

CLASSICAL CIPHERS

SPY GAMES CAMP – PSU, 2014

- **Substitution ciphers:** These change the letters in a text with other letters (or symbols).
 - (1) *Caesar Shift:* Shift every letter forward in the message by a fixed number. For example **abc** becomes **cde** if your shift is 2.
 - (2) *Substitution:* Every letter in the alphabet is sent to a different (random) letter. For example **a** → **f**, **f** → **q**, **q** → **b**, etc.
 - (3) *Vigenère:* Choose a code phrase, for instance **frogs**, then draw a diagram like so.

f	r	o	g	s	f	r	o	g	s	f	r	o	g	s	f	r	o	g	s	f	r	o	g	s
a	l	l	y	o	u	r	b	a	s	e	a	r	e	b	e	l	o	n	g	t	o	u	s	
F	C	Z	E	G	Z	I	P	G	K	J	R	F	K	T	J	C	C	T	Y	Y	F	I	Y	

Here **f** counts as letter 5 (starting with **a** = 0) and so we shift **a** by 5. **r** is 17 and so we shift **l** by 17 to get **c**, etc. This is technically a polyalphabetic substitution cipher (albeit a simple one) since there is more than one way that things are shifted. Basically it is a number of different Caesar shifts (depending on the character position). The German Enigma machine was also a polyalphabetic substitution cipher (although more complicated than this one).

- (4) *Autokey:* Similar to Vigenère.¹ Choose a key, for instance **frogs** and form a table like the one below.

f	r	o	g	s	a	l	l	y	o	u	r	b	a	s	e	a	r	e	b	e	l	o	n	g
a	l	l	y	o	u	r	b	a	s	e	a	r	e	b	e	l	o	n	g	t	o	u	s	
F	C	Z	E	G	U	C	M	Y	G	Y	R	S	E	T	I	L	F	R	H	X	Z	I	F	

The operation is just like Vigenère except after the initial application of the key, the text itself becomes the key.

- **Transposition ciphers:** These reorder the text.
 - (5) *Scytale:* Wrap a piece of cloth around a tube, write on it going down the length of the tube. Unwrap it. It is easy to decrypt with a another tube of the same diameter.
 - (6) *Columnar transposition:* Choose a key, for instance **CAT**, then write the message in rows of the same length as the keyword

C	A	T
T	H	E
G	E	R
M	A	N
F	O	R
C	E	S
A	R	E
H	E	R
E	Y	B

We then read the columns vertically starting from the column with first letter in alphabetical order. In this case, we read the **A** column, then the **C** column, then the **T** column. Thus we get **H E A O E R E Y T G M F C A H E E R N R S E R B**

- (7) *Other transposition:* You don't have to read down the columns, you can read in off the letters in any pattern: diagonally, in a spiral, in a snake-like pattern.

¹and actually invented by Vigenère, unlike the Vigenère cipher.