

# Hidden Messages

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

## 16<sup>th</sup> Century Polyalphabetic Cipher

By Lord Dmitri Skomorochov, AOA, OBL  
House Blackfeather

The year is 1571, and the forces of Christianity and the Ottoman Empire are preparing for the largest naval battle in the history of the world. We are on the Spanish galley *Real*, flagship of the Holy League forces under the command of Don John of Austria, commander of the Holy League fleet.

Fortunately, we have a spy on a Turkish galley, sending us coded messages using a fixed-key polyalphabetic cipher that was first developed by Giovan Batista Belaso in 1553. It is based off of the classic substitution cipher created by Julius Caesar, but uses a different substitution based off of each letter of the alphabet, with a repeated keyword to determine which substitution key letter to translate the coded letter. Our keyword is 'SANGRE', Spanish for blood.

# Table of Contents

Cover Page	I
Introduction	II
Table of Contents	III
Coded Message	IV
Polyalphabetic Cipher	V
<i>Polygraphia and Traicte de Chiffres</i>	VII
Message Coding	VIII
Vigenère Table	X
Original Message	XI
Coding the Message	XII
Message Decoding	XIII
Decoding the Message	XIV
Project Review	XV
Bibliography	XV
Reference Photocopies	

ANGNVQADJGPSXTUOJSMR  
ZUIXSLYOWIAFBAEHEEVTR  
KDOBSPAGOQGXJALMFRWF  
EUDXZECGKLVIEKTXSNQK  
MIFTBZVPDIGCVVWNBKRW  
QTNYBLGWFGMEYEJOCHLH  
NZWSJEFZYSORBALWLAJIS  
MGUOKWYRBGKLOHVIYXGR  
RSVRTEEUEPQMLJZWEALX  
VRWWWFOEFATGKIRWSFTFX  
XAELISED RGKLQEGZFHASP  
ULVKEBLNLSTGNVVWGBU  
UFWFRRCEDLRRJIOIYRZV  
WLNZVHASPUMIJEQZYIJE

# Polyalphabetic Cipher

The evolution of cryptography has taken place since men have learned how to communicate with a written language. Researchers have documented cryptographic codes from early in the Roman Empire until modern times, with most cipher codes growing out of the previous code. The earliest code in this line of evolution is the Julius Caesar cipher, used by the Roman ruler during his days as the almost-Emporer of the mightiest empire on the earth.

The Caesar cipher was a simple substitution cipher; that is, all it involved was changing the letters of the original 'plaintext' message by a set amount of characters. For example, the original plaintext would be considered the 'A' cipher, since it wouldn't be shifted any spaces from the start. However, a 'D' cipher would have each letter of the plaintext shifted 3 characters down the alphabet. However, "...the weakness of the Julius Caesar system is that there are only 25 possible decrypts and so the cryptanalyst can try them all..." (Churchhouse, pg. 28). It wasn't that

hard to decrypt, and if a cryptanalyst were to try the first few letters of the ciphertext with each letter of the alphabet, he would eventually find which letter was used as the key.

During the 15th and 16th century in Italy, cipher codes had their largest jump in evolution, with many variations and alterations, and many great minds came up with ideas that took previous concepts and took them one step further each time. The first of these Leon Battista Alberti, "...Father of Western Cryptography...", "...who developed a type of cipher to which most of today's systems of cryptography belong. This species is polyalphabetic substitution..." (Kahn, pg. 125)

The polyalphabetic ciphers involved two or more different cipher alphabets being used in the same code, done with a combination of ciphers and methods known to both the sender and the recipient (and hopefully no one else). Alberti set off the chain of progress with his cipher disk, a device made of two disks put together, with rearranged letters of the alphabet on both disks, which would be spun around based on the pre-discussed system to code and decode a message. Using

Alberti's techniques, the cipher would be changed after three or four words, and then the position of the disk would be changed to a new cipher, indicated by a capital letter within the text (Kahn, pgs. 127-28).

The next landmark cryptographer on the path of polyalphabetic progress was Johannes Trithemius, who wrote several books on cryptography, called "Steganographia", which unfortunately earned him a negative reputation as a demonologist and occultist, though in reality, he used the study of demons and occult in part to demonstrate his cipher systems. "...in 1508, he addressed himself to a book carefully restricted to cryptology, as if to prove that that was what he meant all along..." (Kahn, pg. 133). This book, called "Polygraphia", became the first book written on the subject of cryptography (Kahn, pg. 133). His methods involved, among other things, of writing out meaningless Latin, where each word was a ciphertext for a letter of a message, with the cipherword for each plaintext letter changing throughout the message. Therefore, a full page of text appearing to be Christian invocations could in fact turn out to be a brief message about the weather.

Trithemius was followed by a relatively unknown practitioner of cryptography, Giovan Batista Belaso. It was Belaso who first suggested having each party of the coded message use a 'countersign', a pre-selected word or phrase that would set the pattern for the polyalphabetic code. With the use of a continuously repeated keyword, there could be a constant shift of cipher codes, easy to solve if the recipient knew the countersign, but almost impossible to break without it.

This method is known today as the Vigenère Tableau, named after Blaise de Vigenère, a cryptographer who published a book containing many of the previous cipher codes, as well as new variations that he came up with himself. It's for Belaso's cipher system, however, that Vigenère is known, and for four centuries, Belaso lost his deserved position in history.



# Message Coding

“...we take the words we wish to write, and put them on paper, writing them not too close together. Then over each of the letters we place a letter of our countersign...” “...the keyletter that is paired with a given plaintext letter indicates the alphabet of the tableau that is to be used to encipher that plaintext letter...” (Kahn, pg. 137)

“...to make encoding easier for us, we write down the keyword in a line in continual repetition and write the plaintext underneath...” “...then, step by step we can look up the ciphers in the table and write them underneath...” (Kippenhahn, pg. 112)

“...the keyword or numerical key would be written repeatedly above the plaintext and each plaintext letter moved the appropriate number of places to give the cipher...” (Churchhouse, pg. 28)

David Kahn is the modern source for most historical ciphers, and almost all modern cryptology is based off of his writings. Other authors, such as Kippenhahn and Churchhouse, have mainly repeated his explanations, reworded in their attempt to clarify Kahn, or perhaps to prove that they understood what he was saying by explaining it in their own words. Like these other historians, I intend to do the same thing with my own interpretation, to both clarify Kahn's explanation, and to prove that I, like the other historians, truly understand what I'm trying to say.

For my enciphered text, I chose the opening stanzas of Dante's *Divine Comedy Inferno* (English translation) as an example of text to be coded. I chose the word 'SANGRE' as my countersign or keyword, due to its small-to-medium size, the fact that it contained an 'A' (which I'll explain later), and because it is the beginning of the name of my shire, Sangre del Sol. Because of these three reasons, the word 'SANGRE' was perfectly suitable for my cipher experiments.

As seen in the ‘Coding the Message’ table, I carefully laid out my lines of repeated countersign - SANGRESANGRESAN - and then laid out Dante’s poem as plaintext beneath it. Instead of having a continuous stream of text, I broke the countersign and plaintext into rows on the page, but I made certain to continue each countersign from where the previous line broke off; otherwise the pattern would have been broken and would have left the recipient of the message with a 1-in-6 chance of continuing his translation in the correct pattern.

Since I was limiting myself to the six letters listed in the countersign, I was able to reduce my original 26x26 table, the *tabula recta*, to just those six rows, and the recipient would have been able to do the same (with caution taken, of course, to prevent anyone from seeing the reduced table and using it to break the cipher). From that point, it was simply a matter of looking up each letter on the table, according to row, column, and their corresponding value.

When we have the countersign and plaintext laid out, we would start by locating the countersign letter on the column to the left,

find the plaintext letter on the top row, and trace them both to locate the cipher letter on the table. For example, the first plaintext letter, ‘I’, we would locate the ‘S’ row on the left side of the table, and then locate the ‘I’ column on the top, which we would bring together to find the cipher letter ‘A’ on the table. For the second plaintext letter ‘N’, we would shift to the second letter of the countersign, ‘A’.

I specifically chose a countersign with the letter ‘A’ because the letter ‘A’ in this type of cipher is unique. Since it is the first letter of the alphabet that we’re using, it has no shift; the cipher for any plaintext lining up with the countersign letter ‘A’ is going to remain the same. For practical purposes, it also meant that I didn’t need to look up every sixth letter, all I had to do was copy the plaintext letter straight down.

On the same method as the countersign ‘A’ formula, it’s also worth noting that anywhere in the plaintext that the letter ‘A’ occurred, the corresponding letter of the countersign would be copied down as the cipher text, since the shift of the letters would catch up with the letter used.

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

## Original Message

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

### Original Work

In the midway of this our mortal life,  
 I found me in a gloomy wood, astray  
 Gone from the path direct: and even to tell  
 It were no easy task, how savage wild  
 That forest, how robust and rough its growth,  
 Which to remember only, my dismay  
 Renews, in bitterness not far from death.  
 Yet to discourse of what there good befell,  
 All else will I relate discovered there...

**The Divine Comedy - Inferno**  
**Dante Alighieri**

### Original Work Compressed Together

INTHEMIDWAYOFTHISOURMORTALL  
 IFEIFOUNDMEINAGLOOMYWOODAST  
 RAYGONEFROMTHEPATHDIRECTAND  
 EVENTOTELLITWERENOEASYTASKH  
 OWSAVAGEWILDTHATFORESTHOWRO  
 BUSTANDROUGHITSGROWTHWHICHT  
 OREMEMBERONLYMYDISMAYRENEWS  
 INBITTERNESNOTFARFROMDEATH  
 YETTODISCOURSEOFWHATHEREGO  
 ODBEFELLALLELSEWILLIRELATED  
 ISCOVEREDTHERE

# Coding the Message

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

**Row - Keyword**                    SANGRESANGRESANGRESANGRESANGRESANGRESANGRESANGRESANGRESANGRESAN  
**Column - Original Message**    INTHEMIDWAYOFTHISOURMORTALLIFEIFOUNDMEINAGLOOMYWOODASTRAY  
**Table - Coded Message**        ANGNVQADJGPSXTUOJSMRZUIXSLYOWIAFBAEHHEEVTRKDOBSPAGOQGGJXJAL

**Row - Keyword**                    GRESANGRESANGRESANGRESANGRESANGRESANGRESANGRESANGRESANGRESANGRESA  
**Column - Original Message**    GONEFROMTHEPATHDIRECTANDEVENTOTELLITWERENOEASYPATHSAVAGE  
**Table - Coded Message**        MFRWFEUDXZECGKLVIEKTXSNQKMIFTBZVPDIGCVVWNBKRWQTNYBLGWFGMEYE

**Row - Keyword**                    NGRESANGRESANGRESANGRESANGRESANGRESANGRESANGRESANGRESANGRESAN  
**Column - Original Message**    WILDTHATFORESTHOWROBUSTANDROUGHITSGROWTHWHICHTOREMEMBER  
**Table - Coded Message**        JOCHLHNZWSJEFZYSORBALWLA AJISM GUOKWYRBGKLOHVIYXGRRSVRTEE

**Row - Keyword**                    GRESANGRESANGRESANGRESANGRESANGRESANGRESANGRESANGRESANGRESANGRESA  
**Column - Original Message**    ONLYMYDISMAYRENEWSINBITTERNESSNOTFARFROMDEATHYETTODISCOURSE  
**Table - Coded Message**        UEPQMLJZWEALXVRWWFOEFATGKIRWSFTFXXAELISEDRGKLQEGZFHASPULVKE

**Row - Keyword**                    NGRESANGRESANGRESANGRESANGRESANGRESANGRESANGRESANGRESANGRESA  
**Column - Original Message**    OFWHATHEREGOODBEFELLALLELSEWILLIRELATEDISCOVEREDTHERE  
**Table - Coded Message**        BLNLSTGNVVWGBUUFWFRRCEDLRRJIOIYRZVWLNZVHASPUMIJEQZYIJE

# Message Decoding

For decoding the message, it is fairly simple, provided that the recipient of the message knows the proper countersign. Otherwise, breaking the code is almost impossible. Even assuming that the interceptor of the message knows that the countersign is six characters long, that still leaves them with over 300 million possible combinations, if the countersign was only made up of only a 26 letter alphabet.

Using the same formula and reduced table that we used to translate the message into ciphertext, we lay out a string of continuous countersign, and right below it the line of ciphertext that we're attempting to decode. However, now that we already have the cipher message, which were the letters located on the table, we will now reverse our search pattern and try to locate the column that each ciphertext letter belongs to.

As before, we would start by locating the countersign letter on the column to the left, but then we would locate the ciphertext letter

along that row, and once we've found the ciphertext letter, we would trace that column up to the top to determine the plaintext letter on the top row. For example, the first ciphertext letter, 'A', we would locate the 'S' row on the left side of the table, and then locate the ciphertext letter 'A' on the table, and we would follow that 'A' up to the column in which it is located to find the plaintext letter 'I', the first letter of the plaintext message.

For the second ciphertext letter 'N', we would shift to the second letter of the countersign, 'A'. Similar to before, when any letter lined up with an 'A', we know that the ciphertext letter 'N' has to line up with the same plaintext letter 'N'.

One by one, as we locate each plaintext letter, the message starts to come into focus, with the only remaining challenge to be separating the new part of plaintext letters into recognizable words and phrases (which is why I chose to code the English language version of Dante's Inferno), and to reveal the message that was meant only for you, the recipient.



# Project Review

Do you think you understand how the code works? Let's find out. Here are three messages that the Holy League has received from our spies in the Turkish fleet. Decode the hidden messages for the sake of our navy. (The plaintext spaces have already been separated per word for ease of use.)

LHRHRXLLRCZPDBRGKPWPNTKS

-----

LHRNFPQLRGXYWIFGKQWSFOEE

-----

OEJOC PSTGGTOXRBSKLWWRYK

-----

# Bibliography

- 1) Kahn, David  
"The Codebreakers - The Story of Secret Writing"  
Scribner, New York, New York  
© 1967, 1996

David Kahn was one of the first men of modern times to explore the history and complexity of cryptography, and many authors and historians have based their research off of his work. Most of the references that can be found for early and medieval cryptography use Kahn as their own primary reference.

- 2) Kippenhahn, Rudolf  
"Code Breaking - A History and Exploration"  
Overlook Press, Woodstock, New York  
© 1999
- 3) Churchhouse, R. F.  
"Codes and Ciphers - Julius Caesar,  
the Enigma and the Internet"  
Cambridge University Press, New York, New York  
© 2002