Cryptography and Network Security - Answer Sheet (All Correct)

1. The Hill cipher encrypts plaintext by multiplying it with an invertible key matrix.

2. The key for Vigenère cipher can be found by analyzing repeating patterns in the ciphertext.

3. The Playfair cipher matrix is constructed using a keyword, excluding 'J'.

4. Decryption in the Playfair cipher follows the reverse of the encryption process.

5. The Caesar cipher shifts each letter by a fixed number (e.g., k = 3 shifts A to D).

6. The Hill cipher encryption process involves matrix multiplication using a key matrix.

7. Additive cipher adds a fixed key value to each letter and decryption subtracts it.

8. Monoalphabetic ciphers use a single alphabet substitution throughout encryption.

9. Polyalphabetic ciphers use multiple shifting alphabets for encryption, making them harder to break.

10. Rail fence cipher arranges text in a zigzag pattern before reading row-wise.

11. Playfair cipher encrypts pairs of letters using a 5x5 matrix constructed from a keyword.

12. Hill cipher encryption is done using matrix multiplication with modular arithmetic.

13. Autokey cipher appends the plaintext to the key for encryption, improving security.

14. Columnar transposition cipher arranges text into a grid and reads column-wise according to the key.

15. Encrypting with both Caesar and transposition ciphers enhances security by combining substitution and permutation.

16. Substitution and transposition ciphers were widely used in World War II, especially in the Enigma machine.

17. Frequency analysis and Kasiski examination are techniques to break substitution and polyalphabetic ciphers.