Cryptography

or ... how to keep a secret

By Peter Westergaard, peter@westergaard.ca

Cryptography (code-making), as any other skill, grew with its use throughout medieval Europe. It enjoyed a rare benefit however: it was pursued hotly by its jealously competitive cousin cryptanalysis (code-breaking). The one hot on the heels of the other, these two skills enjoyed an "arms-race" of growth through several centuries, paving the way for broad leaps in understanding and skill, leading us all the way to the sophisticated cryptographic (and cryptanalytic) techniques of today.

Some Definitions:

Plaintext:	The original text, in plain and readable format.
Ciphertext:	The result of applying some secret key to the plaintext, so that it is 'unreadable'.
Key:	The information needed to convert a message between Plaintext and Ciphertext.
Cipher: (v)	The process of changing the letters of the plaintext, resulting in the ciphertext.
Cipher: (n)	The exact method used to change the letters of the plaintext into the ciphertext
Code: (n)	A process by which whole words or phrases are replaced.

Cryptography:	The study of encrypting text, making it secret, or 'unreadable'.
Cryptanalysis:	The study of reading encrypted ('unreadable') text, breaking the encryption.

Part I: Transposition

Transposition is the first step of actual "cryptography". In this method of secrecy, no letters are changed, but they are re-arranged in a pre-determined order.

Some examples

1. Spelling Backwards.
2. (spoken) "Pig Latin"
3. The ancient Spartan skytale ("staff cipher") [5th century BCE].
4. "Card" cipher.

More details

The Spartan Skytale:

In the 5th century BCE, the Spartans were said to use a method of secret communication where commanders in possession of a staff of a pre-determined thickness would wrap a long strip around the shaft, similar to athletic tape around the grip of a racket or hockey stick. They would then write their message along the length of the staff, and unwind the strip.

The receiving commander would wrap the strip around his own staff, and simply read the message.

People intercepting the unwound strip may find an otherwise 'unreadable' arrangement of letters.

Why does it work?

This type of 'scrambling' expects that the person intercepting the transposed message will have difficulty determining the correct order for the letters.

This may not **seem** to be a terrible assumption.

First, consider how many ways are there are to rearrange the letters in the word "CAT"… six: ACT, ATC, CAT, CTA, TAC, and TCA.

And now, consider how many ways to rearrange the four letters of the word "HARM" … twenty-four! (AHMR, AHRM, AMHR, AMRH, ARHM, ARMH, HAMR, HARM, HMAR, HMRA, HRAM, HRMA, MAHR, MARH, MHAR, MHRA, MRAH, MRHA, RAHM, RAMH, RHAM, RHMA, RMAH, and RMHA) – That's four times as many as for a three-letter word.

Similarly, there are 120 arrangements for five letters… five times more than a four-letter word.

Even counting for duplicated letters, the number of possible rearrangements for a single typical sentence becomes so long that one person could never write them all out *in their lifetime*!

Weaknesses?

Part II: Monoalphabetic Substitution

Substitution is the next step of "cryptography". In this style, letters are replaced with a different letter, or perhaps with a symbol.

Some examples

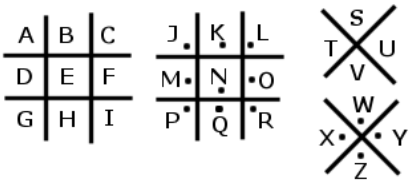
1. Da Vinci's "cipher"
2. "Pigpen Cipher" [Tudors - England].
3. Caesar Cipher [Julius Caesar]\
4. Polybius Square [Greek, 2nd c. BCE]
5. Futhark Table Codes [Norse, 7th – 9th c. CE]

More details

In these methods, a system of substitution is invented.

"Pigpen Cipher"

According to Giovanni Baptista Porta, the Tudors made popular use of this system. A familiar modern-day children's cipher, each letter corresponds to a shape, with or without dots:



Caesar Cipher

Julius Caesar is credited with several different systems. The most commonly-known "Caesar Cipher" is simply to shift each letter in the alphabet down by three places, as so:

Plain	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
Cipher	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

It is important to note that the bottom row of the Caesar Cipher could be replaced arbitrarily, giving an easily-changed 'key'. Memorizing such a key could be done quite easily. For one example, start with Z, Y, X, then the distinct letters of someone's name (Edouard!), and then use the rest of the alphabet:

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

Futhark Table Codes

The futhark alphabet divides into three groups. Each rune then can be represented by two numbers; the group number (1-3) and the rune number (1-8).

Why does it work?

If your attacker does not know the system, they are left with a stream of letters or symbols that has no meaning to them. Guessing randomly is of very little use.

Weaknesses?

Part III: Polyalphabetic Substitution

Polyalphabetic Substitution is the next step of "cryptography". It combats **frequency analysis**, by introducing several different alternatives for encrypting any single plaintext character.

Some examples

1. Alberti's "Cipher Disk" [Italy – 15th c.]
2. "Vigenere's Cipher" (actually created by Giovan Batista Belaso, 1553)
3. Vigenere's true cipher – the autokey [France – 16th c.]
4. Mary Queen of Scots (nomenclators, nulls) [England

More details

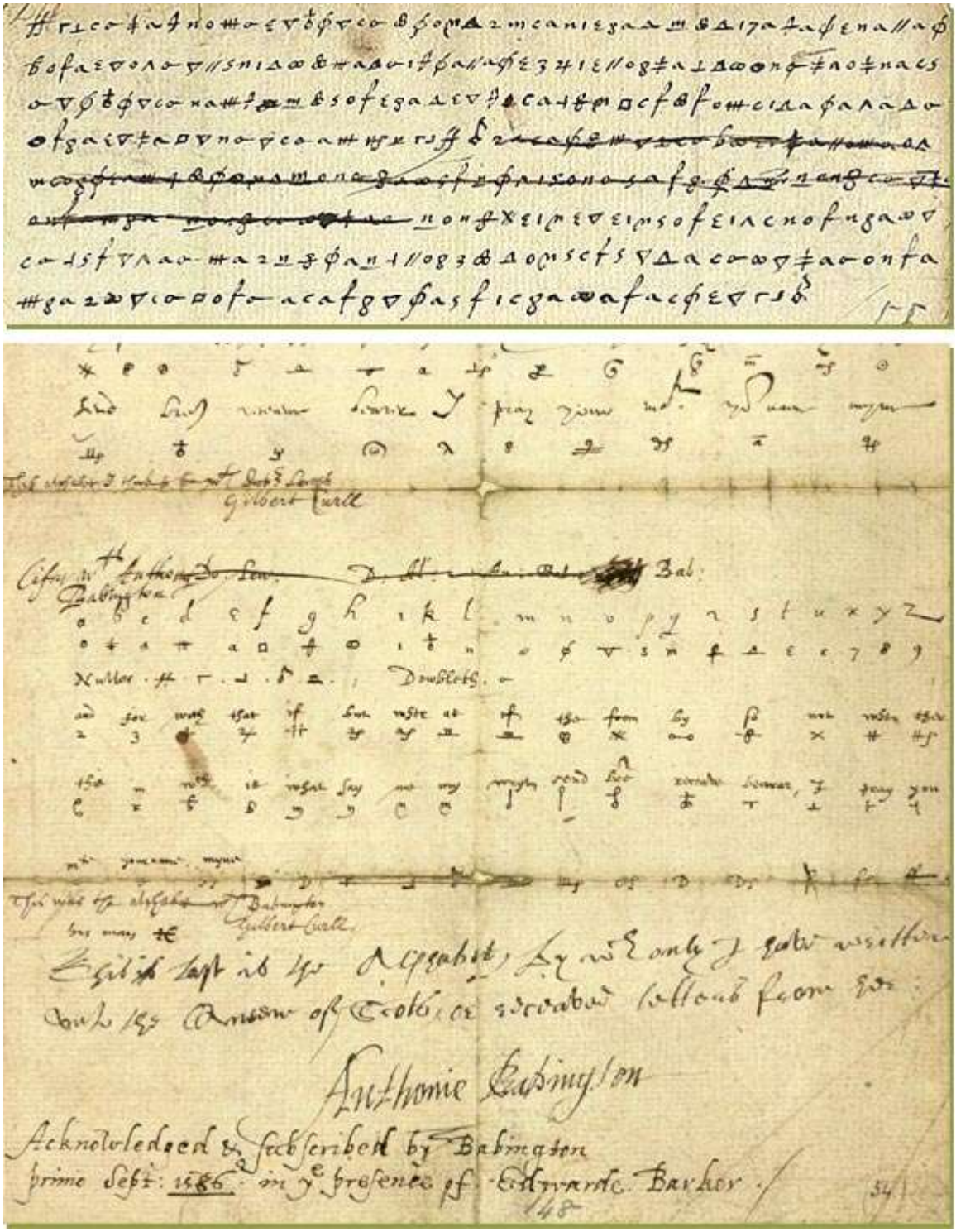
In these methods, a system of substitution is invented. The substitution is like the monoalphabetic substitution, but either the whole substitution changes within the message, or the encryptor is given several choices when performing an encryption (one plaintext letter becomes any of several ciphertext symbols).

Giovan Batista Belaso's cipher (called the "Vigenere Cipher")

This cipher revolves around the simple idea of creating 26 Caesar Cipher rows, each rotated by an additional letter, and labelled with a letter of the alphabet. Adopting an easily-memorized (and thus easily-changed) key, the encryptor writes the letters of the key above the plaintext. Then, each letter in the plaintext is encrypted using the Caesar Cipher row indicated by the letter of the key appearing directly above the 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**
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

Mary Queen of Scots



From: http://upload.wikimedia.org/wikipedia/en/e/e0/Babington_postscript.jpg

(Public Domain image - Thomas Phelippes' forged cipher postscript to Mary, Queen of Scots' letter to Anthony Babington, sourced from UK National Archives article on Mary)