

**Q1. What is the main idea behind the Playfair cipher?**

Using a 5x5 letter matrix for encryption

Shifting letters by a fixed key

Replacing letters with numbers

Using prime numbers for key generation

**Answer:** Using a 5x5 letter matrix for encryption

**Explanation:** Playfair cipher encrypts pairs of letters using a 5x5 matrix constructed from a keyword.

**Q2. If you have the keyword 'MONARCHY', how do you construct the matrix?**

Fill matrix row-wise with keyword letters, then remaining alphabet (I/J combined)

Write keyword vertically, then horizontally

Random letters excluding keyword

Use only vowels from keyword

**Answer:** Fill matrix row-wise with keyword letters, then remaining alphabet (I/J combined)

**Explanation:** You place the unique letters of the keyword first, then fill remaining spots with other letters (I and J share a cell).

**Q3. Why are the letters I and J combined in the Playfair cipher matrix?**

Because Playfair uses a 25-letter matrix

To make encryption faster

To confuse attackers

To avoid vowels

**Answer:** Because Playfair uses a 25-letter matrix

**Explanation:** English alphabet has 26 letters but the 5x5 matrix has only 25 cells, so I and J are combined.

**Q4. How do you encrypt a pair of identical letters in Playfair cipher?**

Insert an 'X' between them

Skip the second letter

Use a different matrix

Replace with numbers

**Answer:** Insert an 'X' between them

**Explanation:** Identical letters in a pair are separated by adding an 'X' to prevent confusion in encryption.

**Q5. Explain what happens if a pair of letters are in the same row of the matrix during encryption.**

Each letter is replaced by the letter to its right, wrapping around

They remain unchanged

Each letter is replaced by the letter below it

Each letter is swapped

**Answer:** Each letter is replaced by the letter to its right, wrapping around

**Explanation:** If both letters are in the same row, you replace each with the letter immediately to the right, cycling back to the start if needed.

**Q6. What if the letters are in the same column?**

Replace each letter with the letter below it, wrapping to top

Replace each letter with the letter to its right

Replace with letters in diagonal

Leave them unchanged

**Answer:** Replace each letter with the letter below it, wrapping to top

**Explanation:** If letters share a column, each is replaced by the letter below it in that column, wrapping to the top if at the bottom.

**Q7. If letters form a rectangle in the matrix, how do you encrypt them?**

Each letter is replaced by the letter in its row but the other letter's column

Swap the letters

Use a random letter

Skip encryption

**Answer:** Each letter is replaced by the letter in its row but the other letter's column

**Explanation:** Letters at rectangle corners swap columns but keep their own row during encryption.

**Q8. Why is Playfair considered more secure than Caesar cipher?**

Because it encrypts digraphs instead of single letters

Because it uses a larger key

Because it uses numbers

Because it is a hash function

**Answer:** Because it encrypts digraphs instead of single letters

**Explanation:** Encrypting letter pairs (digraphs) hides letter frequency patterns better than single-letter substitution.

**Q9. How does Playfair cipher handle letters that don't form a pair, like a single leftover letter?**

Add an 'X' or 'Z' to complete the pair

Ignore the leftover letter

Encrypt only the leftover letter

Double the leftover letter

**Answer:** Add an 'X' or 'Z' to complete the pair

**Explanation:** If the message length is odd, an extra filler letter like 'X' is added to make pairs complete.

**Q10. Can Playfair cipher be broken easily? How?**

It's more complex but still vulnerable to frequency analysis of digraphs

No, it is unbreakable

Only with quantum computers

By guessing the key directly

**Answer:** It's more complex but still vulnerable to frequency analysis of digraphs

**Explanation:** While harder than Caesar, Playfair is still breakable with enough ciphertext and analysis of digraph frequency.

**Q11. What would be a typical first step to decrypt a Playfair cipher if the key is unknown?**

Try possible keywords or use frequency analysis of digraphs

Try all possible shifts like Caesar cipher

Use a dictionary attack on single letters

Decrypt using a hash function

**Answer:** Try possible keywords or use frequency analysis of digraphs

**Explanation:** Attackers attempt to guess the keyword or analyze common digraphs to break the cipher.

**Q12. Why does the Playfair cipher ignore the letter 'J' or combine it with 'I'?**

To fit the alphabet into a 5x5 matrix

To make the cipher more secure

Because 'J' is a vowel

To confuse attackers

**Answer:** To fit the alphabet into a 5x5 matrix

**Explanation:** The matrix is  $5 \times 5 = 25$  cells, so one letter must be merged or excluded, usually 'I' and 'J' are combined.

**Q13. What happens if the keyword contains repeated letters in Playfair cipher?**

Only the first occurrence is used in the matrix

All repeated letters are included

The keyword is rejected

Repeated letters are replaced with numbers

**Answer:** Only the first occurrence is used in the matrix

**Explanation:** Duplicate letters in the keyword are ignored when constructing the matrix to keep letters unique.

**Q14. Explain why Playfair cipher is categorized as a digraph substitution cipher.**

Because it encrypts letters in pairs (digraphs)

Because it uses a  $2 \times 2$  matrix

Because it substitutes digits for letters

Because it uses two keys

**Answer:** Because it encrypts letters in pairs (digraphs)

**Explanation:** Playfair encrypts pairs of letters at a time, rather than one letter individually.