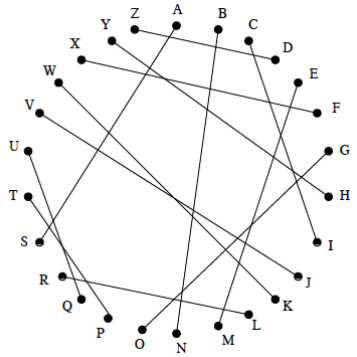
UNIVERSITY OF WATERLOO

Breaking the Vatsyayana Encryption Scheme

The CENTRE for EDUCATION in MATHEMATICS and COMPUTING

This scheme for encrypting secret messages comes from an Indian text from the 4th century AD. The sender and receiver of a message decide in advance on a way to group the letters of the alphabet into pairs. An example of such a pairing is below.



To encrypt a message, the sender replaces each letter of the message with its paired letter. For example, the message `"Silly putty"` is encrypted as `"Acrrh tqpph"`.

To decrypt a message, the receiver replaces each letter with its paired letter. For example the ciphertext `"Cim ilmse asbzkciy"` is decrypted as `"Ice cream sandwich"`.

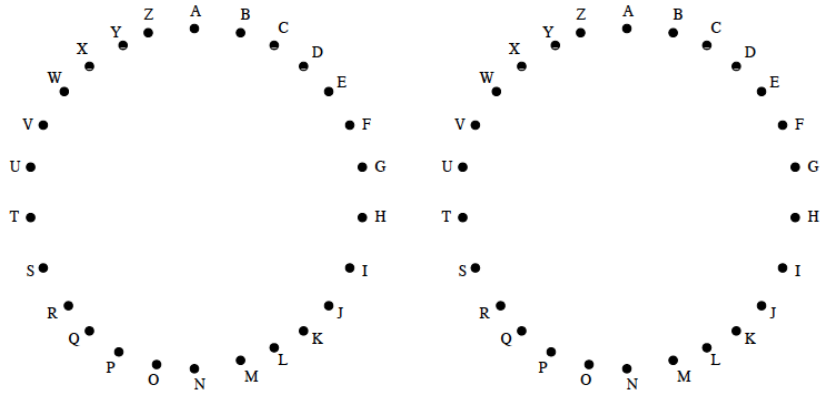
Challenge: Crack the Code

1. Evette and her granddaughter have chosen a different pairing of letters so that they can communicate in secret using the Vatsyayana Encryption Scheme. You intercept a message between them. Can you decrypt it?

```
Mihl Clhzmdh,

Xahzw qvs pvl xai tqrvfavzi hzm xai nijlh fhbhdhu!

Rvoi, Ioixxi.
```



2. How many different ways are there to pair the letters of the English alphabet into 13 pairs?

Connection to the Real World
When your internet browser shows a URL beginning with https, an encryption scheme based on prime numbers is being used to protect your privacy. Mathematics is the foundation of modern cryptography.

Solution:

1. Here are some hints:

   (a) This message is structured like an old-fashioned thank you note. How do these start and end?

   (b) Using this encryption scheme, Evette's name is "Ioixxi".

   (c) Guess at some common 3-letter words to discover some letter pairs.

   (d) Once you are sure of a letter pair, you can decrypt all the instance of those letters.

   We might guess that the first word of the letter is "Dear", and that the letter ends with "Love, Evette". This allows us to pair up D with M, E with I, A with H, R with L, O with V, T with X. Then the partially recovered message looks like

   ```
   Dear ?ra?dma,
   Tha??  ?o?  ?or the ??lo?ho?e a?d the ?e?ra ?a?ama?!
   Love, Evette.
   ```

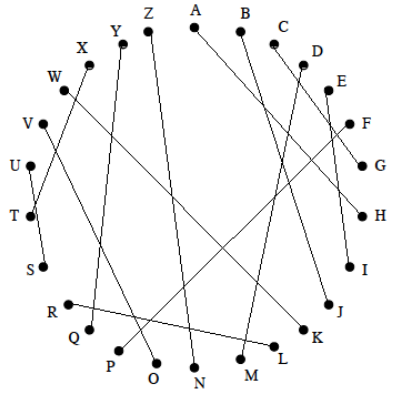
   If we guess that the second word is "Grandma", then we pair C with G and Z with N. We have now recovered:

   ```
   Dear Grandma,
   Than?  ?o?  ?or the ??lo?hone and the ze?ra ?a?ama?!
   Love, Evette.
   ```

   By guessing or consulting a dictionary, we can guess that the message contains the word "zebra", pairing B with J. We have now recovered:

   ```
   Dear Grandma,
   Than?  ?o?  ?or the ??lo?hone and the zebra ?ajama?!
   Love, Evette.
   ```

   There are a limited number of letters to end the word "Than?" so we might guess that K is paired with W. The pairing of letters is given below. Some guessing of the remaining letter pairs and possible words would lead us to the solution.



   The decrypted message is:

   ```
   Dear Grandma,
   Thank you for the xylophone and the zebra pajamas!
   Love, Evette.
   ```

2. There are $\frac{26!}{13!2^{13}}$ ways to pair the alphabet into 13 pairs.

Consider expressing the pairings by a list of the twenty-six letters, where the first and second letters are paired, as are the third and fourth letters, and so on.

For example, the list A G B Q C I D M E J F O H W K R L V N S P T U X Y Z
represents pairing A with G, B with Q, etc. as in the chart.

There are 26! ways to list the twenty-six letters, but many of these lists will represent equivalent pairings of letters.
We get equivalent pairings by listing any pair in the opposite order (reversing the 1st and 2nd letters, or 3rd and 4th letters, etc. There are 2^{13} ways to do this. For example, the list
A G B Q C I D M E J F O H W K R L V N S P T U X Y Z
is equivalent to the list
G A B Q I C D M E J F O H W K R L V N S P T U X Y Z. Each of the 13 pairs may have its order reversed, independently of one another, to give an different list representing the same pairing.
We also get an equivalent pairing by listing the 13 pairs in a different order, and there are 13! ways to do this. For example, the list
A G B Q C I D M E J F O H W K R L V N S P T U X Y Z
is equivalent to the list
F O B Q C I D M A G E J H W K R L V N S P T U X Y Z.