The Playfair Cipher

The cipher was invented in 1854 by Charles Wheatstone, but was named after Lord Playfair who promoted the use of the cipher.

The Playfair cipher is a digraph (pairs of letters) substitution cipher. All non-letters are ignored and not encoded. Numbers, spaces, and punctuation are also skipped.

Many times the pairs of letters are written broken into two letter groups for encoding and decoding. This made it easy to determine that it was a playfair cipher so occasionally they would remove all spaces.

Example: TH EP LA YF AI RC IF ER or THEPLAYFAIRCIPHER

This type of cipher uses a table where one letter of the alphabet is omitted, and the remaining letters are arranged into a 5x5 grid. (One letter is omitted to reduce the alphabet to fit into the 5x5 grid.) You can either omit "Q" or the "J" . Typically, the J is removed from the alphabet and an "I" takes its place in the text that is to be encoded. (This gives it a slightly more thought provoking nature as one has to think about converting the "J" to "I" and back again for decoding.)

This type of cipher also uses a keycode. (A secret word or phrase that is used in creating the table grid.) Without the keycode, one can not decode messages since the grid is made based on the keycode.

To generate the table, one would first fill in the spaces of the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order

Example: If the Keycode is "SHAWN", the table grid would look like:

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

Notice, starting at the top left corner, we list the letters SHAWN. We then follow with the remaining letters of the alphabet reducing by one letter. In this one, the J is left out. (Remember, we could also remove the Q instead of the J.) Also note that the letters of the keycode are already used so they are not listed again later in the table grid.

If the keycode is longer than 5 letters, you just continue the letters on the following row.

If the keycode has a double letter or a letter that is used more than once, we skip the letter the second time it would appear.

Example: If the Keycode is "MARIANNE"

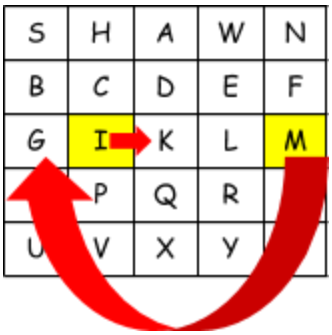
M	A	R	I	N
E	B	C	D	F
G	H	J	K	L
O	P	S	T	U
V	W	X	Y	Z

Notice that the keycode was longer than 5 letters and had to drop to the next line to complete the word. Notice also that the second "A" and the second "N" is omitted in the keyword. One other mention is that one can see that this time the "Q" was omitted instead of the "J".

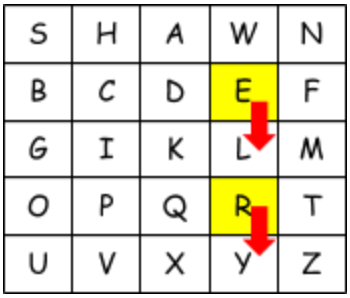
*We will be using the table grid for our SHAWN keycode for the encoding and decoding examples.

To encode a message:

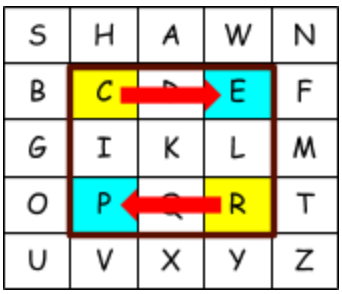
1. Break the code into two-letter chunks.
2. Repeated letters in the same digraph pair chunk are usually separated by an "X". The message, "HELLO HUNTER" would become "HE LX LO HU NT ER".
3. If there is not an even number of letters in the message, it is padded with a spare X at the end.
    a. HELLO DECODER would become "HE LX LO DE CO DE RX".
4. Next, you take your letter pairs and look at their positions in the grid.
    a. If the letters appear on the same row of your table, replace them with the letters to their immediate right, wrapping around to the left side of the row if necessary. For example, using the table above, the letter pair IM would be encoded KG



    b. If the letters appear on the same column of your table, replace them with the letters immediately below, wrapping around to the top if necessary. For example, using the table above, the letter pair ER would be encoded as LY.



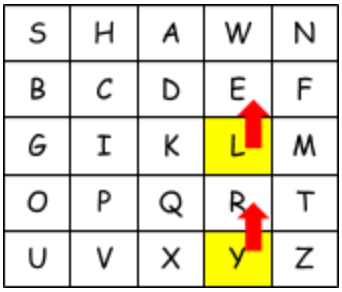
    c. If the letters are on different rows and columns, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important - the first letter of the pair should be replaced first. For example, using the table above, the letter pair CR would be encoded as EP.



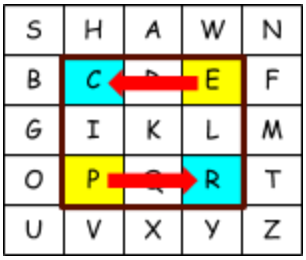
To decode a message:

1. Draw a 5 x 5 table grid.
2. Fill in the grid with the keycode and complete the grid.
    a. First fill in the spaces of the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order.
    b. Remember: One letter is omitted to reduce the alphabet to fit into the 5x5 grid. You can either omit "Q" or the "J".
        i. Hopefully you know which the encoder used. If not, pick one. If your decoding creates gibberish, then you may need to do it the other way later.
3. Break the code into two-letter chunks if it is not. Remember sometimes to make it not look like a playfair cipher, people would remove all the spaces.
4. Next, you take your letter pairs and look at their positions in the grid.
    a. If the letters appear on the same row of your table, replace them with the letters to their immediate left, wrapping around to the right side of the row if necessary. For example, using the table above, the letter pair KG would be decoded IM

    b. If the letters appear on the same column of your table, replace them with the letters immediately above, wrapping around to the bottom if necessary. For example, using the table above, the letter pair LY would be decoded as ER.



    c. If the letters are on different rows and columns, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important - the first letter of the pair should be replaced first. For example, using the table above, the letter pair EP would be decoded as CR.



Time to try it out.

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

PN FC HD TS NO NQ GP AZ

PN	FC	HD	TS	NO	NQ	GP	AZ
TH	EB	AC	ON	ST	AT	IO	NX

Translation: THE BACON STATION

On August 2, 1943 President J. F. Kennedy, Jr. used a playfair cipher to alert others of where the PT boat under his command was lost in a military conflict with the Japanese destroyer Amagiri which had rammed and sliced in half the American patrol boat (PT-109.)

Australian Coastwatcher Lieutenant Arthur Reginald Evans of the Royal Australian Naval Volunteer Reserve received the following message at 0930 on the morning of the 2 of August 1943 via Morse Code:

KXJEY UREBE ZWEHE WRYTU HEYFS
KREHE GOYFI WTTTU OLKSY CAJPO
BOTEI ZONTX BYBWT GONEY CUZWR
GDSON SXBOU YWRHE BAAHY USEDQ

Evans, often having used the Playfair system, deciphered it with the key ROYAL NEW ZEALAND NAVY

The translation:

PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKETT
STRAIT TWO MILES SW MERESU COVE X CREW OF TWELVE
X REQUEST ANY INFORMATION.

Kennedy and his crew were rescued. Kennedy became a war hero and later becomes a U.S.President.

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

The Kennedy Cipher split into two letter pairs:

KX JE YU RE BE ZW EH EW RY TU HE YF SK RE HE GO YF I W TT TU OL KS YC AJ PO
BO TE IZ ON TX BY BW TG ON EY CU ZW RG DS ON SX BO UY WR HE BA AH YU SE DQ

Let us translate one letter pair at a time:

PT BO AT ON EO WE NI NE LO ST IN AC TI ON IN BL AC KE TT ST RA IT TW OM IL
ES SW ME RE SU CO CE XC RE WO FT WE LV EX RE QU ES TA NY IN FO RM AT IO NX

Combine the pairs and complete the translation:

PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKETT STRAIT TWO MILES SW
MERESU COCE X CREW OF TWELVE X REQUEST ANY IN FORMATI N X

*Note: there is a double TT that did not get translated. We can not do that in a Playfair Cipher. Some believe Kennedy did this to make people believe this was not a Playfair Cipher others think it is just a mistake he made.

**Note: COCE is misspelled. It is interpreted to supposedly mean COVE.