	p	q	r	s	t	u	x	c	d	e	f	g	h	i	l	m	a	b
O	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	x	y	z	n	o	p	q	r	s	t	u	d	e	f	g	h	i	l	m	a	b	c
V	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	u	x	y	z	n	o	p	q	r	s	t	e	f	g	h	i	l	m	a	b	c	d
B	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	t	u	x	y	z	n	o	p	q	r	s	f	g	h	i	l	m	a	b	c	d	e

- Permutation, cipher text, decoding alphabet.

Notice here that each half of the alphabet rotates by one position for each successive cipher text. Once the rotation is complete the cipher alphabets are swapped and the process is repeated for the second half of the cipher generation.



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

Nobilis. Viri. D. Io. Baptiste Bellasii. Iuris. Consulti. Brixiensis
M. D. LII.

By the Nobleman John Baptist Bellaso, Jurist, of Brescia, 1552

Process

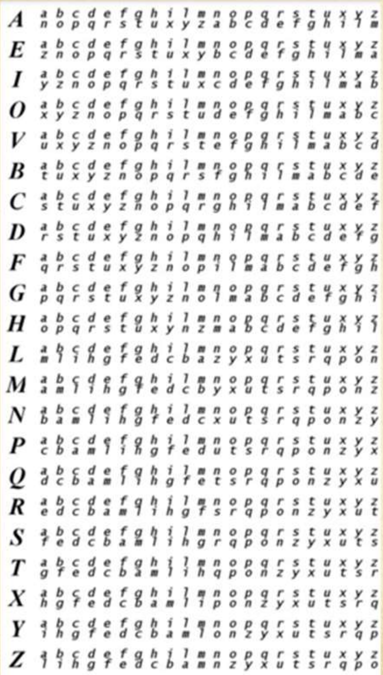
Encryption:

Countersign:	D	O	G
Plaintext:	C A T	F O X	B E A R
Alphabet:	D F G	O V B	G H L M
Ciphertext:	T Q E	P F C	Q S M S

Decryption:

Countersign:	D	O	G
Ciphertext:	T Q E	P F C	Q S M S
Alphabet:	D F G	O V B	G H L M
Plaintext:	C A T	F O X	B E A R

Now we'll take a detailed look at the encryption and decryption process.



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

Nobilis. Viri. D. Io. Baptiste Bellasii. Iuris. Consulti. Brixiensis
M. D. LII.

By the Nobleman John Baptist Bellaso, Jurist, of Brescia, 1552

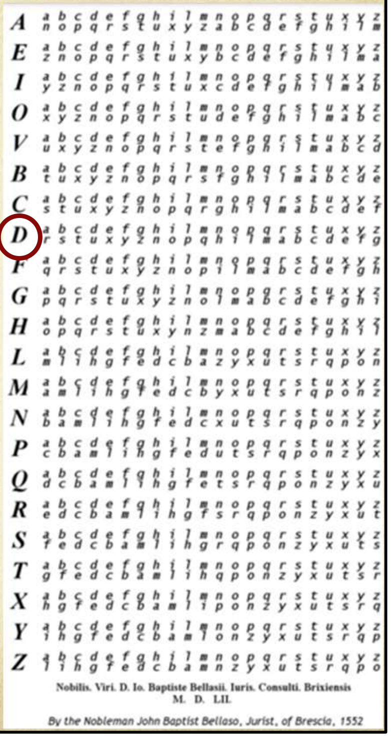
Process Overview

- **Encryption:**

Countersign:	D	O	G
Alphabets:	D F G	O V B	G H L M
Plaintext:	C A T	F O X	B E A R
Ciphertext:	T Q E	P F C	Q S M S

Select Initial Alphabet

- **Encryption:**
  - Countersign: D O G
  - Alphabet: DFG OVB GHLM
  - Plaintext: CAT FOX BEAR



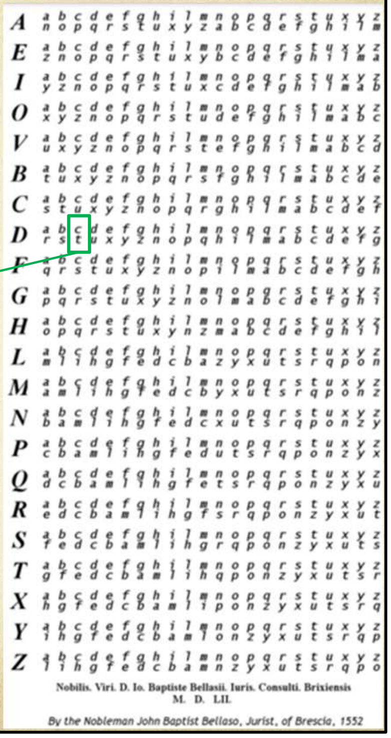
A	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	n	o	p	q	r	s	t	u	x	y	z	a	b	c	d	e	f	g	h	i	l	m
E	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	z	n	o	p	q	r	s	t	u	x	y	b	c	d	e	f	g	h	i	l	m	a
I	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	y	z
	y	z	n	o	p	q	r	s	t	u	x	c	d	e	f	g	h	i	l	m	a	b
O	a	b	c	d	e	f	g	h	i	l	m	n	o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

Nobilis. Viri. D. Io. Baptiste Bellasii. Iuris. Consulti. Brixiensis
M. D. LII.

By the Nobleman John Baptist Bellaso, Jurist, of Brescia, 1552

Encode Letter

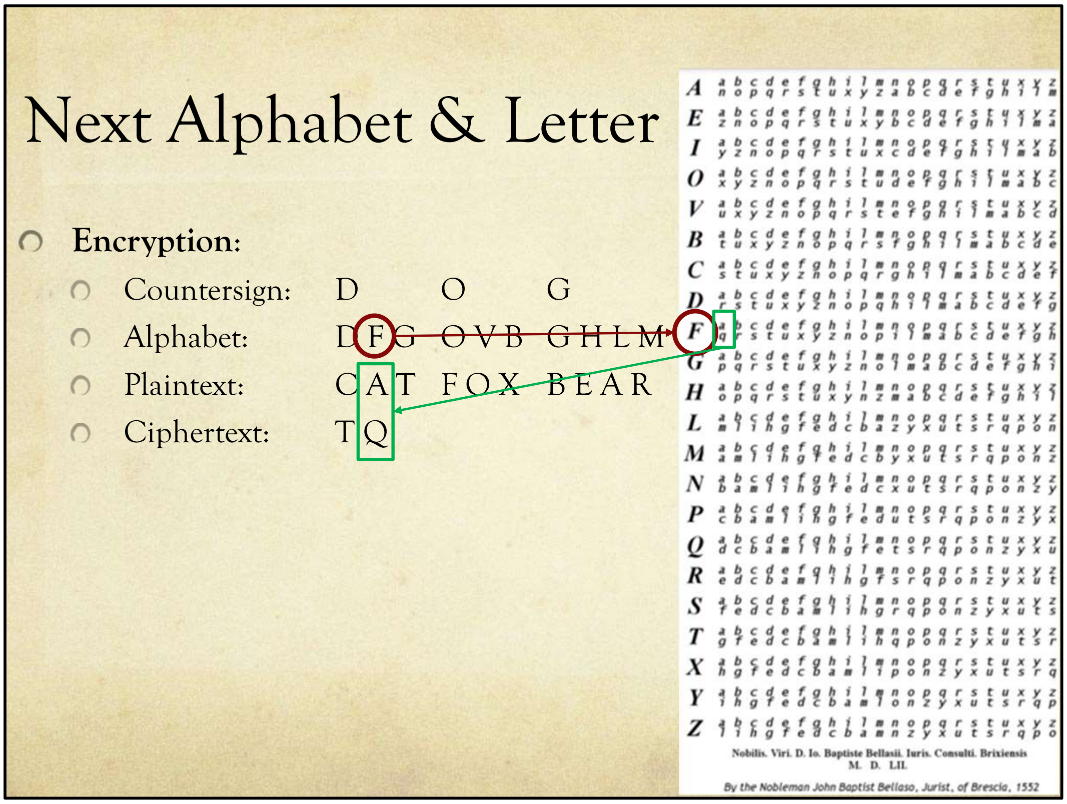
- **Encryption:**
  - Countersign: D O G
  - Alphabet: D F G O V B G H L M
  - Plaintext: C A T F O X B E A R
  - Ciphertext: T



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

Nobilis. Viri. D. Io. Baptiste Bellasii. Iuris. Consulti. Brixiensis
M. D. LII.

By the Nobleman John Baptist Bellaso, Jurist, of Brescia, 1552



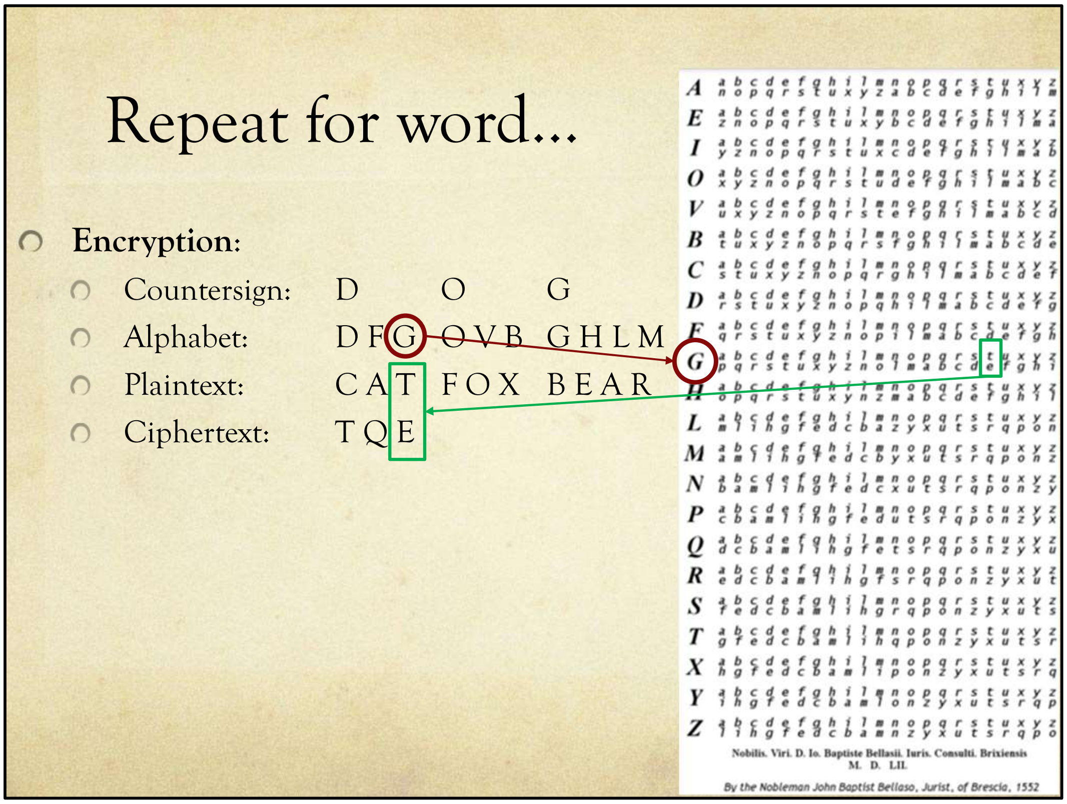
Next Alphabet & Letter

- **Encryption:**
  - Countersign: D O G
  - Alphabet: D F G O V B G H L M
  - Plaintext: C A T F O X B E A R
  - Ciphertext: T Q

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

Nobilis. Viri. D. Io. Baptiste Bellasii. Iuris. Consulti. Brixiensis
M. D. LII.

By the Nobleman John Baptist Bellaso, Jurist, of Brescia, 1552



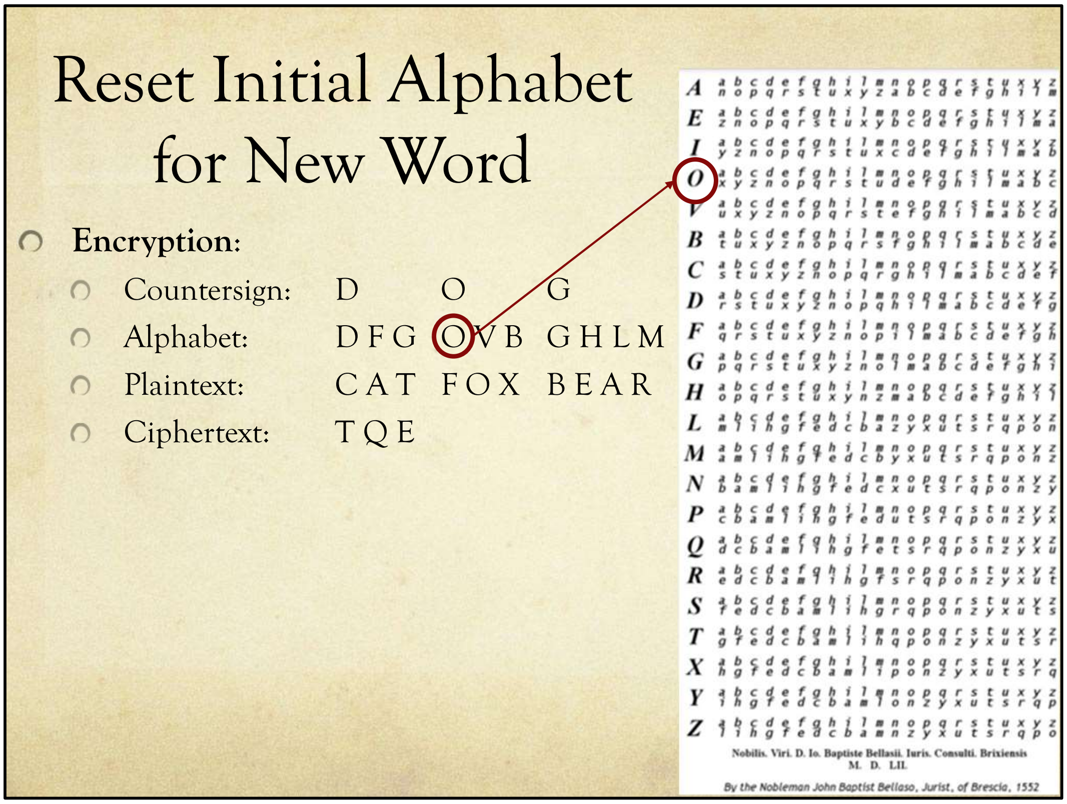
Repeat for word…

- **Encryption:**
  - Countersign: D O G
  - Alphabet: D F G O V B G H L M
  - Plaintext: C A T F O X B E A R
  - Ciphertext: T Q E

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

Nobilis. Viri. D. Io. Baptiste Bellasii. Iuris. Consulti. Brixiensis
M. D. LII.

By the Nobleman John Baptist Bellaso, Jurist, of Brescia, 1552



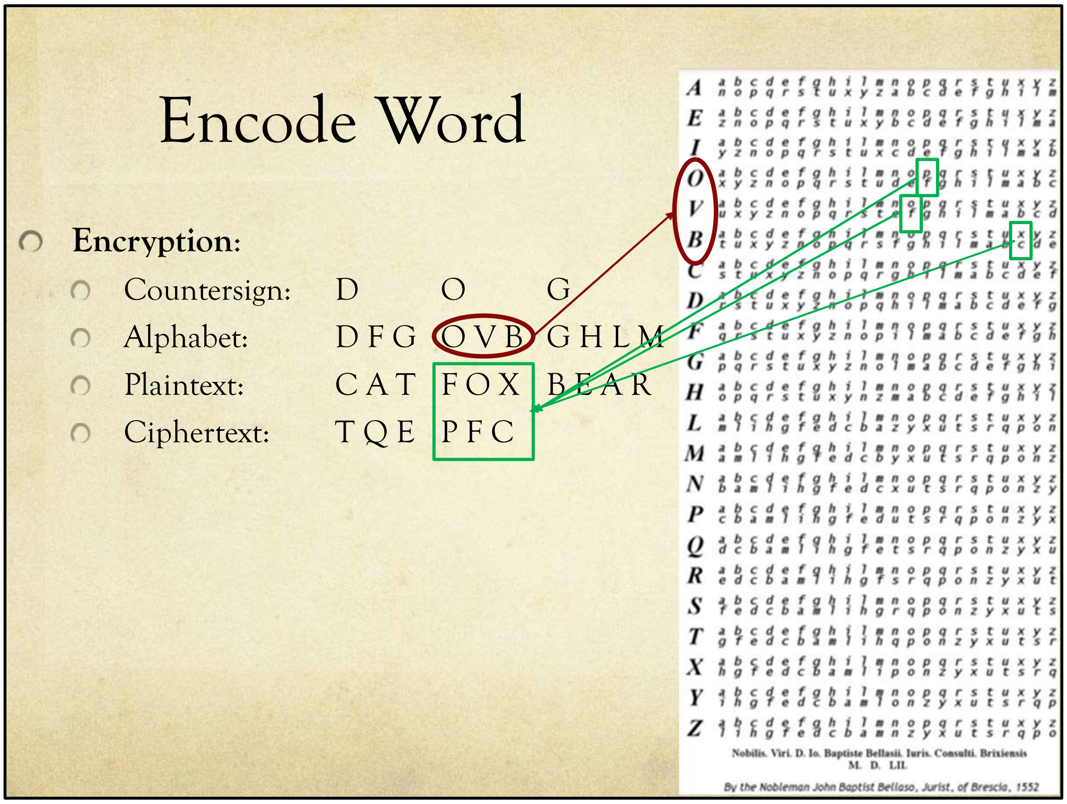
Reset Initial Alphabet for New Word

- **Encryption:**
  - Countersign: D O G
  - Alphabet: DFG OVB GHLM
  - Plaintext: CAT FOX BEAR
  - Ciphertext: TQE

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

Nobilis. Viri. D. Io. Baptiste Bellasii. Iuris. Consulti. Brixiensis
M. D. LII.

By the Nobleman John Baptist Bellaso, Jurist, of Brescia, 1552



Encode Word

- **Encryption:**
  - Countersign: D O G
  - Alphabet: D F G OVB GHLM
  - Plaintext: C A T F O X B E A R
  - Ciphertext: T Q E P F C

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

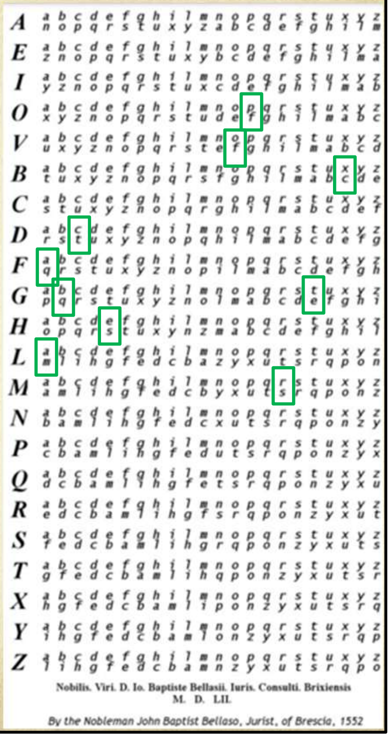
Nobilis. Viri. D. Io. Baptiste Bellasii. Iuris. Consulti. Brixiensis
M. D. LII.

By the Nobleman John Baptist Bellaso, Jurist, of Brescia, 1552

Repeat for all words

- **Encryption:**

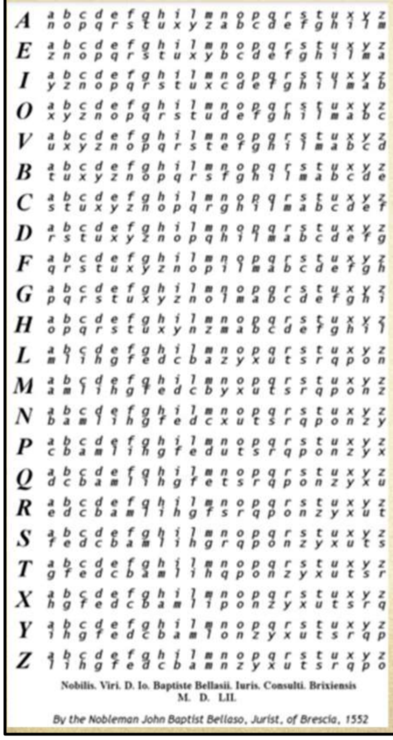
Countersign:	D	O	G
Alphabet:	D F G	O V B	G H L M
Plaintext:	C A T	F O X	B E A R
Ciphertext:	**T Q E**	**P F C**	**Q S M S**



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

Nobilis. Viri. D. Io. Baptiste Bellasii. Iuris. Consulti. Brixiensis
M. D. LII.

By the Nobleman John Baptist Bellaso, Jurist, of Brescia, 1552



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

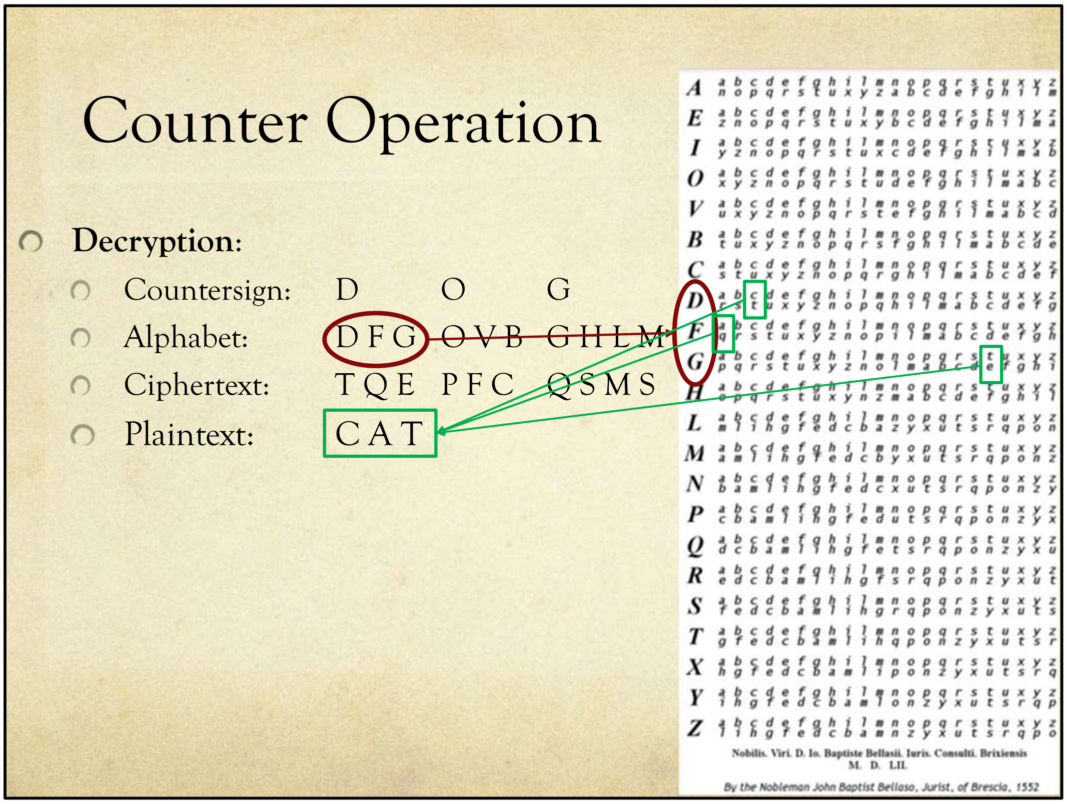
Nobilis. Viri. D. Io. Baptiste Bellasii. Iuris. Consulti. Brixiensis
M. D. LII.

By the Nobleman John Baptist Bellaso, Jurist, of Brescia, 1552

Process Overview

- **Decryption:**

Countersign:	D	O	G
Alphabets:	D F G	O V B	G H L M
Ciphertext:	T Q E	P F C	Q S M S
Plaintext:	C A T	F O X	B E A R



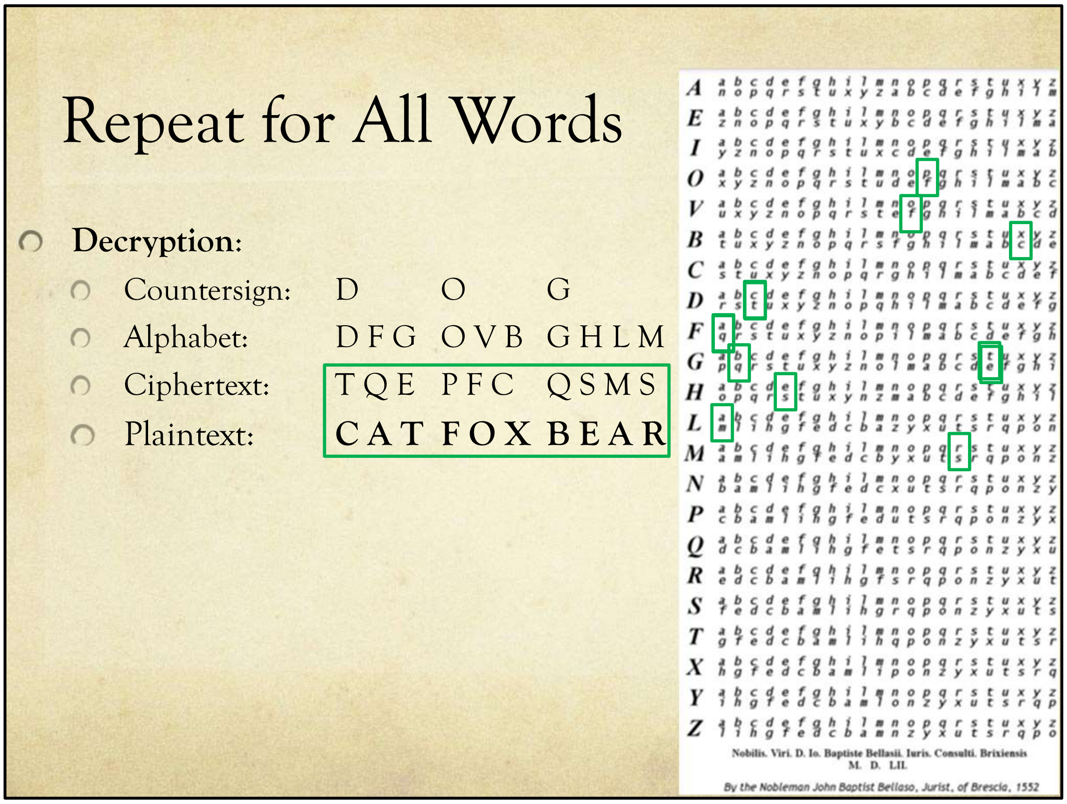
Counter Operation

- **Decryption:**
  - Countersign: D O G
  - Alphabet: D F G OVB GHLM
  - Ciphertext: T Q E P F C Q S M S
  - Plaintext: C A T

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

Nobilis. Viri. D. Io. Baptiste Bellasii. Iuris. Consulti. Brixiensis
M. D. LII.

By the Nobleman John Baptist Bellaso, Jurist, of Brescia, 1552



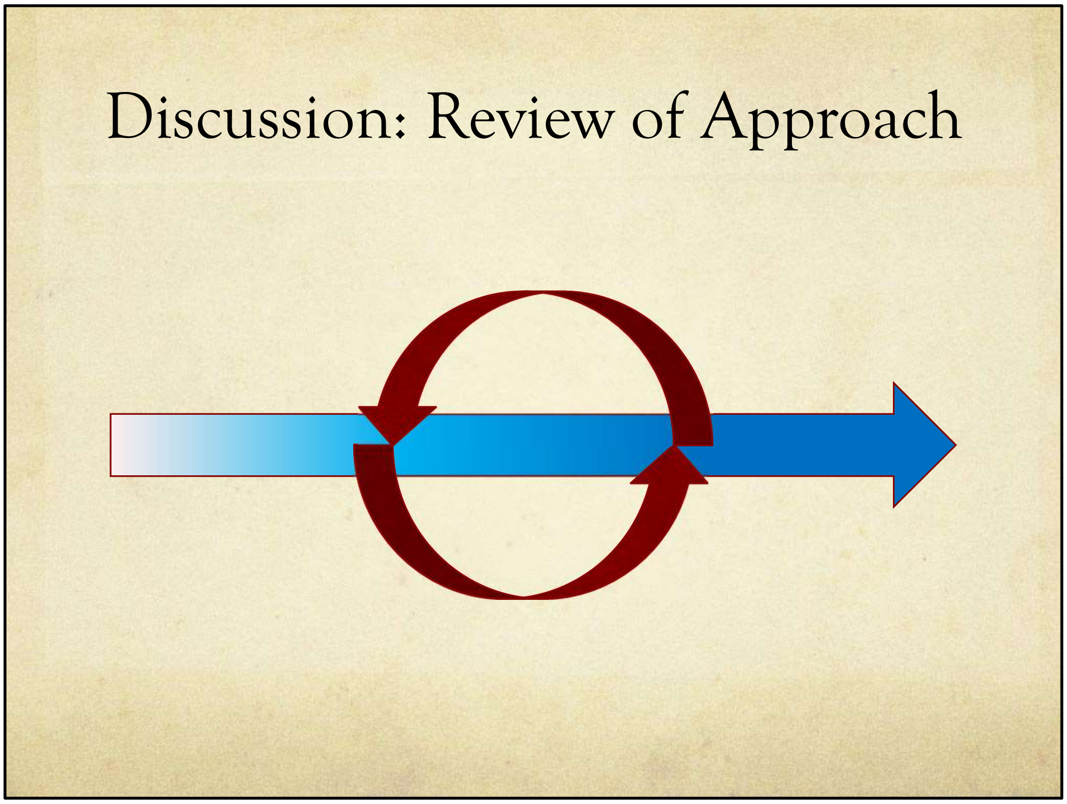
Repeat for All Words

- **Decryption:**
  - Countersign: D O G
  - Alphabet: DFG OVB GHLM
  - Ciphertext: TQE PFC QSMS
  - Plaintext: **CAT FOX BEAR**

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

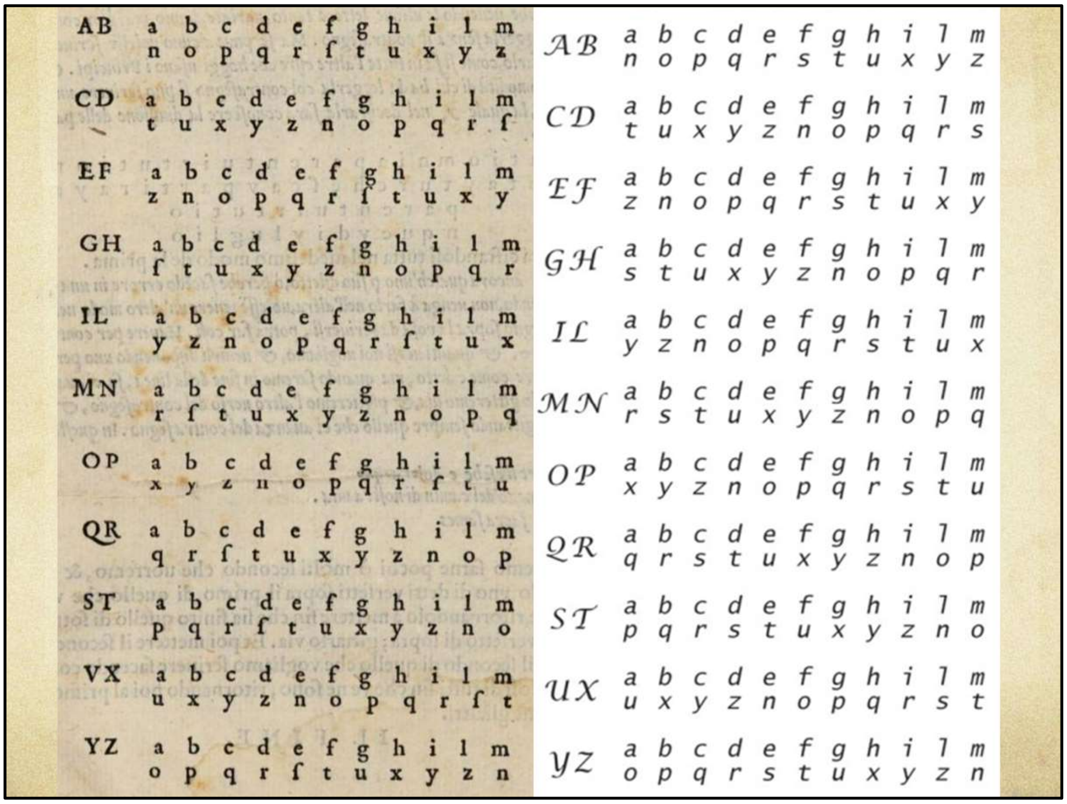
Nobilis. Viri. D. Io. Baptiste Bellasii. Iuris. Consulti. Brixiensis
M. D. LII.

By the Nobleman John Baptist Bellaso, Jurist, of Brescia, 1552



Discussion: Review of Approach

This slide is intentionally blank to allow for discussion and answering any questions before we move on to the next section.



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

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
UX	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

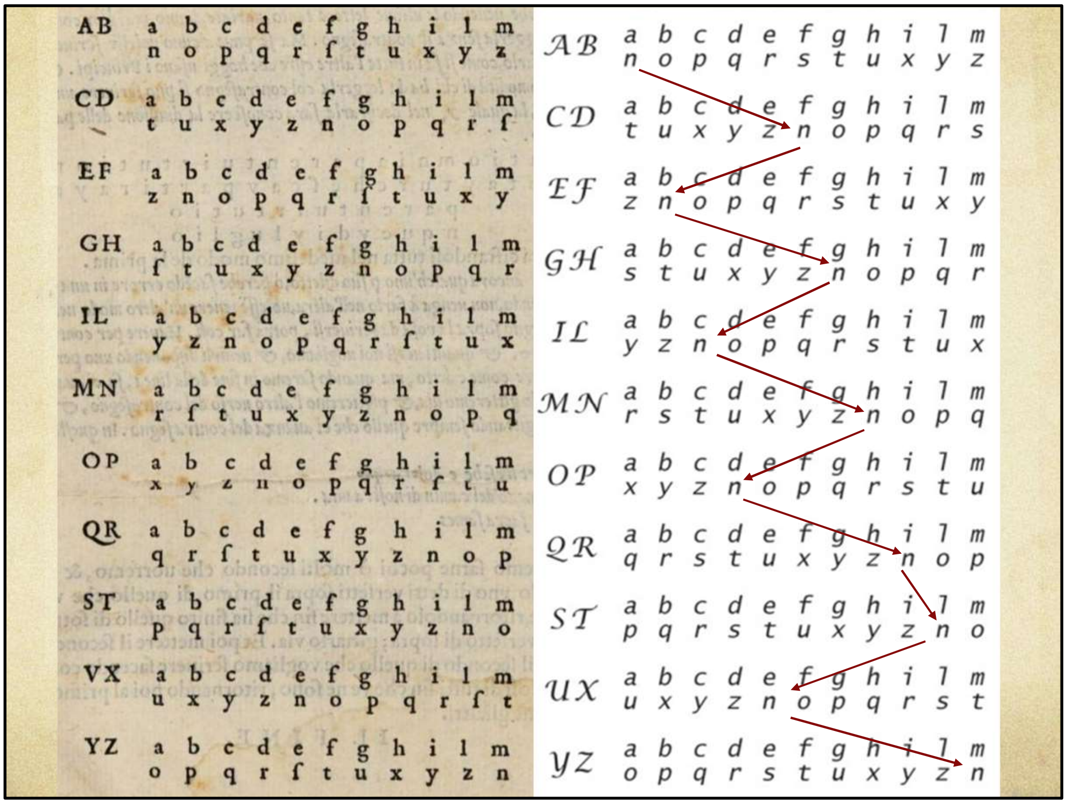
Here we see Bellaso's cipher from 1553s La cifra reduced to a total of 11 (half) and the alphabet for the key is placed into natural order. Also notice that the rather than 11 full substitution sets we see each alphabet split with the first half retaining natural order and the second half employing an inconsistent rotational mechanism. We'll take a closer look at that on the next page. This basic modification aside, the cipher operates in the same fundamental manner as that of the 1552 leaflet. That is, the letter pair to the left is used by the countersign to identify, index to, alphabet it pairs to which is used to perform the enciphering. For example, using the AB reciprocal alphabet A=N and N=A, and so on. This cipher uses the same progressive index for characters within a word with the next sequential character is used as the starting index for the following word, and so on.

References

Bellaso, G. B. (1553) La cifra … nuouamente da lui ridotta a grandissima breuita e perfettione. Venezia, VE.

Bonavoglia, P. (2019) Bellaso's 1552 cipher recovered in Venice, Cryptologia, 43:6, 459-465, DOI: 10.1080/01611194.2019.1596181

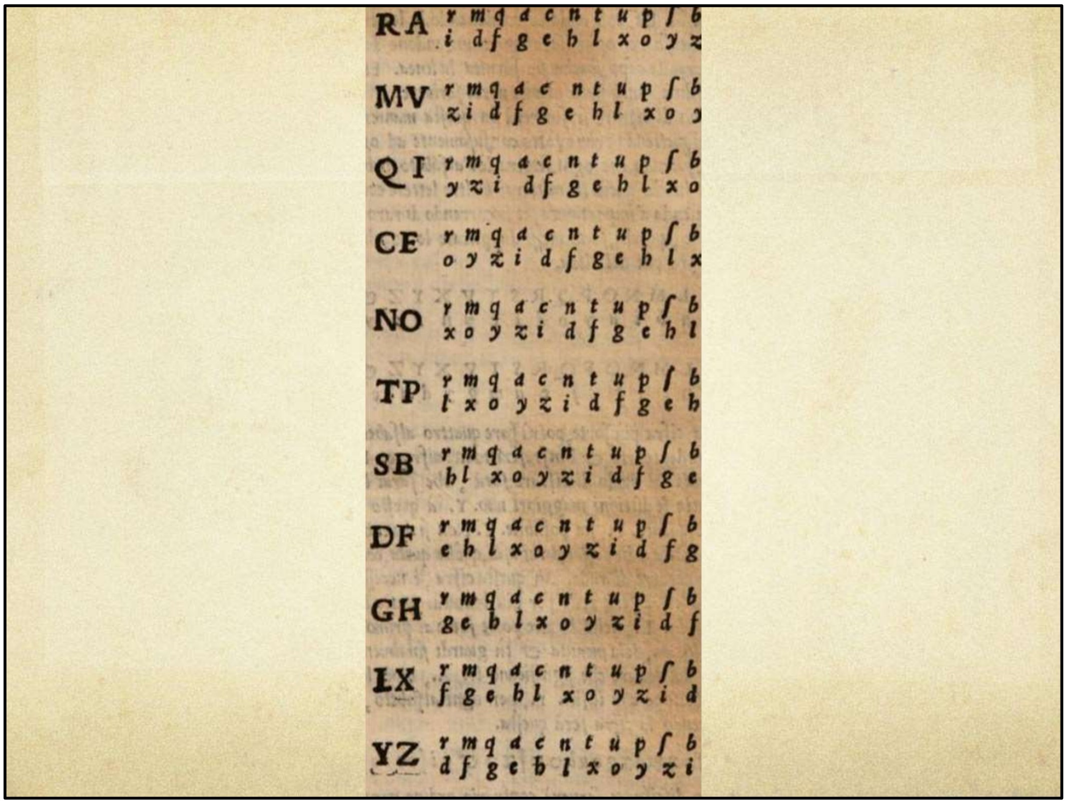
Google Books: Retrieved 25 Feb 2022: https://play.google.com/books/reader?id=GbZRAAAAcAAJ&pg=GBS.PP16



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

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
UX	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

DESCRIPTION

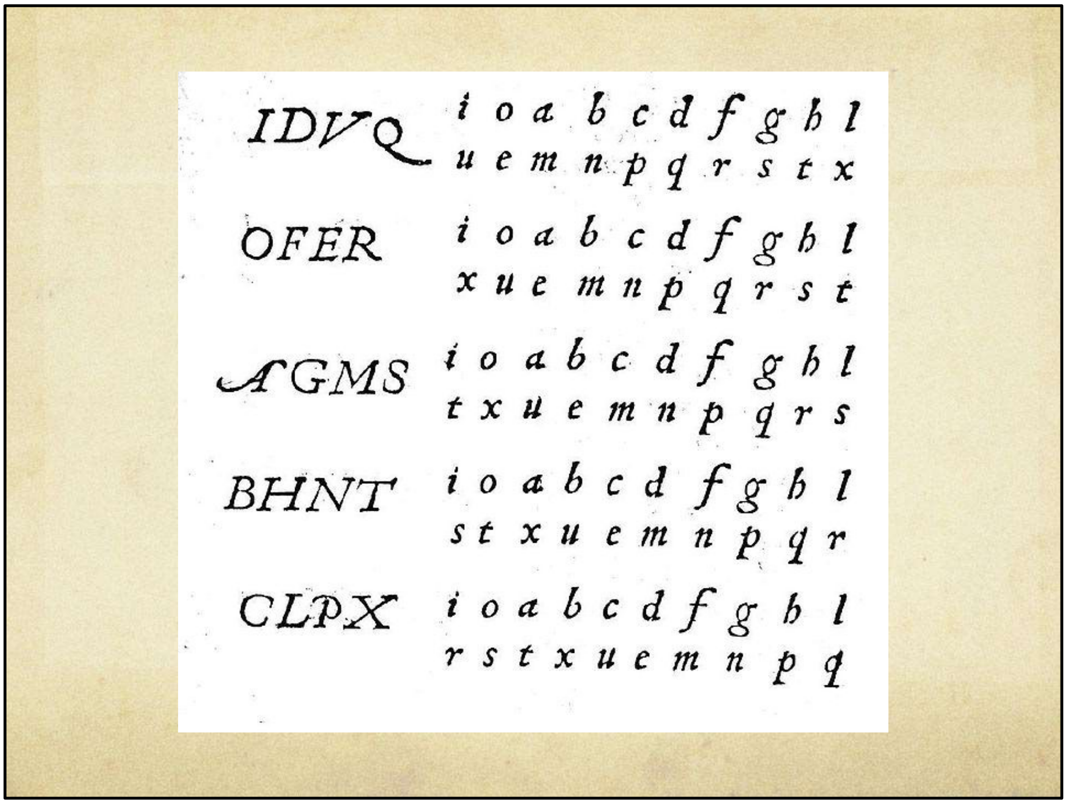


RA	r	m	q	d	c	n	t	u	p	ſ	b
	i	d	f	g	e	h	l	x	o	y	z
MV	r	m	q	d	c	n	t	u	p	ſ	b
	z	i	d	f	g	e	h	l	x	o	y
QI	r	m	q	d	c	n	t	u	p	ſ	b
	y	z	i	d	f	g	e	h	l	x	o
CE	r	m	q	d	c	n	t	u	p	ſ	b
	o	y	z	i	d	f	g	e	h	l	x
NO	r	m	q	d	c	n	t	u	p	ſ	b
	x	o	y	z	i	d	f	g	e	h	l
TP	r	m	q	d	c	n	t	u	p	ſ	b
	l	x	o	y	z	i	d	f	g	e	h
SB	r	m	q	d	c	n	t	u	p	ſ	b
	h	l	x	o	y	z	i	d	f	g	e
DF	r	m	q	d	c	n	t	u	p	ſ	b
	e	h	l	x	o	y	z	i	d	f	g
GH	r	m	q	d	c	n	t	u	p	ſ	b
	g	e	h	l	x	o	y	z	i	d	f
LX	r	m	q	d	c	n	t	u	p	ſ	b
	f	g	e	h	l	x	o	y	z	i	d
YZ	r	m	q	d	c	n	t	u	p	ſ	b
	d	f	g	e	h	l	x	o	y	z	i

In 1555s Noui et singulari modi di cifrare Bellaso takes the previous reciprocal cipher a step further by introcucing seeming randomization into the order of the alphabet indexes. Notice, however, that each cipher continues to utilize the same alphabet (rmqdcntupsb) for the first half of the cipher. This is consistent with what we have seen from the previous ciphers. Also notice that the initial sequence 'rmq' is seen in the first index letters, on the left, 'rmq'. Interestingly you will notice the the indexs jump over the 'd' and then continues on with 'cnt'. You will also notice that the keyword/countersign alphabets have been similarly modified. For example R is now paired with A, and so on.

References

Bellaso, G. B. (1555) Noui et singulari modi di cifrare … . Brescia, BS: Lodovico Britannico
Biermann, N. (2018) Analysis of Giouan Battista Bellaso's cipher challenges of 1555, Cryptologia, 42:5, 381-407, DOI: 10.1080/01611194.2017.1422050hl=en
Bonavoglia , P. (2019) Bellaso's 1552 cipher recovered in Venice, Cryptologia, 43:6, 459-465, DOI: 10.1080/01611194.2019.1596181
Google Books: Retrieved 25 Feb 2022: https://play.google.com/books/reader?id=Gw5mAAAAcAAJ&pg=GBS.PP2&
Buonafalce, A. (2006) Bellaso's Reciprocal Ciphers, Cryptologia, 30:1, 39-51, DOI: 10.1080/01611190500383581



IDVQ	i	o	a	b	c	d	f	g	h	l
	u	e	m	n	p	q	r	s	t	x
OFER	i	o	a	b	c	d	f	g	h	l
	x	u	e	m	n	p	q	r	s	t
AGMS	i	o	a	b	c	d	f	g	h	l
	t	x	u	e	m	n	p	q	r	s
BHNT	i	o	a	b	c	d	f	g	h	l
	s	t	x	u	e	m	n	p	q	r
CLPX	i	o	a	b	c	d	f	g	h	l
	r	s	t	x	u	e	m	n	p	q

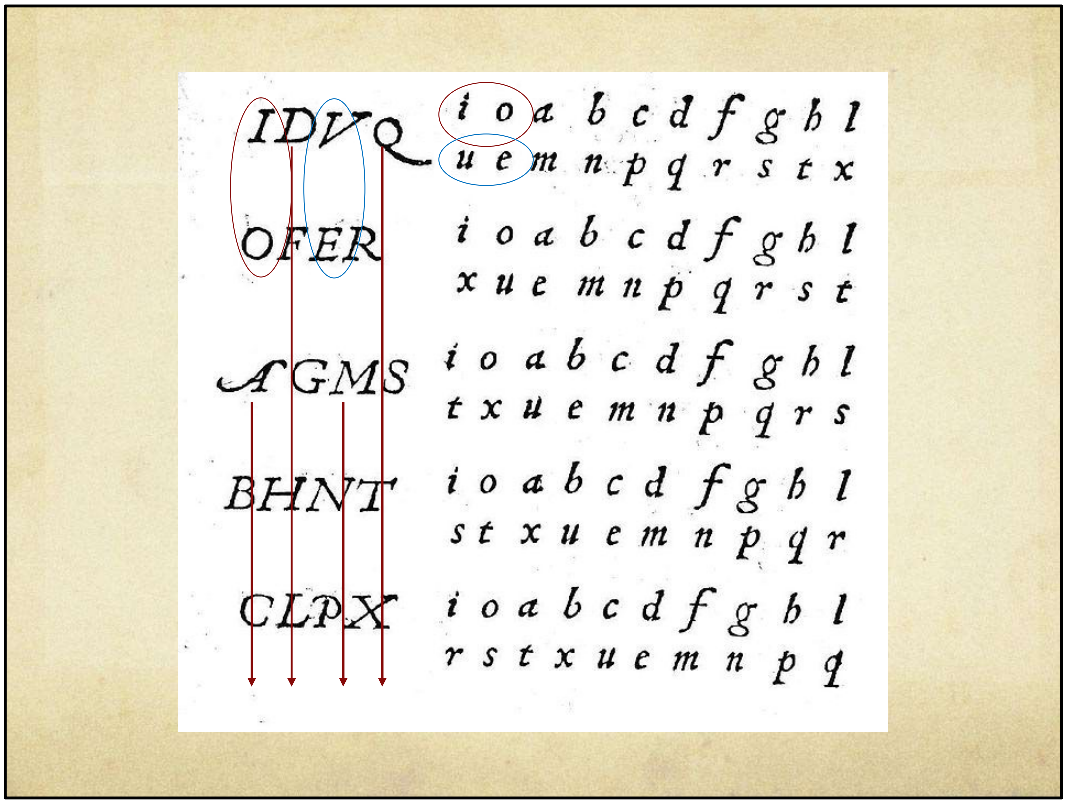
In 1564s Il uero modo di scriuere… we see a further reduction of the number of ciphers to 5 and the cipher alphabets to a total of 20 total characters, rather than 22. You will note the omission of the Y and Z from the alphabet sets. Again, the same mechanism is used for the purpose of encipher and decipher operations. It is also of interest that the key (IOVE) is used to prime the alphabets. Bellaso describes the construction as follows:

“If repeated letters exist in the keyword they are discarded. The first syllable of the keyword is placed in the top half and the rest of the keyword in the bottom half, followed by the unused letters in alphabetical sequence.”
“we do not include Y or Z because they rarely occur. If necessary they will be put in the cipher text.”
“the X has no other function than to mark the end of the words. When needed as a plaintext letter one dot may be put over the cyphertext letter to indicate x.”

ioabcdfghl
uemnpqrstx
x**ue**mnpqrst
…

References

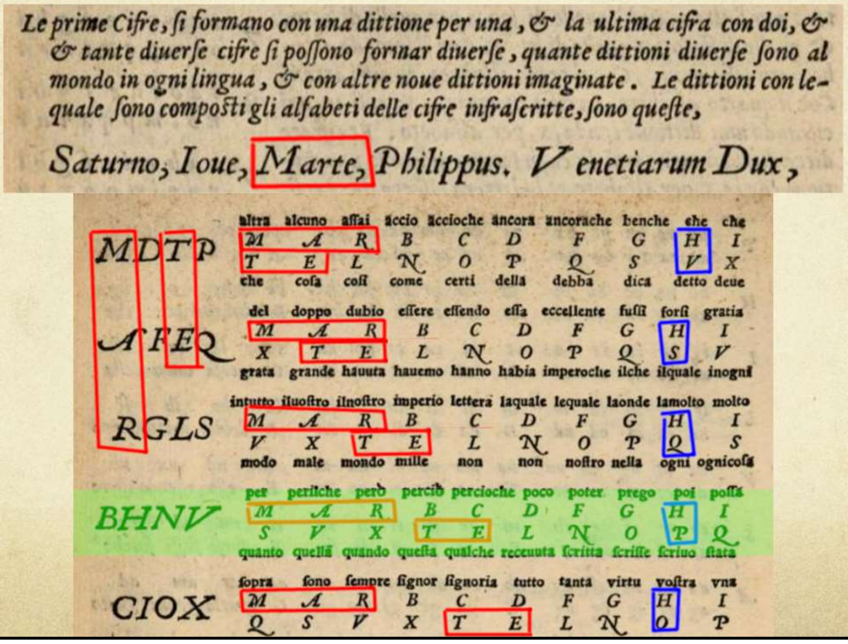
Bellaso, G. B. (1564) Il uero modo di scriuere in cifra, con facilita, prestezza et securezza. Brescia, BS: Iacobo Britannico.
Bonavoglia, P. (2019) Bellaso’s 1552 cipher recovered in Venice, Cryptologia, 43:6, 459-465, DOI: 10.1080/01611194.2019.1596181
Wikipedia: Retrieved 25 Feb 2022: https://commons.wikimedia.org/wiki/File:Bellaso_reciprocal_table_IOVE_1564.JPG
Wikipedia: Retrieved 25 Feb 2022: https://en.wikipedia.org/wiki/Giovan_Battista_Bellaso



IDVQ	i	o	a	b	c	d	f	g	h	l
	u	e	m	n	p	q	r	s	t	x
OFER	i	o	a	b	c	d	f	g	h	l
	x	u	e	m	n	p	q	r	s	t
AGMS	i	o	a	b	c	d	f	g	h	l
	t	x	u	e	m	n	p	q	r	s
BHNT	i	o	a	b	c	d	f	g	h	l
	s	t	x	u	e	m	n	p	q	r
CLPX	i	o	a	b	c	d	f	g	h	l
	r	s	t	x	u	e	m	n	p	q

Here we're just showing how the countersign is used to prime each alphabet. We'll take a look at another example from the period material on the next slide but this is a nicely simplified example.

Keywords in play



Le prime Cifre, ſi formano con una dittione per una, & la ultima cifra con doi, & & tante diuerſe cifre ſi poſſono formar diuerſe, quante dittioni diuerſe ſono al mondo in ogni lingua, & con altre noue dittioni imaginate. Le dittioni con lequale ſono compoſti gli alfabeti delle cifre infraſcritte, ſono queſte,

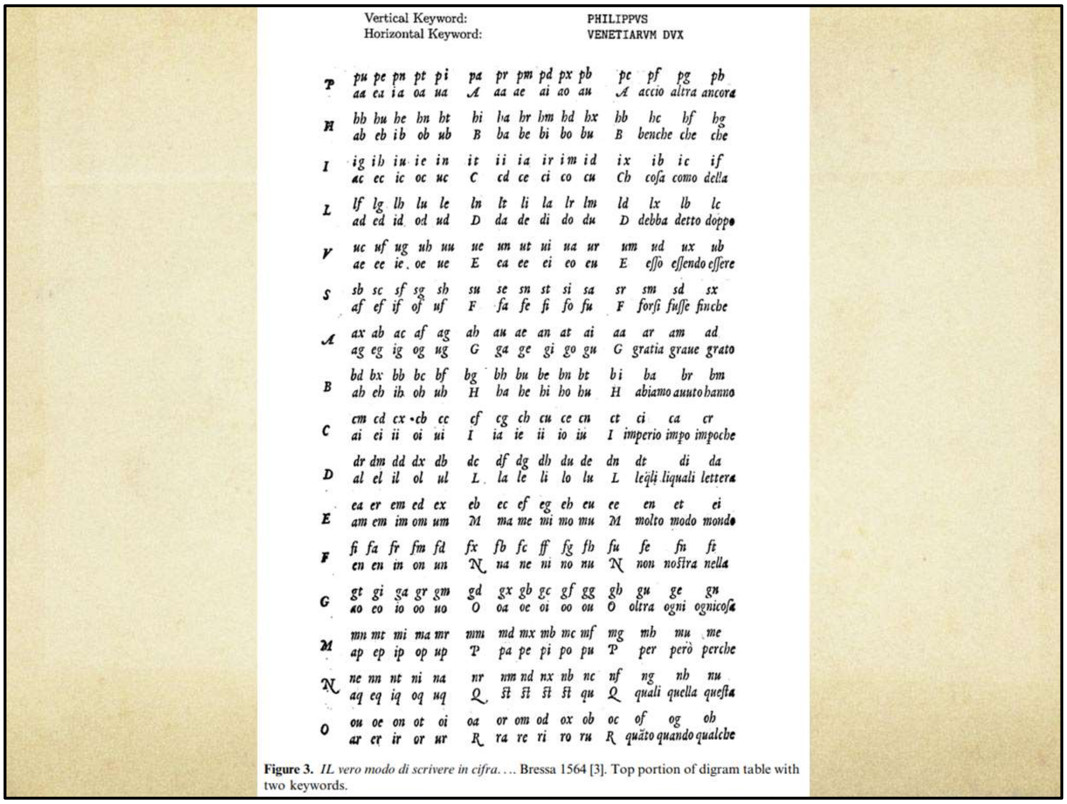
Saturno, Ioue, Marte, Philippus. Venetiarum Dux,

	altra	alcuno	aſſai	accio	accioche	ancora	ancorache	benche	che	che
MDTP	M	A	R	B	C	D	F	G	H	I
	T	E	L	N	O	P	Q	S	V	X
	che	coſa	coſi	come	certi	della	debba	dica	detto	deue
	del	doppo	dubio	eſſere	eſſendo	eſſa	eccellente	fuſſi	forſi	gratia
AFEQ	M	A	R	B	C	D	F	G	H	I
	X	T	E	L	N	O	P	Q	S	V
	grata	grande	hauuta	hauemo	hanno	habia	imperoche	ilche	ilquale	inogni
	intutto	iluoſtro	ilnoſtro	imperio	lettera	laquale	lequale	laonde	lamolto	molto
RGLS	M	A	R	B	C	D	F	G	H	I
	V	X	T	E	L	N	O	P	Q	S
	modo	male	mondo	mille	non	non	noſtro	nella	ogni	ognicoſa
	per	perilche	però	perciò	percioche	poco	poter	prego	poi	poſſa
BHNV	M	A	R	B	C	D	F	G	H	I
	S	V	X	T	E	L	N	O	P	Q
	quanto	quella	quando	queſta	qualche	receuuta	ſcritta	ſcriſſe	ſcriuo	ſtata
	ſopra	ſono	ſempre	ſignor	ſignoria	tutto	tanta	virtu	voſtra	vna
CIOX	M	A	R	B	C	D	F	G	H	I
	Q	S	V	X	T	E	L	N	O	P

Here we see how the keys and alphabets are primed in a bit more detail. On page 5 of the 1564 text (top image) Bellaso presents five keywords (not countersigns) to be used in later examples in the text. The lower, annotated, example is taken from page 11 and uses the 'Marte' keyword. Again, remember that the letters Y & Z have been removed from the alphabet bringing the total length down to 20. To do this our alphabet is split into 5 ciphers each with 4 indexes (nicely rounding out to the alphabet space of 20). The first thing we need to do is construct our alphabet indexes. To begin, we will use the first syllable of the keyword to create the beginning of the index. The first column, as you see, contains that first syllable and the remainder of the column, and the next, is populated with the next successive characters, excepting those that are used in the countersign itself. The remainder of the word, omitting any duplicate characters, begins in the third column and once completed the alphabet continues in order from where it left off. Priming the first cipher alphabets works in a similar fashion. Each of the following cipher rotates the bottom alphabet one position to the right, as it shown. I have marked the letter H pair to make it clear that the alphabets are not changing but simply rotating. Once constructed you use the countersign as described.

References

Bellaso, G. B. (1564) Il uero modo di scriuere in cifra, con facilita, prestezza et securezza. Brescia, BS: Iacobo Britannico.
Google Books: Retrieved 25 Feb 2022: https://play.google.com/books/reader?id=dqNNAAAAcAAJ&pg=GBS.PP14



Vertical Keyword: PHILIPPVS
Horizontal Keyword: VENETIARVM DVX

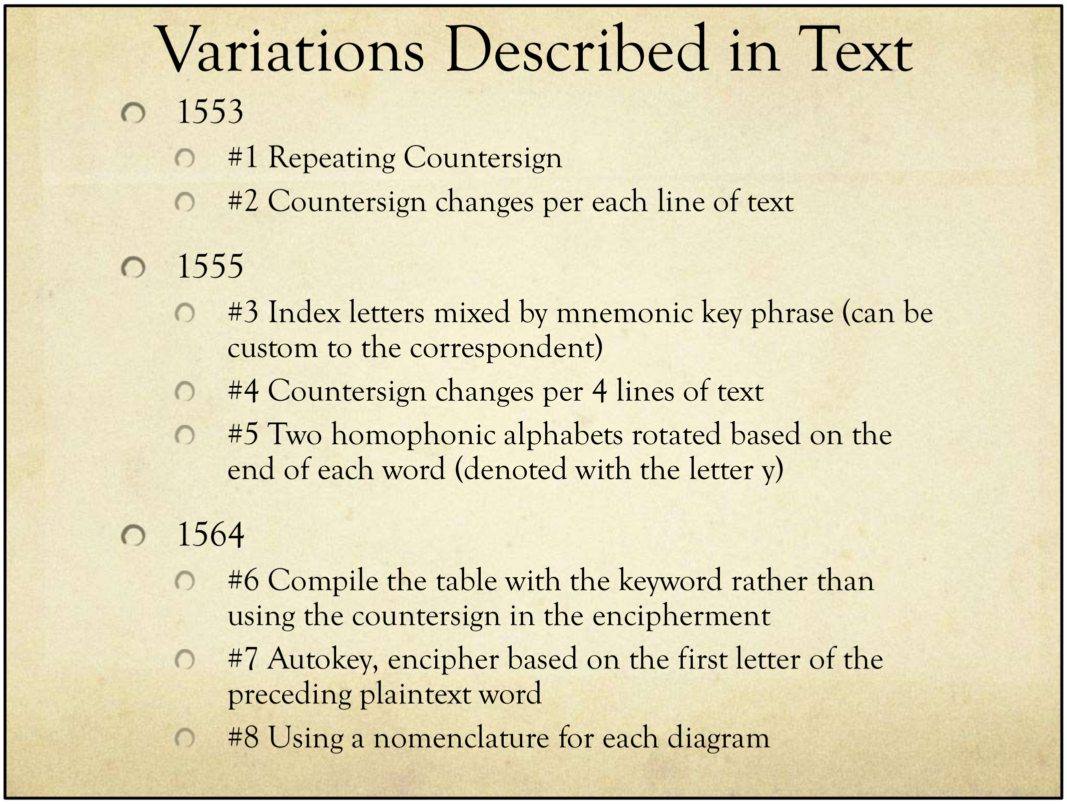
P	pu	pe	pn	pt	pi	pa	pr	pm	pd	px	pb	pc	pf	pg	ph
	aa	ea	ia	oa	ua	A	aa	ae	ai	ao	au	A	accio	altra	ancora
H	hb	hu	he	hn	ht	hi	ha	hr	hm	hd	hx	hh	hc	hf	hg
	ab	eb	ib	ob	ub	B	ba	be	bi	bo	bu	B	benche	che	che
I	ig	ih	iu	ie	in	it	ii	ia	ir	im	id	ix	ib	ic	if
	ac	ec	ic	oc	uc	C	ca	ce	ci	co	cu	Ch	coſa	como	della
L	lf	lg	lh	lu	le	ln	lt	li	la	lr	lm	ld	lx	lb	lc
	ad	ed	id	od	ud	D	da	de	di	do	du	D	debba	detto	doppo
V	uc	uf	ug	uh	uu	ue	un	ut	ui	ua	ur	um	ud	ux	ub
	ae	ee	ie	oe	ue	E	ea	ee	ei	eo	eu	E	eſſo	eſſendo	eſſere
S	sb	sc	sf	sg	sh	su	se	sn	st	si	sa	sr	sm	sd	sx
	af	ef	if	of	uf	F	fa	fe	fi	fo	fu	F	forſi	fuſſe	finche
A	ax	ab	ac	af	ag	ah	au	ae	an	at	ai	aa	ar	am	ad
	ag	eg	ig	og	ug	G	ga	ge	gi	go	gu	G	gratia	graue	grato
B	bd	bx	bb	bc	bf	bg	bh	bu	be	bn	bt	bi	ba	br	bm
	ah	eh	ih	oh	uh	H	ha	he	hi	ho	hu	H	abiamo	auuto	hanno
C	cm	cd	cx	cb	cc	cf	cg	ch	cu	ce	cn	ct	ci	ca	cr
	ai	ei	ii	oi	ui	I	ia	ie	ii	io	iu	I	imperio	impo	impoche
D	dr	dm	dd	dx	db	dc	df	dg	dh	du	de	dn	dt	di	da
	al	el	il	ol	ul	L	la	le	li	lo	lu	L	leq̃li	liquali	lettera
E	ea	er	em	ed	ex	eb	ec	ef	eg	eh	eu	ee	en	et	ei
	am	em	im	om	um	M	ma	me	mi	mo	mu	M	molto	modo	mondo
F	fi	fa	fr	fm	fd	fx	fb	fc	ff	fg	fh	fu	fe	fn	ft
	an	en	in	on	un	N	na	ne	ni	no	nu	N	non	noſtra	nella
G	gt	gi	ga	gr	gm	gd	gx	gb	gc	gf	gg	gh	gu	ge	gn
	ao	eo	io	oo	uo	O	oa	oe	oi	oo	ou	O	oltra	ogni	ognicoſa
M	mn	mt	mi	ma	mr	mm	md	mx	mb	mc	mf	mg	mh	mu	me
	ap	ep	ip	op	up	P	pa	pe	pi	po	pu	P	per	però	perche
N	ne	nn	nt	ni	na	nr	nm	nd	nx	nb	nc	nf	ng	nh	nu
	aq	eq	iq	oq	uq	Q	ſt	ſt	ſt	ſt	qu	Q	quali	quella	queſta
O	ou	oe	on	ot	oi	oa	or	om	od	ox	ob	oc	of	og	oh
	ar	er	ir	or	ur	R	ra	re	ri	ro	ru	R	quãto	quando	qualche

Figure 3. *IL vero modo di scrivere in cifra. . . .* Bressa 1564 [3]. Top portion of digram table with two keywords.

The last cipher we will discuss in this brief introduction is the use of diagrams intermixed with nomenclator. This is a blending of multiple known techniques and those of his own devising. This cipher uses the same basic mechanic of the reciprocal ciphers we've already discussed, namely the polyalphabetic approach which was first described by Albreti in 1467 and the use of a nomenclator, which was known to and described by Trithemius in 1518. A nomenclator cipher, as used by Trithemius, uses lists of words (huge lists, books worth) as substitutions for letters, other words, names, etc. In this case the nomenclator, as seen in the far right column, generally replaces digraphs with words. In this case there are two keys which form an index, horizontal and vertical intersection. This cipher is provided for completeness but we will not be going into further detail as the digraphs add complexities that do not lend themselves to teaching in the little time we have. It is sufficient to see that the core technique of Bellaso's cipher continued to grow in detail and complexity while maintaining the basic operation that we have previously discussed.

References

Bellaso, G. B. (1564) Il uero modo di scriuere in cifra, con facilita, prestezza et securezza. Brescia, BS: Iacobo Britannico.
Buonafalce, A. (2006) Bellaso's Reciprocal Ciphers, Cryptologia, 30:1, 39-51, DOI: 10.1080/01611190500383581



Variations Described in Text

- 1553
  - #1 Repeating Countersign
  - #2 Countersign changes per each line of text
- 1555
  - #3 Index letters mixed by mnemonic key phrase (can be custom to the correspondent)
  - #4 Countersign changes per 4 lines of text
  - #5 Two homophonic alphabets rotated based on the end of each word (denoted with the letter y)
- 1564
  - #6 Compile the table with the keyword rather than using the countersign in the encipherment
  - #7 Autokey, encipher based on the first letter of the preceding plaintext word
  - #8 Using a nomenclature for each diagram

Now that we've covered the basics; here we see the eight variations of the reciprocal ciphers that I have identified in reviewing the literature. One interesting addition to this collection is the autokey cipher. In this approach the first letter of each preceding word indicates the alphabet to be used and each letter of that word would be encrypted using the subsequent alphabets. This is novel approach for the time in that the key is contained in the ciphertext itself. We will touch on this again in a minute.

References

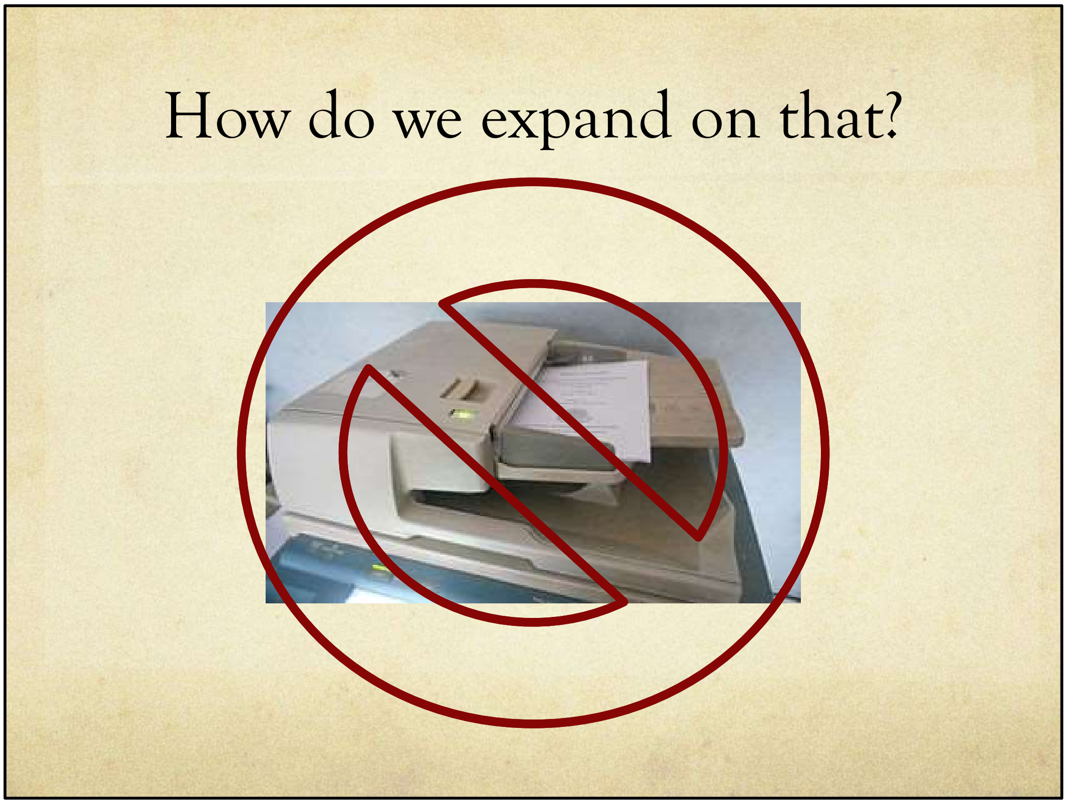
Bellaso, G. B. (1553) La cifra … nuouamente da lui ridotta a grandissima breuita e perfettione. Venezia, VE

Bellaso, G. B. (1555) Noui et singulari modi di cifrare … . Brescia, BS: Lodovico Britannico

Bellaso, G. B. (1564) Il uero modo di scriuere in cifra, con facilita, prestezza et securezza. Brescia, BS: Iacobo Britannico.

Biermann, N. (2018) Analysis of Giouan Battista Bellaso's cipher challenges of 1555, Cryptologia, 42:5, 381-407, DOI: 10.1080/01611194.2017.1422050hl=en

Buonafalce, A. (2006) Bellaso's Reciprocal Ciphers, Cryptologia, 30:1, 39-51, DOI: 10.1080/01611190500383581

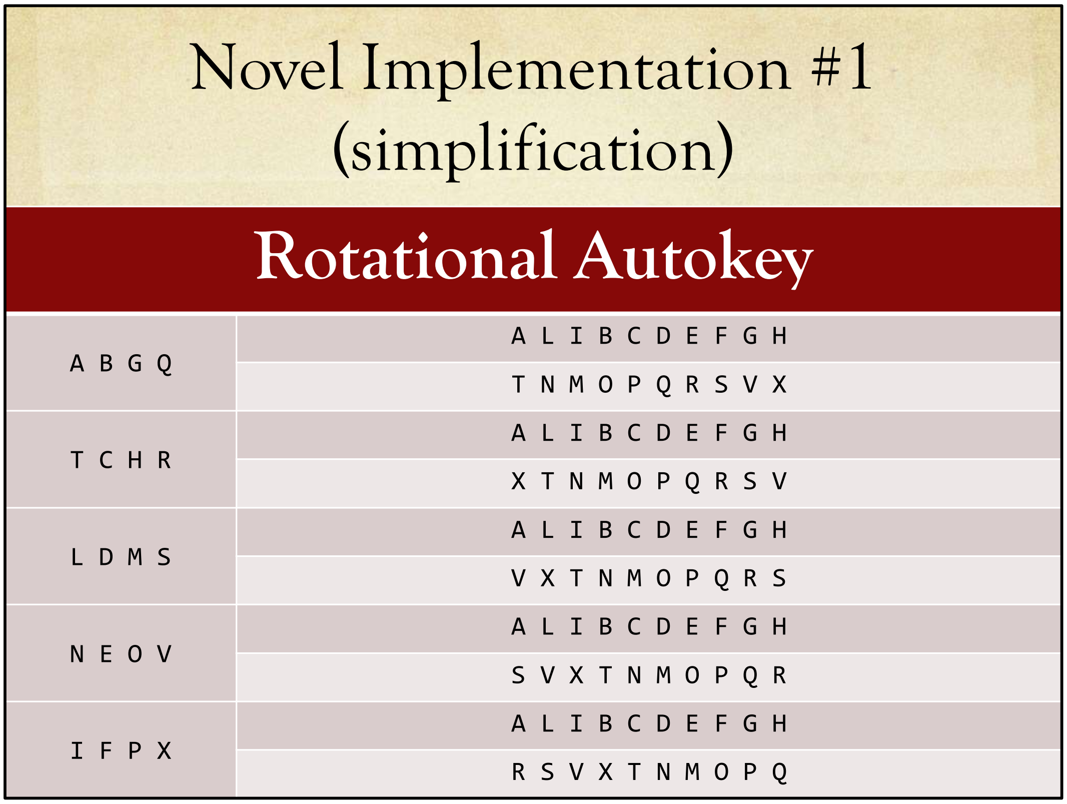


How do we expand on that?

Now that we have a working understanding of Bellaso's reciprocal ciphers we will take a look at some options for creating novel implementations that use those same techniques. There are some obvious options: introducing nulls into the text system, using non-character symbols for the cipher text, changing the direction of the alphabet rotation, changing the rotation offset, swapping the syllable placement, etc. There are countless variations on the theme. In this class we will explore a couple of those options and construct a new 'Bellaso cipher' from the original 'autokey' cipher. So, this is something new made in the period way.

References

Image: https://commons.wikimedia.org/wiki/File:DADF_(Canon_IR6000).JPG



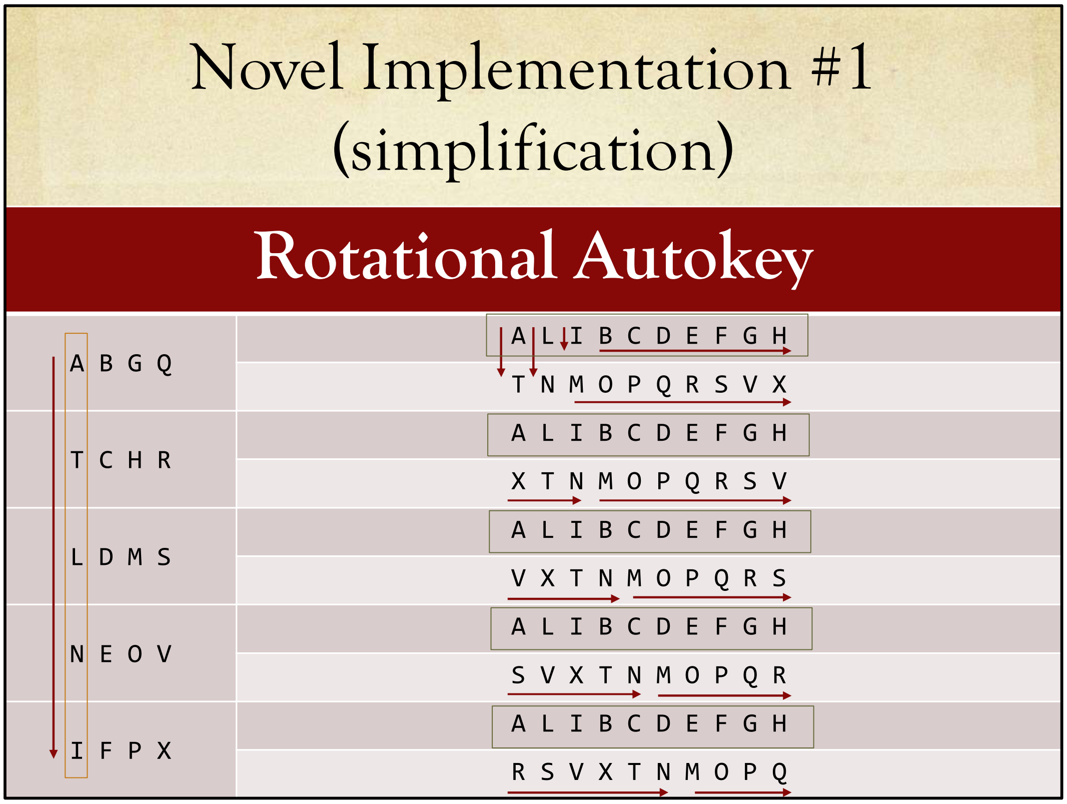
Novel Implementation #1 (simplification)

Rotational Autokey

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

Step 1 is to make some slight variations to the keyword/countersign table that we discussed before

- Same 20 character alphabet.
- Keyword is placed vertically but isn’t split by syllable. More direct to implement.
- Keyword used to prime the table alternated top-bottom instead of left right.
- Keyword is not split by syllables across the rows due to the above.
- Basically we’ve just removed the syllable component for ease of use.
- Still want to use a long keyword as the end of the table will continue to be somewhat normalized

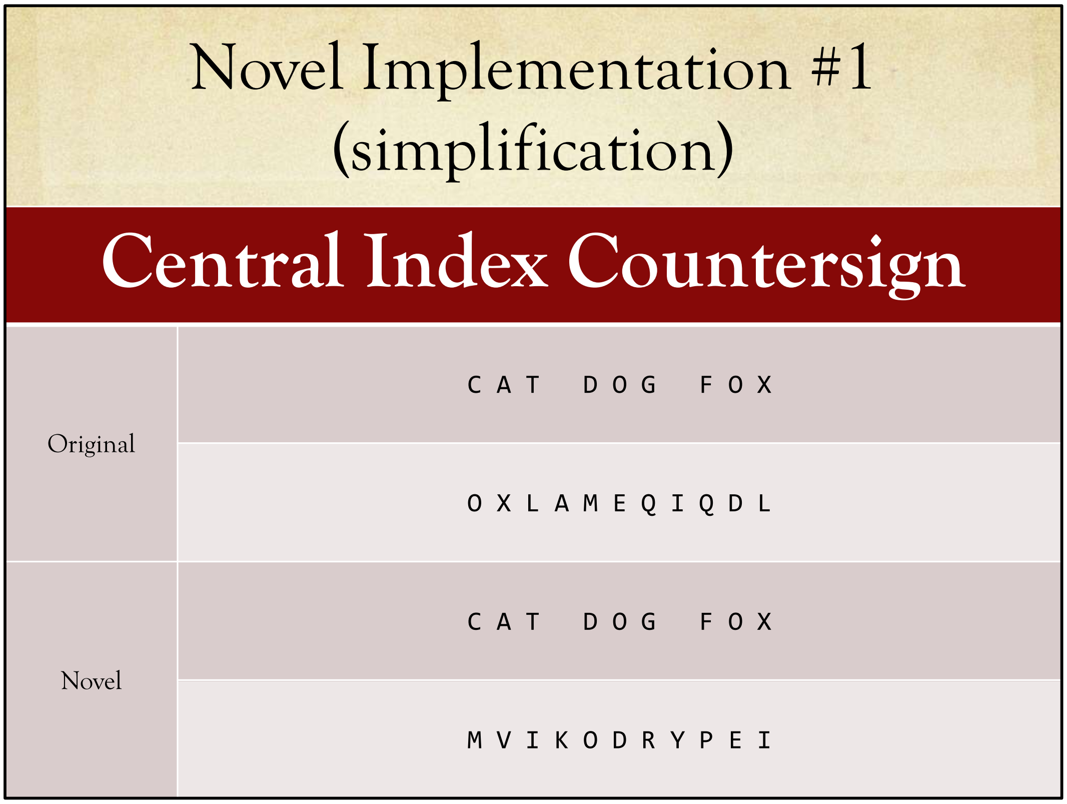


Novel Implementation #1 (simplification)

Rotational Autokey

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

Showing the alphabet and cipher priming using the countersign of “Atlantia”



Novel Implementation #1 (simplification)

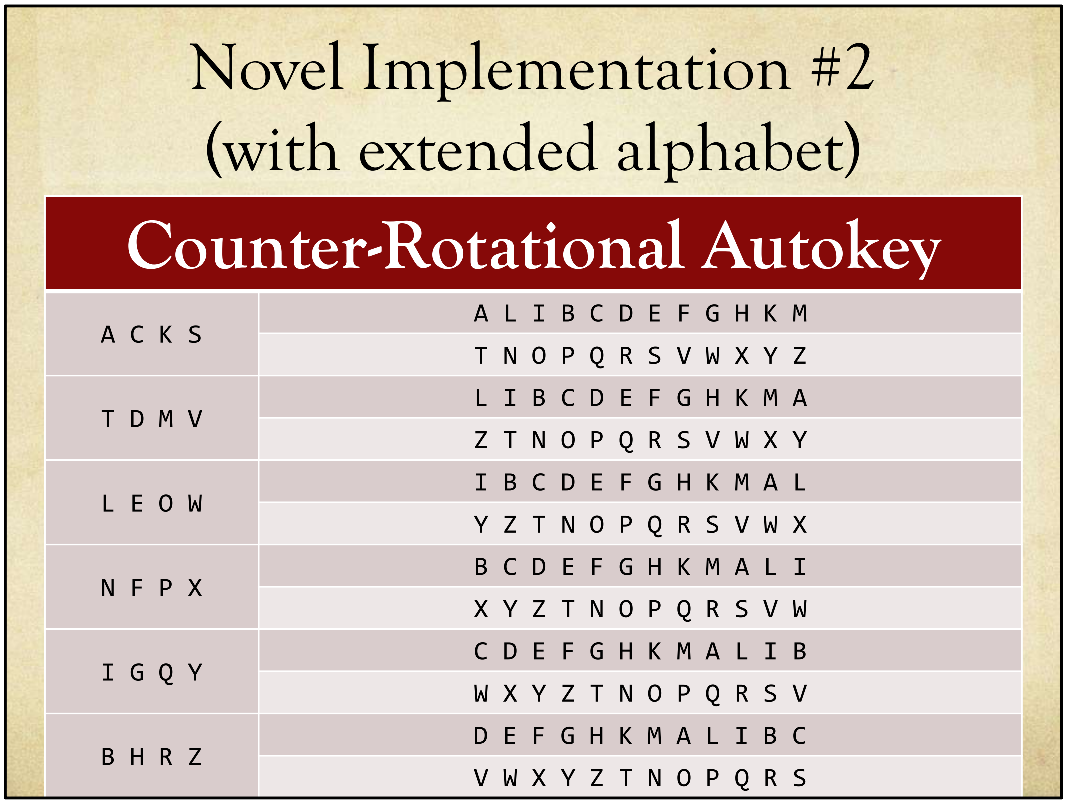
Central Index Countersign

Original	CAT DOG FOX
	OXLAMEQIQDL
Novel	CAT DOG FOX
	MVIKODRYPEI

Step 2 is to modify the 'autokey' methodology itself

- The original always starts using the index of the plaintext letter for the first word and then every word after that uses the first letter of the ciphertext word before it. Words are separated with an enciphered X. 'True' Xs have a dot over the ciphered value.
    - CAT uses the C alphabet
    - DOG uses the O alphabet
    - FOX uses the M alphabet

- For the novel implementation the word's alphabet index will be the 1st letter in the 3nd index row. Instead of splitting words by X we will use an otherwise omitted letter: K, Y, Z. This avoids repeating delimitators. These letters are not enciphered, again, for simplicity.
    - CAT uses the M alphabet
    - DOG uses the M alphabet
    - FOX uses the O alphabet
- For this example comparison we are using the previous table for both the original and the novel implementation.



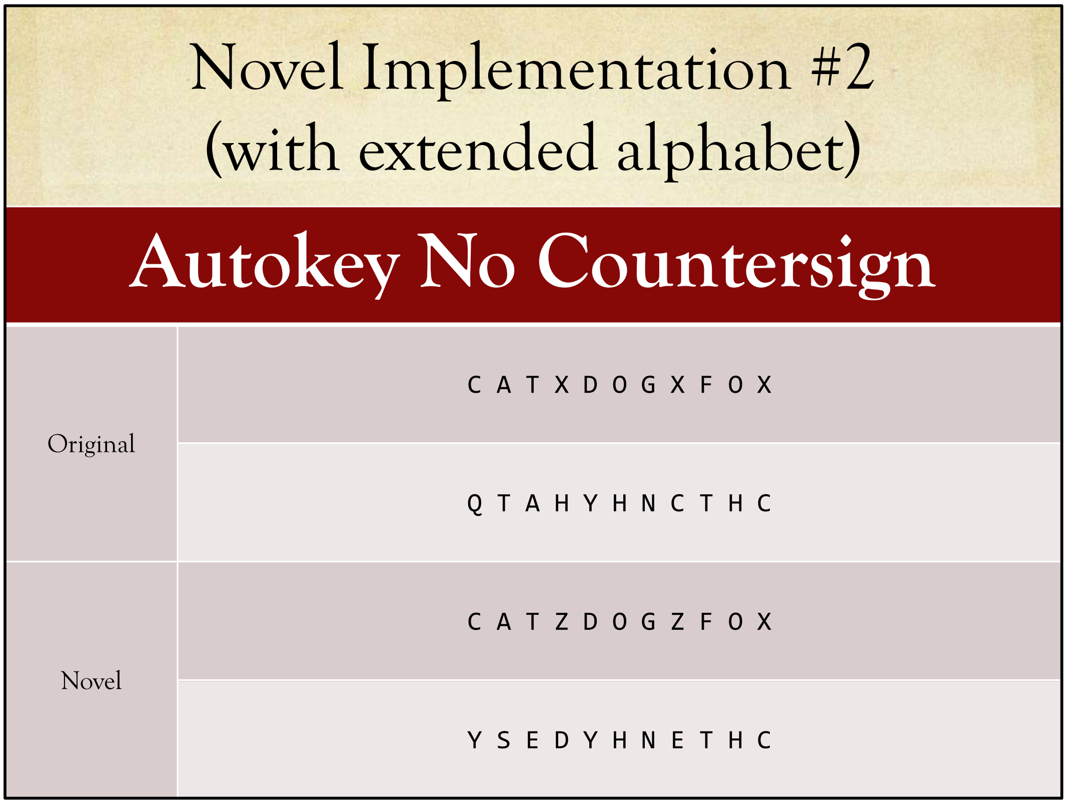
Novel Implementation #2 (with extended alphabet)

Counter-Rotational Autokey

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

Step 1 is to make some slight variations to the keyword/countersign table that we discussed before

- 24 character alphabet with K W Y Z, still missing U and J
- Now both alphabets rotate, top left, bottom right.



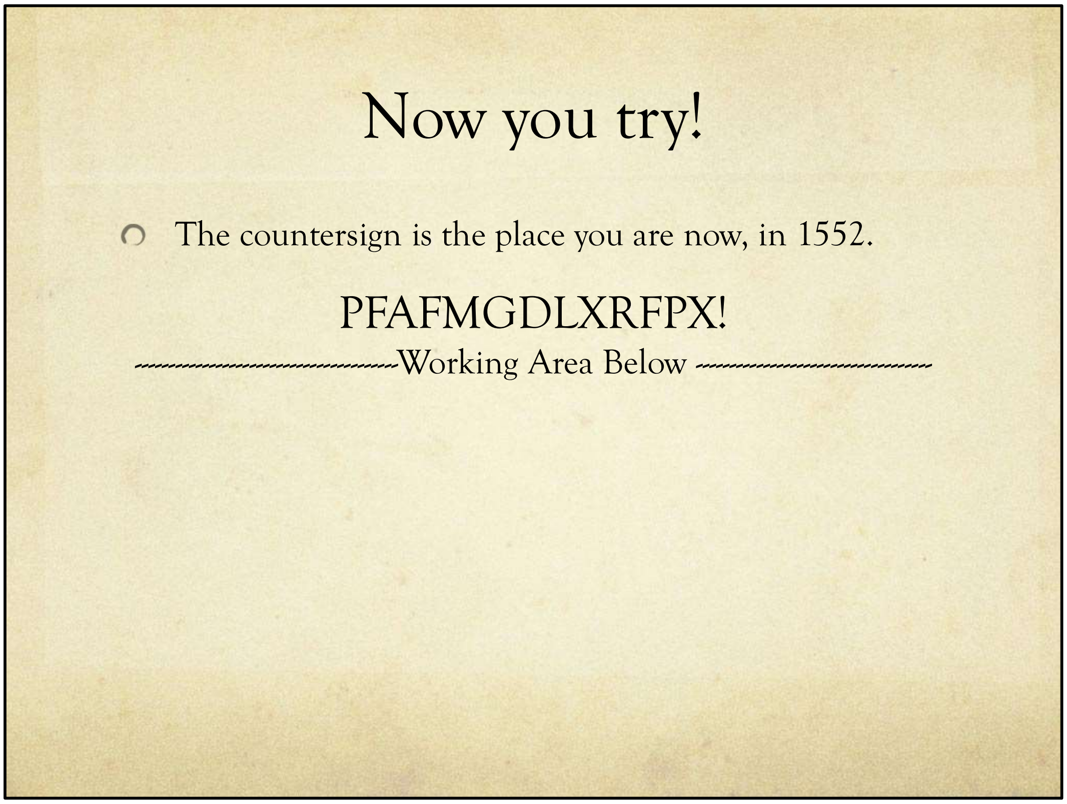
Novel Implementation #2 (with extended alphabet)

Autokey No Countersign

Original	CATXDOGXFOX
	QTAHYHNCTHC
Novel	CATZDOGZFOX
	YSEDYHNETHC

Step 2 is to modify the ‘autokey’ methodology itself

- The original, as before, starts using the index of the plaintext letter for the first word and then every word after that uses the first letter of the word before it. Words are separated with an enciphered X. ‘True’ Xs have a dot over the ciphered value of X.
    - CAT uses the C alphabet
    - DOG uses the Q alphabet
    - FOX uses the Y alphabet
- For the this novel implementation the word’s alphabet index will be the 1st letter the previous word with the first word using the plaintext letter of the last word (as it has not been ciphered yet). Instead of splitting words by X we will use the letter Z as it has the lowest frequency in the English language. This adheres to Bellaso’s approach of using the letter with the lowest available frequency.
    - CAT uses the F alphabet
    - DOG uses the Y alphabet
    - FOX uses the Y alphabet
- This approach has a critical flaw in that there is no way for the recipient to know what the first letter of the last plaintext word is. Still we have made several novel modifications to the period cipher:
    - We’ve changed the way that the keyword constructs the alphabet indexes from split syllables to a continuous vertical progression.
    - We’ve changed the way that the keyword primes the alphabets themselves from split syllables between the two alphabets to being continuously columnar.
    - We’ve introduced counter rotation in the first alphabet.
    - We’ve extended the plaintext alphabet from 20 to 24 to better support modern English.
    - We’ve updated the delimitator letter to be the new lowest frequency letter, Z.

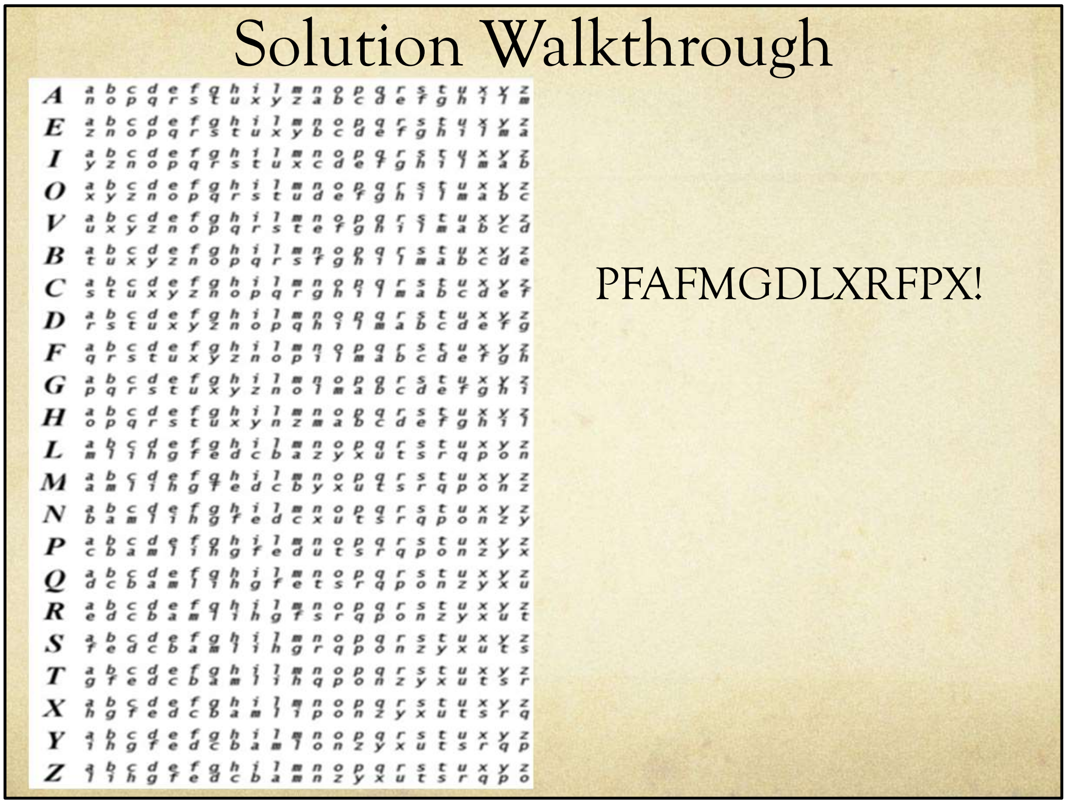


Now you try!

- The countersign is the place you are now, in 1552.

PFAFMGDLXRFPX!

---------------------------------Working Area Below ------------------------------

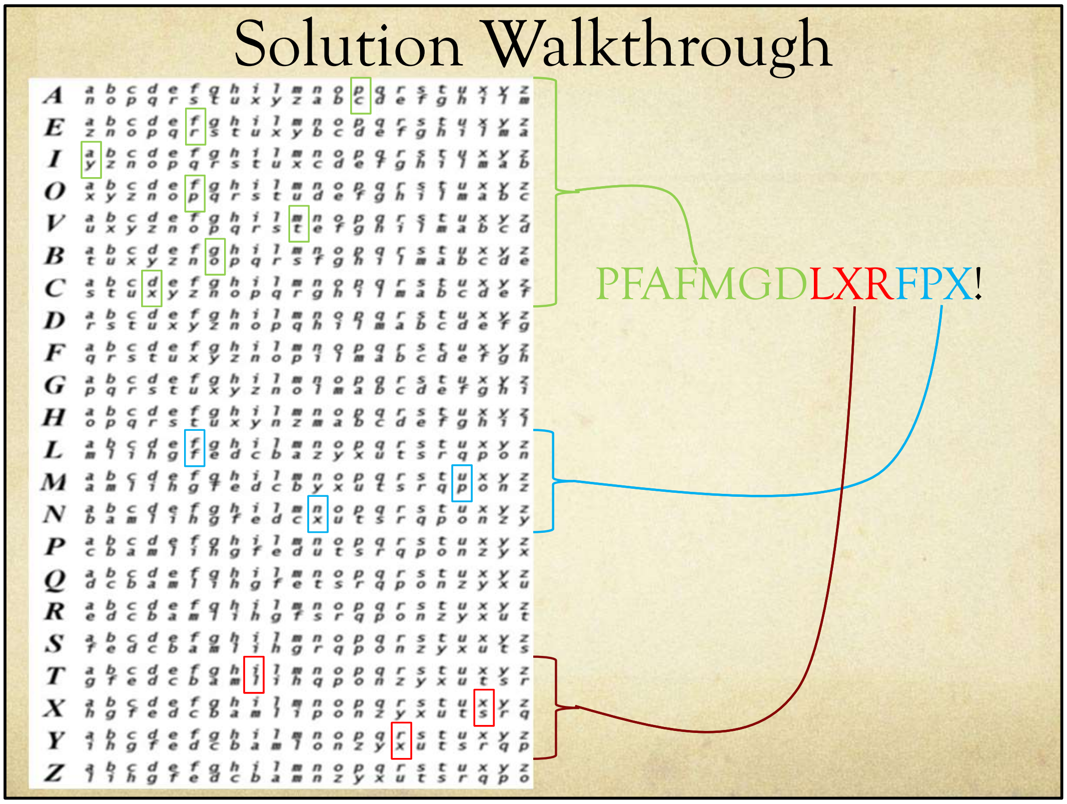


Solution Walkthrough

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

PFAFMGDLXRFPX!

In the previous slide there are two fairly obvious clues. The first of which is down right blatant. The date of 1552 points directly to the cipher to be used, Bellaso's first cipher from 1552. I have chosen to use this cipher as it is easy to reference and solve by hand. The pictures above outline the process for decoding the cipher text. On the left, we identify the alphabets to be used. The countersign here is the second of the clues, "Where you are now". Now this is me making a big assumption here but the answer should be an obvious 'Atlantia'. To identify our alphabets we pick the rows that have the letters used in the countersign. Remembering that each word uses the consecutive letter of the countersign and each letter in the word uses the next consecutive alphabet after the initial. Knowing the countersign is ATLANTIA we simply cycle through each countersign letter position looking for the cipher text letter on the bottom row. A full breakdown is available in the course notes. When fully deciphered you get the most important thing to take from this class…



Solution Walkthrough

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

PFAFMGDLXRFPX!

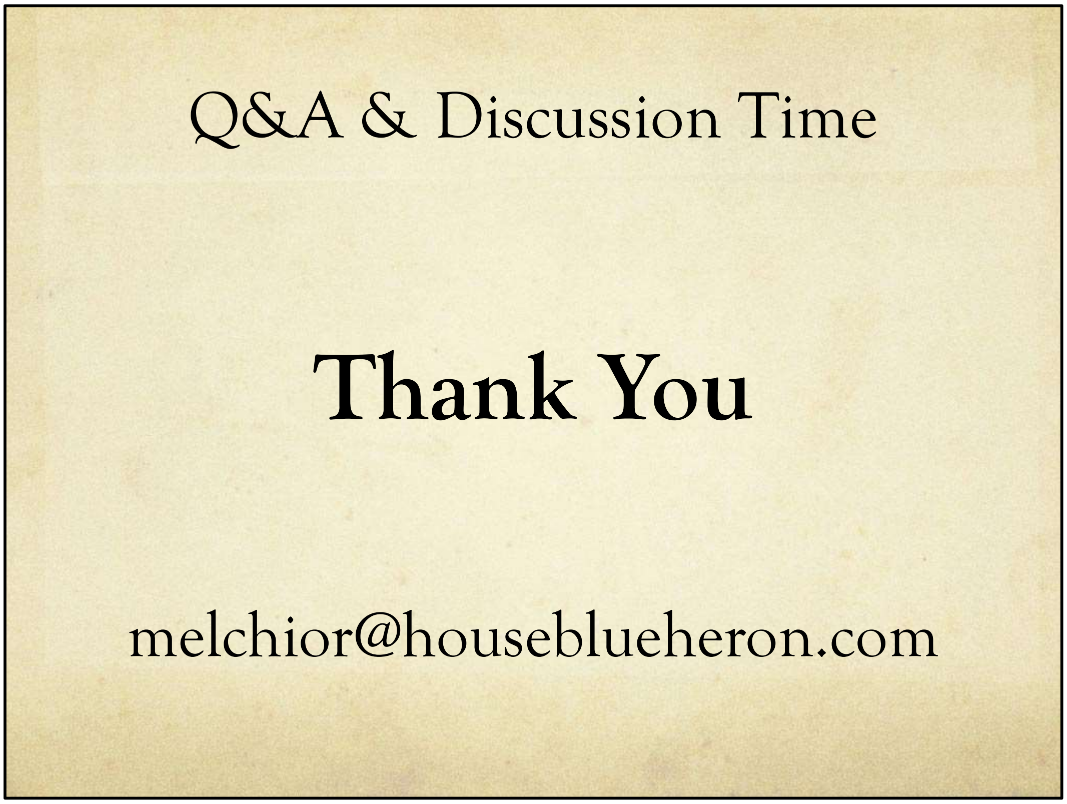
A(X) = Y where A is the alphabet, X is the letter to be encoded or decoded, and Y is the output character

'Crypto is fun' is enciphered using the countersign of ATLANTIA so the alphabets should be:
A(C) = P E(R) = F I(Y) = A O(P) = F V(T) = M B(O) = G C(X) = D
T(I) = L X(S) = X Y(X) = R
L(F) = F M(U) = P N(N) = X

'PFAFMGDLXRFPX!' is deciphered in the same manner. Simply start with the first letter of the countersign, A, and decode until you hit the delimitator of X. Then move to the next alphabet indicator in the countersign, T, and keep moving forward.

A(P) = C E(F) = R I(A) = Y O(F) = P V(M) = T B(G) = O C(D) = X
T(L) = I X(X) = S Y(R) = X
L(F) = F M(P) = U N(X) = N

PFAFMGDLXRFPX! = CRYPTO IS FUN!



Q&A & Discussion Time

Thank You

melchior@houseblueheron.com