**CIPHERS**

VIGENERE CIPHER

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Q. Encrypt the message “MAKE IT HAPPEN” using the keyword “MATH”.

STEPS

1. Write down the position of each letter in the keyword.

M A T H

12 0 19 7

1. Repeat the number sequence ( 12 0 19 7 in this case) under the message.

M A K E I T H A P P E N

12 0 19 7 12 0 19 7 12 0 19 7

1. Add the position of letters to their corresponding numbers and then write down the new letters with the position (resultant value)%25 in the same order.

For example, the first letter M has position 12 and the corresponding number as 12. 12+12 = 24.

24%25 = 24 which is the position of Y. So M is replaced by Y in the encrypted message.

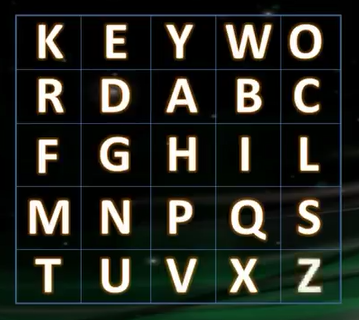
Continue in this manner to get the encrypted message.

1. The final encrypted message is YADL UT AHBPX.

PLAYFAIR CIPHER

STEPS

1. First choose a keyword with no repeating letters (for example, the keyword will be keyword).
2. We will create a 5x5 matrix



Fill the 5x5 matrix by writing the keyword (KEYWORD in this case) first followed by the rest of the alphabet (excluding J).

1. Let the message to be encrypted be “secret message”.
2. Split the message into pairs of letters.

* Separate repeated letters by inserting the letter X.
* If there is an odd letter at the end of the message, insert the letter X.
* Ignore all spaces.

The final result will be

SE CR ET ME SX SA GE

1. Find each pair of letters in the table we had prepared earlier.

* If the letters are in the same column, prepare the cipher text by writing down the letters just below the corresponding letters in the same order.

If the end of table is reached, wrap around.

* If the letters are in the same row, write down the letters to the right of the corresponding letters.

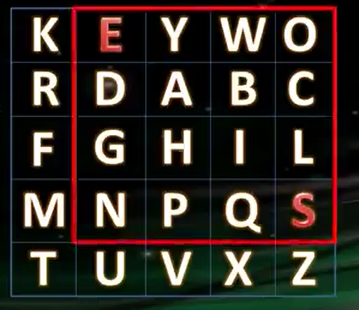
If the end of table is reached, wrap around.

* If the letters are neither in the same row or in the same column, draw a rectangle in which the letters are in the opposite corners. Move horizontally and write down the letters on the other end in the same order.

ENCRYPTING THE MESSAGE

Taking the first pair of letters

**SE** CR ET ME SX SA GE

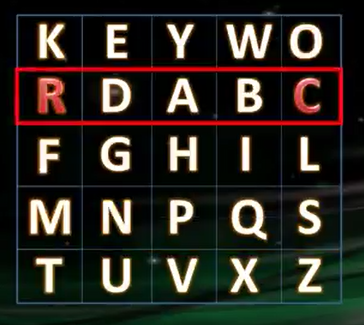


Here, the letters S and E form the opposite corners of a rectangle. Starting with S, we move horizontally and write down the letter at the other end of the table. Hence, S becomes N in cipher text.

In the same manner, E becomes O.

Therefore, SE becomes NO.

SE **CR** ET ME SX SA GE



Here, the letters C and R are in the same row. The letter to the right of C is R.

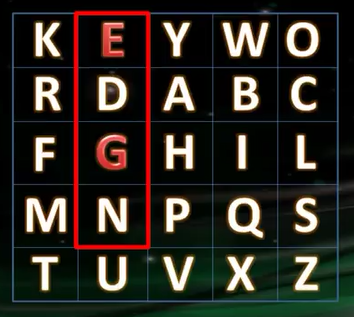
Therefore, C becomes R.

And R becomes D.

So, CR becomes RD.

Encrypt the message in this way until you reach the last pair of letters.

SE CR ET ME SX SA **GE**



Move down vertically and write down the letter immediately below the chosen letter.

G becomes N.

E becomes D.

GE becomes ND.

The final encrypted message is NORDKUNKQZPCND.

DISADVANTAGE OF VIGENERE CIPHER

If a cryptanalyst correctly guesses the length of the key, the cipher text will just be a combination of individual Caesar ciphers which can be easily broken individually.The cipher was first broken by Charles Babbage and later by Kasiski, who published the technique he used. In 1920, the famous American Army cryptographer William F. Friedman developed the so-called Friedman test (a.k.a. the Kappa test). Both Friedman and Kasiski have developed mathematical methods to find out the length of the key.

DISADVANTAGE OF PLAYFAIR CIPHER

All occurrences of the same pair of letters (for eg, NO) in a cipher text will have the same plain text (SE in this case).

An interesting weakness is the fact that the ciphertext (AB) and its reverse (BA) will have corresponding plaintexts like UR and RU (and also ciphertext UR and RU will correspond to plaintext AB and BA, i.e. the substitution is self-inverse). That can easily be exploited with the aid of frequency analysis, if the language of the plaintext is known.

*Will chaining Playfair with a substitution cipher help?* Nope... The (monoalphabetic) substitution cipher will act (almost completely) transparent against the frequency attack. Eventually, the Playfair cipher is a digraph substitution cipher itself. (But it will make the resulting cipher not self-inverse anymore.)

Well, polyalphabetic ciphers are a whole different case of course. It's still a play-toy for today's computers, but it'd completely render the text unbreakable in that era. But then again, we needed machines like Enigma to properly and acceptably implement it. The German Enigma implemented a polyalphabetic cipher.

OTHER CIPHERS

ROT1

Each letter of the alphabet is replaced with the following letter, so A is replaced with B, B with C and so on.”ROT1” literally means rotate 1 letter forward through the alphabet. The message “GOOD MORNING” becomes “HPPE NPSOJOH” and so on. The cipher is easy to understand and use and it is equally easy to decipher also.

TRUE CODES

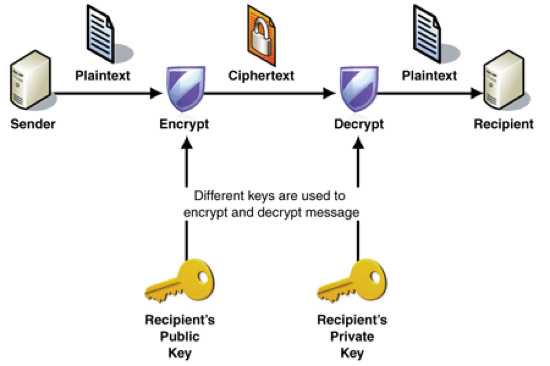
In a true code, each word is replaced by a code word or number according to a key. Since there are many words that might be in the message, the key is usually a code book where someone can look up an English word and find the corresponding code word, not unlike a dictionary. Just as short messages are difficult to decipher with letter frequency analysis, a code needs to be extraordinarily long before word frequency analysis becomes useful, so codes are harder to decode than ciphers. Many countries have used variants of codes, where each day a new code was used to keep them safe from word frequency analysis. For everyday life, however, codes are slow and making a code book is cumbersome. Worse, if the code book is stolen, then the code is no longer safe and a new one must be made, taking a tremendous amount of time and effort. Codes are mainly useful to the rich and powerful who can delegate this work to others.

ENIGMA CODE



The Enigma code, which was a very sophisticated cipher, was used during the Second World War by the Germans. It involved an Enigma machine, similar to a typewriter, where pressing a letter would make the cipher letter light up on a screen. The Enigma machine involved several wheels which connected letters with wires, determining which cipher letter would light up. All Enigma machines were identical, and knowing the initial configuration of the wheels inside was the key to enciphering messages. To make things harder, each wheel would rotate after a certain number of letters were typed, so the cipher was continuously changing within a message. German commanders had Enigma machines and would be issued lists of the initial wheel configuration to use for each day so that all the Germans used the same one and could decipher each other’s messages. Even when the Allies procured a copy of the Enigma machine they could not decipher anything, as there were over one hundred trillion possible wheel configurations to check. The Enigma code was broken by Polish ingenuity and perfected by the British using geniuses and computers. Knowledge of the German communications gave the Allies a vital advantage in the War, and from breaking the Enigma code, the ancestor of modern computers was born.

PUBLIC KEY CRYPTOGRAPHY



This is the ultimate modern cipher, and it has several variants. This cipher, used world-wide, has two keys: one public and one private. The public key is a large number available to everyone. The number is special in that only two whole numbers (apart from 1 and the number itself) will divide into it perfectly. These two numbers are the private key, and if multiplied together, produce the public key. So the public key might be 1961, and the private key 37 and 53. The public key is used to encipher a message, but it is impossible to decipher without the private key. When you email personal details to a bank, or when your bank card is read by a machine, the details are enciphered this way and only the bank can access them with their private key. The reason this is so secure is that mathematically it is very difficult to find divisors of large numbers. To help security, until recently RSA Laboratories gave money to anyone who could find the two divisors of the numbers they gave. For a relatively easy example, once worth $1000 USD, try to find the two 50-digit divisors of 1522605027922533360535618378132637429718068114961  
380688657908494580122963258952897654000350692006139.