MEDIUM

Challenge
Grandpré cipher

Developed 120 years ago, the Grandpré cipher is not very well known, but easy to use. You and a friend can share short, encrypted messages that are very hard to break without the key.

Grid structure

Traditionally, these grids have dimensions 10 by 10 or 8 by 8. A 9x9 grid is also possible, of course.

In the grid there are ten words written from left to right. These words were chosen so that all 26 letters of the alphabet are represented. An eleventh word runs down the left-hand side, which tells you how to order the ten other words. This word is an isogram, meaning that each letter in the word appears only once in the word. Instead of using an isogram, the person making the grid could choose alphabetical order, or reverse alphabetical order, but these options are less secure.

Here's an example of a Grandpré grid, ready to encipher or decipher a message.

	0	1	2	3	4	5	6	7	8	9
0	A	Q	U	A	P	L	A	N	E	D
1	L	U	M	B	E	R	J	A	C	K
2	G	O	O	G	O	L	P	L	E	X
3	O	R	C	H	E	S	T	R	A	L
4	R	E	M	A	R	K	A	B	L	E
5	I	N	S	I	G	H	T	F	U	L
6	T	R	A	N	S	L	A	T	E	D
7	H	A	Z	E	L	B	R	O	O	K
8	M	I	C	R	O	W	A	V	E	S
9	S	T	A	L	A	C	T	I	T	E

How to use the grid for encryption

Say you want to encrypt the message “Meet me at the cafe at four”.

First, find an M in the grid. There are multiple Ms to choose from. Choose any M that you want and record its coordinates in the grid, by noting the number down the left and the number across the top. There’s an M (second-last letter in the word of ALGORTHIMS) at position 8,0. If you choose this M, the encrypted message begins with 80.

Now you need an E. There are lots to choose from. Say you choose the E in ORCHESTRAL. The coordinates are 3,4, so the next part of the encrypted message will be 34. Now you need another E. It’s best to choose a different E in the grid, to make the most of the benefits of the Grandpre cipher. Similarly, when it comes time to choose a second M for the first letter of ‘me’, it’s best not to choose the M of ALGORTHMS again.

A completed encrypted message could look like:

80 34 88 56 42 14 43 67 60 33 28 18 00 57 73 62 36 57 24 58 76

You might like to arrange the numbers as one long string without spaces or turn them into five-digit groups.

80348856421443676033281800577362365724587 6

Or

80348 85642 14436 76033 28180 05773 62365 72458 76

Decryption

This is a symmetrical cipher, meaning that the decryption process is the mirror of the encryption process.

To decrypt 8189575087418445, the first thing to do it to split the number into pairs like so:
81 89 57 50 87 41 84 45

To decrypt 81, go down to the second-last row (row 8) and across to column one. The letter in that grid position is I.

Continue reading off the coordinates to decrypt the whole message:

IS FIVE OK

Weaknesses of the Grandpré cipher

While the Grandpré cipher is a lot more secure than a monoalphabetic substitution cipher, it is still vulnerable when used for long messages or multiple messages. In other words, it’s safest to use this cipher for short messages, and to use a different key (grid) after a few short messages have been exchanged. This results in the key distribution problem that plagued cryptographers for millennia.

The Challenge

Alice and Bob's key distribution method

Alice and Bob are very conscious of the weaknesses of the Grandpré cipher, so Alice sends a new key to Bob every Monday. They worked out that because the Grandpré cipher's key consists of words that are found in dictionaries, one way to distribute a new key to a correspondent is to hide the words in plain sight in a letter or email. Alice and Bob had an agreement that the final ten-letter word in a sentence or paragraph was part of the key. They also had an agreement that on the first Monday of the month, the ten keywords needed to be arranged alphabetically, on the second Monday, the keywords needed to be arranged in order of appearance in the email, the third Monday, the keywords needed to be arranged reverse alphabetically, the fourth Monday in reverse order of appearance, and in the case where there were five Mondays in the month, the words needed to be arranged by order of an isogram what would appear in an eleventh paragraph of the letter.

On the third Monday of the month, Alice sends the following to Bob:

Dear Bob,

I'm sitting in my study, listening to a wattlebird chirping away outside my window. I'm eating jellybeans and thinking about applying for a job. I actually started an application yesterday, but I left it unfinished. A cryptology job at ASD has caught my eye this morning and I am thinking that I will go for it. You might laugh at this because you remember how hopeless I was with quadratics etc back in high school. (Remember that time when Mr Davis threw me out of class because I was shooting some classmates with a peashooter?) But I've grown to love maths in the past five years, and a career in crypt is more interesting than a career as a divemaster. Or than my previous career as a folksinger. Yes, a horizontal move to a new career is what I need at the moment. I can just imagine my excitement when I hear that I've got the job.

Love Alice,

PS 99352 17607 67170 36281 63418 79558 30930 44412 55528 57299 06709 13346
90108 92774 99935 14915 79533 61497 24016 63248 22594 48602 40614 5

Can you decipher Alice's message?

Find the correct ten-letter words:

Word grid

Use the grid below to place the ten-letter words into their correct order.

	0	1	2	3	4	5	6	7	8	9
0										
1										
2										
3										
4										
5										
6										
7										
8										
9										

Ciphertext

As shown in the letter from Alice to Bob. 99352 17607 67170 36281 63418 79558 30930 44412 55528 57299 06709 13346 90108 92774 99935 14915 79533 61497 24016 63248 22594 48602 40614 5

Pairs of numbers :

Plaintext (decrypted message):

Clues and answers can be found on the relevant puzzle page on www.asd.gov.au