

# Secret Writing: the Development and Methods of Early and Renaissance Ciphers

*Lady Cécile de Brétigny*

ladycecilia@hotmail.com

*A man is crazy who writes a secret in any other way than one which will conceal it from the vulgar.*

--Roger Bacon, 12<sup>th</sup> C. monk

The first recorded attempts of secret writing are attributed to the ancient Egyptians, where non-standard hieroglyphics were used to conceal the meaning of the message outside a tomb. Many civilizations used cryptography. There is evidence of secret writing from Egypt, Babylon, Greece, Rome, India, China, Scandinavia, Persia and many others. (Kahn, 1967)

The medieval examples of cryptography are very simple and did not improve much on systems developed by the Greeks and Romans. As literacy was relatively rare, the cryptography did not have to be advanced. According to David Kahn, “phrases were written vertically or backwards; dots were substituted for vowels; foreign alphabets were used; plaintext was replaced by the [letter] that follows it” (1967, p. 89). Notably, cipher was used by Geoffrey Chaucer in *Treatise on the Astrolabe* for six passages (Kahn, 1967). In many cases, the use of cryptography with symbols was considered black magic and used by alchemists and inventors to obscure their notes.

The innovations and politics of the Renaissance affected the world of cryptography and the need for secret communication. It was very common for messages of nobility and diplomats to be intercepted and read. Cryptography spread rapidly in the Renaissance with an increase in literacy rates and the invention of polyalphabetic ciphers which are much more robust than ancient and medieval ciphers. Many decrypted letters are published in *Secret Writing in the Public Records: Henry VIII-George II* (Richards, 1974). Remarkably, several of the included letters were to and from Mary, Queen of Scots, who was later beheaded by Elizabeth I for her incessant scheming to usurp the throne of England.

## Terminology:

Autokey:	after using a priming letter, the decrypted message becomes its own key
Cipher:	method of concealment focused on the letter
Ciphertext:	message of encrypted letters
Code:	method of concealment focused on a word or phrase

Cryptanalysis: the process of solving an encrypted message.

Cryptography: “secret writing” from the Greek *kryptos* “secret, hidden” and *graphia* “writing”

Decrypt: reveal a message that has been encrypted a cipher or a code

Encrypt: concealed by a cipher or a code so that the original message is no longer easily legible

Key: set of instructions to encrypt or decrypt a message

Monoalphabetic substitution: a single alphabet is used to conceal a plaintext communication

Plaintext: the actual content of the message when not encrypted.

Polyalphabetic substitution: multiple alphabets have been used to conceal a plaintext communication.

Steganography: the art/science of concealing the existence of a message.

### ***Ciphers vs. Codes and Cryptography vs. Steganography***

Ciphers are based on the individual characters in a message, and generally translate letter to another letter or symbol. On the other hand, codes translate whole words or phrases where “dog” could be the code for “escape” or “the sun is bright” could be code for “the transport has arrived”.

Cryptography and steganography are also regularly confused. Steganography involves concealing the existence of a message such as invisible inks or messages buried within other messages. Cryptography does not conceal the fact that a message exists; cryptography conceals the meaning of the message from those who do not know how to decipher it.

## **Types of Ciphers:**

### ***Transposition ciphers:***

The Greeks allegedly created transposition ciphers. Transposition ciphers just move the letters in a word around similar to an anagram. As all the letters are present, transposition ciphers are relatively easy to decrypt. (Haldane, 1976)

Example:

Plaintext: The sun and the moon.

Ciphertext: Het nsu dan eht omon.

### ***Alphabetical substitution:***

There are several types of alphabetical substitution ciphers. Alphabetical substitution ciphers generally translate letter to letter where an “A” becomes an “I”, “B” becomes a “J” and so on. The first alphabetical substitution ciphers were fairly simple, but these were later improved and obscured by adding more refinements.



circular copper plates, one larger than the other and attached through the center. One plate had the alphabet, while the other had the cipher alphabet. Each disk was divided into 24 sections related to 20 letters and the numbers 1-4. Only 20 letters were used in the outer ring, because Alberti determined that the letter H, K, and Y were redundant. The letters J, U and W were not in use (Newton, 1997). The inner circle did not have numbers, so that the encrypted numbers would blend into the cipher text and be indistinguishable from the rest of the message (Servos, 2003).

In modern terms, the Alberti Diskus is essentially the “secret decoder ring” loved by children. Every few letters, the reference alphabet could be changed by shifting the top disk. This method reduced the threat of frequency analysis that made the Caesar Cipher so susceptible to being broken (Haldane, 1976).

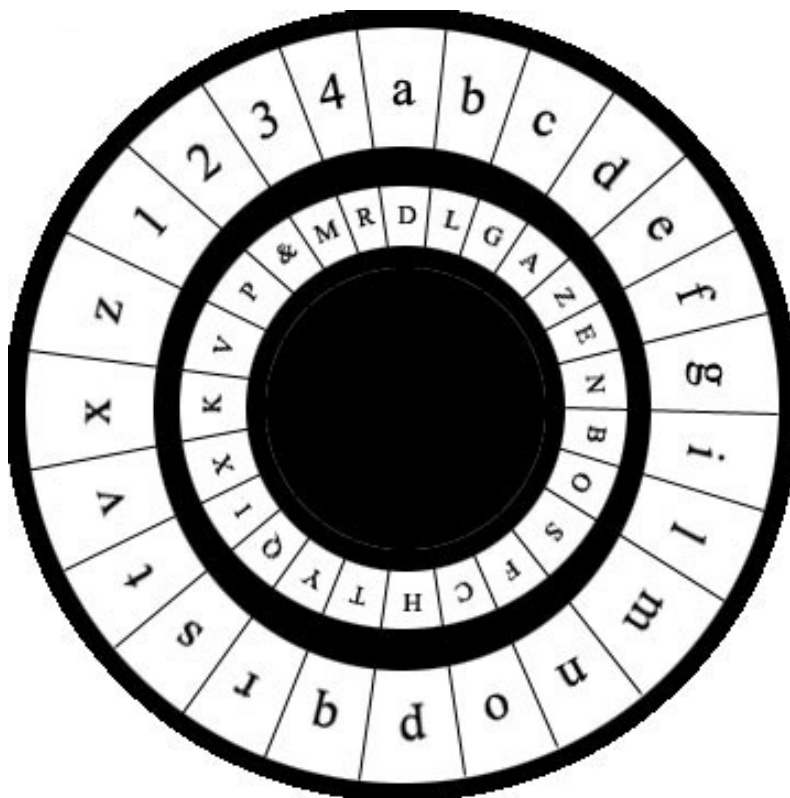


Figure 1. The Alberti Diskus (Servos, 2003).

### The Trithemius Cipher Table:

Johannes Trithemius was an abbot, writer and cryptologist, and he published the six-volume work *Polygraphia* in 1510. In his work, he proposed a substitution cipher which used Latin words in the place of letters. A seemingly innocent prayer or note could contain critical secret information. One of the negative aspects of this method is that the writer could use several pages of paper to elicit one thought. Trithemius is primarily known for the “Trithemius Cipher Table”. The alphabet shifts by one letter as the writer encodes the message. The first letter would use the first row, the second letter would use the second row, and so on. (Newton, 1997)

Example:

Plaintext	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
Shift																										
0	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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

Plaintext: THE EMISSARY  
 Ciphertext: TIG HQNYZIAI

Although “Emissary” has two s, the s is encrypted to different letters. Frequency analysis is much more difficult for the cryptanalyst, because the letters change depending on where the cryptographer is in the message. Gabriel de Lavinde introduced simple ways to increase cipher robustness in his *Trattiti in Cifra* in 1579. He suggested using alternatives for vowels, using numbers or symbols and the use of nulls. Each of these could be used to confuse a cryptanalyst. (Haldane, 1976)

### The Vigenère Cipher:

Blaise de Vigenère (1523-1596) was a French diplomat and cryptographer. He developed a system based off the Trithemius table, yet made the system more robust by using an autokey. The recipient would know the initial letter of the sequence and use the previously deciphered letter as the key for the following letter. The difference is the additional alphabet down the left side for the plaintext letters. This cipher system was finally broken after nearly 200 years by Kasiski in 1861 (Haldane, 1976). This system also allows the cryptographer to autokey. The recipient would know the initial letter of the sequence and use the previously deciphered letter as the key for the following letter.

Plaintext	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	
Key																											
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	

Example:

Plaintext: THE EMISSARY  
Key: JTH EEMISSAR  
Ciphertext: CAL IQUAKSSP

## BIBLIOGRAPHY:

- Churchhouse, R. (2002). *Codes and ciphers: Julius Caesar, the Enigma, and the internet*. Cambridge: Cambridge University Press.
- Haldane, R. A. (1976). *The hidden world*. London: Robert Hale & Company.
- Kahn, D. (1967). *The codebreakers: the story of secret writing*. New York: Macmillan Company.
- Newton, D. (1997). *Encyclopedia of cryptography*. Santa Barbara, California: Instructional Horizons, Inc.
- Richards, S. R. (ed.). (1974). *Secret writing in the public records: Henry VIII – George II*. London: Crown.
- Schmaker, W. (1982). *Renaissance curiosa*. Binghamton, New York: Center for Medieval and Early Renaissance Studies State University New York at Binghamton.
- Servos, W. (2003). *The Alberti Cipher*. Retrieved on August 12, 2005 from <http://starbase.trincoll.edu/~crypto/historical/alberti.html>
- Wrixon, F. B. (1992). *Codes and Ciphers*. New York, New York: Prentice Hall.