Playfair Instructions

The Playfair cipher or Playfair square is a manual symmetric encryption technique and was the first literal digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but bears the name of Lord Playfair who promoted the use of the cipher. It was used to great effect by Commonwealth armies in the First World War.

Playfair is a **cipher** because it enciphers individual characters rather than **encoding** whole words – though the distinction is unnecessary for our purposes – we will talk of encoding and decoding because most people are familiar with the terms.

We are going to develop a ruby encoder/decoder, which will:

(a) Create a cipher square from a given key-phrase
(b) Encode a given plain-text message and display its enciphered equivalent
(c) Decode a given cipher-text message and display its plain-text equivalent

The rules for Playfair are very simple, and hence can be easily codified in Ruby. There are several alternatives/options for the rules however, so be careful when using web resources to compare your output – the rules they use may be slightly different!

Creating the Cipher Square

A Playfair cipher square is a 5 x 5 square containing all the letters of the alphabet except the letter J – which is converted to an I.

To create a cipher square from a key-phrase, the key-phrase is placed into the cipher square one letter at a time from left to right, and top to bottom. The keyphrase is made into upper-case. All non-letter characters are removed, and all duplicate letters are also ignored.

It is important to remember for ALL Playfair text that the rule is always upper-case letters only, no spaces, punctuation, or other non-letter characters.

When all the letters of the key-phrase are used up and placed in the square properly, all the remaining spaces of the cipher square are filled up with the remaining letters in the alphabet in order – remembering the J is replaced by an I.

Thus, the key-phrase “playfair example” creates the cipher square below.

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

Encoding a Message – The Preparation

To encode a message, you first need to prepare it for encoding. This is a simple operation but it does have a couple of rules of its own.

The text of the message is split into digraphs (groups of two letters) which will be encoded one at a time using the cipher table. BUT….

If a digraph has two identical letters (EE for example), you insert an “X” between the two identical characters – shifting the second character to be the first character of the next digraph. If THAT digraph also contains an identical letter, then you insert a “Z” between those. For any more identical characters you switch between X and Z again.

Thus the word FREEDOM becomes “FR EX ED OM”, and the phrase ‘Congress shall’ becomes “CO NG RE SX SZ SH AL L” (we are using spaces to show the boundaries between digraphs just for simplicity – how you choose to create your digraphs is up to you!)

As you can see, the phrase “CO NG RE SX SZ SH AL L” has an odd number of letters in it. The final rule for preparing a message is to add an “X” to the end of a message with an odd number of letters – thus the message to be encoded is “CO NG RE SX SZ SH AL LX”

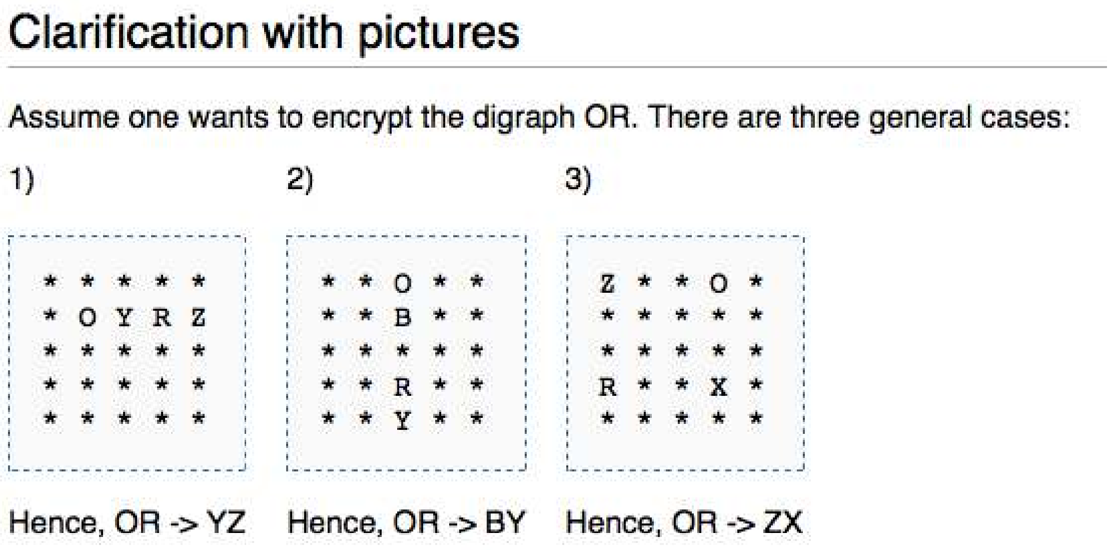
As a further example, given a plain text phrase “Hide the gold in the tree stump”, it becomes “HI DE TH EG OL DI NT HE TR EX ES TU MP” when converted into digraphs.

Encoding a Message – The Actual Encoding

Once a message is prepared, it can be correctly encoded. There are 3 rules to be followed – in order to each pair of letters in the plaintext:

1. If the letters appear on the same row of your cipher square, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).
2. If the letters appear on the same column of your cipher square, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).
3. If the letters are not on the same row or column, 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 encrypted pair is the one that lies on the same row as the first letter of the plaintext pair.

All but the last rule is fairly straightforward….. Wikipedia has a good example using simple diagrams.



Clarification with pictures

Assume one wants to encrypt the digraph OR. There are three general cases:

1)

```
* * * * *
* O Y R Z
* * * * *
* * * * *
* * * * *
```

Hence, OR -> YZ

2)

```
* * O * *
* * B * *
* * * * *
* * R * *
* * Y * *
```

Hence, OR -> BY

3)

```
Z * * O *
* * * * *
* * * * *
R * * X *
* * * * *
```

Hence, OR -> ZX

Therefore, using our cipher table from above:

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

And the text HI DE TH EG OL DI NT HE TR EX ES TU MP we encode it as follows:

1. The pair HI forms a rectangle, replace it with BM
2. The pair DE is in a column, replace it with OD
3. The pair TH forms a rectangle, replace it with ZB
4. The pair EG forms a rectangle, replace it with XD
5. The pair OL forms a rectangle, replace it with NA
6. The pair DI forms a rectangle, replace it with BE
7. The pair NT forms a rectangle, replace it with KU
8. The pair HE forms a rectangle, replace it with DM
9. The pair TR forms a rectangle, replace it with UI
10. The pair EX is in a row, replace it with XM
11. The pair ES forms a rectangle, replace it with MO
12. The pair TU is in a row, replace it with UV
13. The pair MP forms a rectangle, replace it with IF

So the enciphered text becomes BM OD ZB XD NA BE KU DM UI XM MO UV IF

Decoding

Decoding is easy. It is exactly the opposite of encoding. First you prepare the cipher text into digraphs – you won’t need to add any extra Xs or Zs this time of course or remove spaces and non-letter characters etc., then you use the 3 encoding rules as before – except where encoding moves RIGHT or DOWN, decoding moves LEFT and UP.

You will be left with a plain-text decoding of the cipher-text message which should be ‘mostly’ readable. It’s only ‘mostly’ readable because there will still be some extra Xs and Zs in it which may have been added during encoding. It is not possible to automatically remove these extra characters so you will have to remove them yourself to make complete sense of the message. In the First World War users of the code learned quickly not to use words with too many Xs or Zs in them naturally to reduce this effort ☺

The Rules (again)

1. The letter J is always converted to an I
2. All Playfair text is UPPER-CASE only, with all spaces and all non-letter characters removed.
3. When preparing plain text, split it into digraphs. If a digraph would contain two identical letters insert an “X” between the duplicates. If a duplicate is followed **immediately** by another duplicate, insert a “Z” between those. For any more duplicates after that alternate an X and a Z in that order.
4. When encoding, If the letters appear on the same row of your cipher square, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).
5. When encoding, If the letters appear on the same column of your cipher square, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).
6. When encoding, if the letters are not on the same row or column, 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 encrypted pair is the one that lies on the same row as the first letter of the plaintext pair.

Extended Example

The wikipedia page on Playfair has a good (but very small) example of a cipher square, plain-text message, and cipher-text message. Since it is sometimes helpful to see longer examples with more occurrences of duplicated letters etc. We have included a much longer example of a cipher square, plain-text message, and cipher-text message. If your code works on the wikipedia example however, you should have no problems with the longer one….

Key Phrase: First Amendment

The contents of the cipher key is...

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

Plain-Text is "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."

The processed plain-text becomes:

```
CO NG RE SX SZ SH AL LM
AK EN OL AW RE SP EC TI
NG AN ES TA BL IS HM EN
TO FR EL IG IO NO RP RO
HI BI TI NG TH EF RE EX
EX ER CI SE TH ER EO FO
RA BR ID GI NG TH EF RE
ED OM OF SP EX EC HO RO
FT HE PR ES SO RT HE RI
GH TO FT HE PE OP LE PE
AC EA BL YT OA SX SE MB
LE AN DT OP ET IT IO NT
HE GO VE RN ME NT FO RA
RE DR ES SO FG RI EV AN
CE SX
```

And is encoded thus:

The pair CO is in a column, replace it with OW
The pair NG forms a rectangle, replace it with EH
The pair RE is in a column, replace it with EG
The pair SX forms a rectangle, replace it with RY
The pair SZ forms a rectangle, replace it with TY
The pair SH is in a column, replace it with NQ
The pair AL is in a column, replace it with BV
The pair LM forms a rectangle, replace it with OA

The pair AK forms a rectangle, replace it with DB
The pair EN is in a row, replace it with ND
The pair OL is in a row, replace it with PO
The pair AW forms a rectangle, replace it with MV
The pair RE is in a column, replace it with EG
The pair SP forms a rectangle, replace it with RQ
The pair EC forms a rectangle, replace it with MG
The pair TI is in a row, replace it with FR
The pair NG forms a rectangle, replace it with EH
The pair AN is in a row, replace it with MD
The pair ES forms a rectangle, replace it with NR
The pair TA forms a rectangle, replace it with FD
The pair BL is in a column, replace it with LV
The pair IS is in a row, replace it with RT
The pair HM forms a rectangle, replace it with CN
The pair EN is in a row, replace it with ND
The pair TO forms a rectangle, replace it with IU
The pair FR is in a row, replace it with IS
The pair EL forms a rectangle, replace it with AP
The pair IG forms a rectangle, replace it with RC
The pair IO is in a column, replace it with MW
The pair NO forms a rectangle, replace it with MQ
The pair RP is in a column, replace it with EX
The pair RO forms a rectangle, replace it with IP
The pair HI forms a rectangle, replace it with CS
The pair BI forms a rectangle, replace it with CF
The pair TI is in a row, replace it with FR
The pair NG forms a rectangle, replace it with EH
The pair TH forms a rectangle, replace it with SK
The pair EF forms a rectangle, replace it with AR
The pair RE is in a column, replace it with EG
The pair EX is in a column, replace it with GR
The pair EX is in a column, replace it with GR
The pair ER is in a column, replace it with GE
The pair CI is in a column, replace it with OM
The pair SE forms a rectangle, replace it with RN
The pair TH forms a rectangle, replace it with SK
The pair ER is in a column, replace it with GE
The pair EO forms a rectangle, replace it with MP
The pair FO forms a rectangle, replace it with IL
The pair RA forms a rectangle, replace it with FE
The pair BR forms a rectangle, replace it with GF
The pair ID forms a rectangle, replace it with TM
The pair GI forms a rectangle, replace it with CR
The pair NG forms a rectangle, replace it with EH
The pair TH forms a rectangle, replace it with SK
The pair EF forms a rectangle, replace it with AR
The pair RE is in a column, replace it with EG
The pair ED is in a row, replace it with NA
The pair OM is in a column, replace it with WC
The pair OF forms a rectangle, replace it with LI
The pair SP forms a rectangle, replace it with RQ
The pair EX is in a column, replace it with GR
The pair EC forms a rectangle, replace it with MG
The pair HO forms a rectangle, replace it with CQ
The pair RO forms a rectangle, replace it with IP

The pair FT is in a row, replace it with IF
The pair HE forms a rectangle, replace it with GN
The pair PR is in a column, replace it with XE
The pair ES forms a rectangle, replace it with NR
The pair SO forms a rectangle, replace it with IQ
The pair RT is in a row, replace it with SF
The pair HE forms a rectangle, replace it with GN
The pair RI is in a row, replace it with SR
The pair GH is in a row, replace it with HK
The pair TO forms a rectangle, replace it with IU
The pair FT is in a row, replace it with IF
The pair HE forms a rectangle, replace it with GN
The pair PE is in a column, replace it with XG
The pair OP is in a row, replace it with PQ
The pair LE forms a rectangle, replace it with PA
The pair PE is in a column, replace it with XG
The pair AC forms a rectangle, replace it with MB
The pair EA is in a row, replace it with NM
The pair BL is in a column, replace it with LV
The pair YT forms a rectangle, replace it with ZS
The pair OA forms a rectangle, replace it with LM
The pair SX forms a rectangle, replace it with RY
The pair SE forms a rectangle, replace it with RN
The pair MB forms a rectangle, replace it with AC
The pair LE forms a rectangle, replace it with PA
The pair AN is in a row, replace it with MD
The pair DT is in a column, replace it with KD
The pair OP is in a row, replace it with PQ
The pair ET forms a rectangle, replace it with DR
The pair IT is in a row, replace it with RF
The pair IO is in a column, replace it with MW
The pair NT forms a rectangle, replace it with DS
The pair HE forms a rectangle, replace it with GN
The pair GO forms a rectangle, replace it with CP
The pair VE forms a rectangle, replace it with XA
The pair RN forms a rectangle, replace it with SE
The pair ME is in a row, replace it with EN
The pair NT forms a rectangle, replace it with DS
The pair FO forms a rectangle, replace it with IL
The pair RA forms a rectangle, replace it with FE
The pair RE is in a column, replace it with EG
The pair DR forms a rectangle, replace it with ET
The pair ES forms a rectangle, replace it with NR
The pair SO forms a rectangle, replace it with IQ
The pair FG forms a rectangle, replace it with RB
The pair RI is in a row, replace it with SR
The pair EV forms a rectangle, replace it with AX
The pair AN is in a row, replace it with MD
The pair CE forms a rectangle, replace it with GM
The pair SX forms a rectangle, replace it with RY

Cipher-Text in full is therefore:

OWEHEGRYTYNQBVOADBNDPOMVEGRQMGFREHMDNRFDLVRTCNNDIUISAPRCMWMQE
XIPCSCFFREHSKAREGGRGRGEOMRNSKGEMPILFEGFTMCREHSKAREGNAWCLIRQGRM
GCQIPIFGNXENRIQSFGNSRHKIUIFGNXGPQPAXGMBNMLVZSLMRYRNACPAMDKDPQDRR
FMWDSGNCPXASEENDSILFEEGETNRIQRBSRAXMDGMRY