POLYALPHABETIC SUBSTITUTION .. annotated by Ivar (2001)

Polyalphabeticity means that for every plain text letter, there are multiple cypher letter substitutes. Almost always, polyalphabetic cyptosystems are keyword based.

The best example is the Vigenere table. It is best illustrated below:

PLAIN TEXT LETTERS

KEY LETTERS	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
K 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
E 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
Y 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
L 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
E 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
T 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
T 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
E 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
R 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
S 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

How to use the Vigenere

Example

KEYWORD : EXCALIBUR
PLAIN TEXT:
Now is the time for all good men to come to the aid of their fellow man

KEY : exc al ibu rexc ali bur exca lib ur exca li bur exc al ibure xcalib ure
PLAIN TEXT : now is the time for all good men to come to the aid of their fellow man

To encipher the first letter of the plain text (letter n), locate n in the PLAIN TEXT LETTERS row of the table, also the key letter (letter e) in the KEY LETTERS column. Note where the row of the key letter intersects with the column of the plain text letter. The letter in which they intersect is the cypher letter. Thus,

KEY : exc al ibu rexc ali bur exca lib ur exca li bur exc al ibure xcalib ure
PLAIN TEXT : now is the time for all good men to come to the aid of their fellow man
CYPHER : rly id biy kmjg ...

Notice that the t in 'the' and 'time' are enciphered as letters b and k respectively. This is the nature of polyalphabeticity. It doesnt take a genius to know that this cryptosystem offers better protection compared to monoalphabet enciphering.

NOTES:

The strength of the Vigenere lies in the length of its keyword and on the sequence of the cypher equivalents.

In the illustration below

PLAIN TEXT LETTERS

```
      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
   e
   f
K  g
E  h
Y  i
   j
L  k
E  l
T  m
T  n
E  o
R  p
S  q
   .
   .
   z
```

Notice that the first cypher alphabet is just the normal sequence of the standard English alphabet (a..z). The normal sequence greatly increases the susceptibility of the Vigenere for solutions via cryptanalysis. A common method of reordering the cypher alphabet is to use a mixed alphabet. Any letter or letter placed not in the normal position will make a mixed alphabet.

To create a thoroughly mixed alphabet is easy. We could use the keyword EXCALIBUR in our example above.

```
e x c a l
i b u r d
f g h j k
m n o p q
s t v w y
z
```

then write them together starting from the first column

```
e i f m s z x b g n t c u h o v a r j p w l d k q y
```

we could then use the resulting jumbled alphabet as the cypher alphabet

```
                     PLAIN TEXT LETTERS

      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  e i f m s z x b g n t c u h o v a r j p w l d k q y
   b  i f m s z x b g n t c u h o v a r j p w l d k q y e
   c  f m s z x b g n t c u h o v a r j p w l d k q y e i
   d
   e
   f
K  g
E  h
Y  i
   j
L  k
E  l
T  m
T  n
E  o
R  p
S  q
   .
   .
   z
```