Playfair Cipher

Overview: This is a type of cipher that is very difficult to break because no specific letter or number represents any specific letter. The Playfair Cipher uses a matrix of numbers and letters to develop the key.

Materials

- Pencil
- Paper

A	H	M	V	L	3	Y	D
X	K	B	5	P	Z	E	O
N	7	W	U	F	T	6	J
G	R	2	Q	C	A	I	S

Activity: This is a super-hard cipher to break. It's encoded by taking pairs of letters and numbers from a matrix. There are three rules to follow:

> If both letters are in the same row, then use the letters immediately to the right of each other. (Think of the rows as wrapping from the right end back around to that same row's left end).
>
> If both letters are in the same column, then use the letters immediately below them. If necessary, the bottom letter wraps back around to the top of the same row.
>
> If the two letters or numbers are in different rows **and** in different columns, then each letter is replaced by the letter in the same row that's also in the same column of the other letter. Basically, you find each intersection of the pair. Use the letter or number below the pair and then the one above the pair.

Play Fair sounds really complicated, but that also makes it a tough code to crack! Let's do an example:

> I WILL ARRIVE AT FOUR PM

We group the message in twos:

> IW IL LA RX RI VE AT FO UR PM

Note that we added an "X" between the double R term "RR," as we can't encode "RR" with this method.

Also note that the number of characters must be even, so add a space filler like Z or Q as needed.

To encode the message:

> IW: These are in different rows and columns, so we have I–2 and W-6 to make "26."
>
> LA: These are in the same row so we have L-3 and A-H to make "3H."
>
> AT: These are in the same column so we have A-3 and T-A to make "3A."

Replacing the pairs of letters in the original message we now have:

> 26 CY 3H GK 25 5Y 3A JP 7Q BL

To make it even harder, you can group them in groups of four or five to get:

26CY 3CGK 255Y 3AJP 7QBL

Just remember, when *decoding* the Playfair Cipher, you have to shift *up* instead of down and *left* instead of right. And it's easy to make a mistake by encoding in the incorrect order. Always double check your cipher before sending it on to the recipient. Mistakes make messages much harder for the decoder to interpret.

Now it's your turn! Work out the exercises below. (You'll find answers at the back of this book.)

Exercises

1. What is the name given to the following table?

A	H	M	V	L	3	Y	D
X	K	B	5	P	Z	E	O
N	7	W	U	F	T	6	J
G	R	2	Q	C	A	I	S

Use the table in 1 above to answer question 2 – 10.

What will be the cipher for the following?

2. KB
3. HR
4. AR
5. EU
6. COME TO SCHOOL
7. GO HOME THEN

Decode the following messages

8. 73 3N SG YZ 6X
9. SG MN YK A7 JO HD

10. Why is it important the number of letters in the message to be encoded be even?

Answers to Exercises: Playfair Cipher

1. The key
2. B5
3. KH
4. HG
5. 56
6. SP YB JZ GA DK PD
7. XS DK YB 73 X6
8. THAT IS MINE
9. I SAW HER TODAY
10. So as to enable one to apply the three rules when encoding the message