Cryptography and Network Security - Answer Sheet (Partial Correct)

1. The Hill cipher uses matrix multiplication to encrypt plaintext.

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 is done using the same encryption rules in reverse.

5. The Caesar cipher shifts each letter by a fixed number (incorrect: shift value is 5).

6. The Hill cipher encryption process involves matrix multiplication (incorrect: key matrix is not invertible).

7. Additive cipher adds a fixed key value to each letter.

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

9. Polyalphabetic ciphers use multiple shifting alphabets for encryption (incorrect: they use a single key).

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.

12. Hill cipher encryption is done using matrix multiplication.

13. Autokey cipher appends the plaintext to the key for encryption.

14. Columnar transposition cipher arranges text into a grid and reads column-wise.

15. Encrypting with Caesar and transposition ciphers results in a more secure ciphertext.

16. Substitution ciphers were widely used in World War II (incorrect: they were only used in early wars).

17. Frequency analysis is used to break substitution ciphers, but not polyalphabetic ciphers (incorrect).