PlayFair Cipher

Commands

1. go (It takes us near the boulder having some symbols)
2. go (It takes us to the glass panel near the door)
3. read (To read the encrypted text on the glass panel)

Another set of command will also work: go, back, read.

Cryptosystem

1. Morse Code (to decoding symbols on boulders)
2. Playfair Cipher (to decrypt the cipher text on glass panel)

Analysis

After noticing funny patterns on one of the distant boulder, we used command "go" to reach near that boulder. We observed that it has some symbols like dash (-) and dot (.) . These symbols were like some code. After analyzing the symbols, we get to know that message on the boulder was encoded using "Morse Code".
We decoded it and get to know that the word was "SECURITY". While respecting the spirit of Cave Man by bowing down, we heard a faint voice stating, "You have been blessed, my child. Keep in mind that you must always believe in yourself and PLAY FAIR".
After listening the word PLAY FAIR at the last in his statement, we guessed that there maybe PLAY FAIR cipher used. And as we know that encryption using PLAY FAIR cipher requires a key and the word SECURITY we get was pointing as the key of this PLAY FAIR cipher. This strengthen our guess. Now, we moved towards the glass panel using command "go" and used command "read" to get the message on the glass panel. We applied PLAY FAIR cipher with key as SECURITY to decrypt the message and successfully got the sensible plain text. This concluded that the cryptosystem used was "PLAY FAIR" cipher.

Decryption algorithm

PLAY FAIR cipher decryption algorithm was used. The algorithm is as follows :

1. **Create 5 x 5 key square** : Key square is a 5 x 5 grid containing 25 unique alphabets. The initial entries of grid must be the alphabets of the key (SECURITY) in the order as they are present in the key. Rest entries of the grid should be filled with remaining letters of alphabets in alphabetical order keeping in mind that no letter should repeat. Also we do not include one letter, generally J, in the grid.

$$\begin{pmatrix} S & E & C & U & R \\ I & T & Y & A & B \\ D & F & G & H & K \\ L & M & N & O & P \\ Q & V & W & X & Z \end{pmatrix}$$

2. Remove all other character/symbols/digits which are not present in key square from the Cipher text.
3. Form the pair of two letters (digraphs). Usually Cipher text has even number of letters.
4. Rules to decrypt :
    - Take a pair of letter and check if the letters are in same row in the grid (Key square). Replace each letter with its immediate left letter from the grid. If the letter is present in leftmost position, then, replace it with rightmost letter of that row.

- Take a pair of letter and check if the letters are in same column in the grid (Key square). Replace each letter with its immediate above letter from the grid. If the letter is present at the top, then, replace it with bottom letter of that column.
- If the letters of pair are present in different row and different column, then form a rectangle with the letters such that they appear on the corners. Now, replace each letter with the letter present at opposite corner on the SAME row of the rectangle.

5. Now observe the decrypted text and remove unnecessary X's , because these X are inserted at the time of encryption due to occurrence of same letters in a pair (digraphs) of plaintext. Also, replace letter 'I' with 'J' if it is not making sensible word because we usually omit 'J' at the time of generating Key square and replace 'J' present in plain text with the letter 'I'. Example : words like WILXL ⇒ WILL, NEXED ⇒ NEED etc. and IOY ⇒ JOY in our deciphered text.

After applying the above algorithm manually, deciphered plaintext is : BE WARY OF THE NEXT CHAMBER, THERE IS VERY LITTLE JOY THERE. SPEAK OUT THE PASSWORD "OPEN_SESAME" TO GO THROUGH. MAY YOU HAVE THE STRENGTH FOR THE NEXT CHAMBER. TO FIND THE EXIT YOU FIRST WILL NEED TO UTTER MAGIC WORDS THERE.

Password

OPEN_SESAME