2 The Invention of Polyalphabetic Substitution

Polyalphabetic Encryption in Renaissance

See the web page `http://www.staff.uni-mainz.de/pommeren/Cryptology/Classic/2_Polyalph/Renaissance.html`

The Trithemius Table (aka Vigenère Table)

This table is used for polyalphabetic substitution with the standard alphabet and its cyclically shifted secondary alphabets. It has n rows. The first row consists of the alphabet Σ. Each of the following rows has the alphabet cyclically shifted one position further to the left. For the standard alphabet this looks like this:

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Trithemius used it progressively, that is he used the n alphabets from top to down one after the other for the single plaintext letters, with cyclic repetition.

> Note that this procedure involves no key and therefore is not an encryption in the proper sense. Its security is only by obscurity.

Notwithstanding this weakness even Trithemius's method results in a crucial improvement over the monoalphabetic substitution: Each letter is encrypted to each other the same number of times in the mean. The frequency distribution of the ciphertext is perfectly uniform.

The Bellaso Cipher (aka Vigenère Cipher)

Even Vigenère himself attributes this cipher to Bellaso. It uses the Trithemius table but with the alphabet choice controlled by a keyword: for each plaintext letter choose the row that begins with this letter. This method uses a key and therefore is a cipher in the proper sense.

As an **example** take the keyword MAINZ. Then the 1st, 6th, 11th, ... plaintext letter is encrypted with the "M row", the 2nd, 7th, 12th, ... with the "A row" and so on. Note that this results in a periodic Caesar addition of the keyword:

```
p o l y a l p h a b e t i c
M A I N Z M A I N Z M A I N
---------------------------
B O T L Z X P P N A Q T Q P
```

In general the Bellaso cipher uses a group structure on the alphabet Σ. For the key $k = (k_0, \ldots, k_{l-1}) \in \Sigma^l$ we have

Encryption: $c_i = a_i * k_{i \bmod l}$

Decryption: $a_i = c_i * k_{i \bmod l}^{-1}$

The first one who described this cipher algebraically as an addition apparently was the French scholar Claude Comiers in his 1690 book using a 18 letter alphabet. Lacking a suitable formal notation his description is somewhat long-winded. Source:

> Joachim von zur Gathen: *Claude Comiers: The first arithmetical cryptography.* Cryptologia 27 (2003), 339 - 349.