Q1. What is the Hill Cipher primarily based on?

Substitution of letters
Matrix multiplication
Frequency analysis
Bitwise operations
Answer: Matrix multiplication
Explanation: Hill Cipher uses linear algebra concepts like matrix multiplication over mod 26 to encrypt plaintext.

Q2. What must the key matrix of Hill Cipher be for successful decryption?

Singular matrix
Invertible matrix mod 26
Zero matrix
Diagonal matrix
Answer: Invertible matrix mod 26
Explanation: The key matrix must have an inverse modulo 26 for decryption to be possible.

Q3. What happens if the key matrix is not invertible mod 26?

Encryption is impossible
Decryption is impossible
Both encryption and decryption fail
No effect on cipher
Answer: Decryption is impossible
Explanation: Without an inverse key matrix modulo 26, you cannot decrypt the ciphertext.

Q4. Hill Cipher operates on blocks of letters. What is the typical block size?

1
2 or more
3 only
5
Answer: 2 or more
Explanation: Hill Cipher processes plaintext in blocks (vectors) of size equal to the key matrix dimension (usually 2x2 or 3x3).

Q5. Which of these is a common modulus used in Hill Cipher?
26
128
256
100
Answer: 26
Explanation: Mod 26 corresponds to the number of letters in the English alphabet.

Q6. How is plaintext represented mathematically in Hill Cipher?
As numbers mod 26
As ASCII values
As binary bits
As decimal digits
Answer: As numbers mod 26
Explanation: Each letter is converted to a number between 0 and 25 to work with modulo arithmetic.

Q7. If the key matrix is 3x3, how many letters are encrypted at once?
1
2
3
4
Answer: 3
Explanation: The block size matches the key matrix dimension, so 3 letters are encrypted together.

Q8. What type of cipher is Hill Cipher considered?
Substitution cipher
Transposition cipher
Polyalphabetic substitution cipher
Hash function
Answer: Polyalphabetic substitution cipher
Explanation: Hill Cipher replaces blocks of letters with other blocks using matrix multiplication, making it polyalphabetic.

Q9. Which property of matrices is crucial for the Hill Cipher key matrix?
Determinant must be 0

Determinant must be 1
Determinant must be coprime with 26
Determinant must be negative
Answer: Determinant must be coprime with 26
Explanation: The determinant must be invertible mod 26, meaning it must be coprime with 26.

Q10. Why is Hill Cipher more secure than Caesar Cipher?
Uses larger key space with matrices
Only shifts letters by one
Encrypts letters independently
Uses symmetric keys
Answer: Uses larger key space with matrices
Explanation: Hill Cipher's use of matrix keys and block encryption increases complexity and resists simple frequency analysis.

Q11. What is the decryption key in Hill Cipher?
The transpose of the key matrix
The inverse of the key matrix modulo 26
The negative of the key matrix
The same as encryption key
Answer: The inverse of the key matrix modulo 26
Explanation: Decryption involves multiplying by the inverse key matrix modulo 26.

Q12. Can Hill Cipher encrypt messages of arbitrary length directly?
Yes, without padding
No, it requires padding to fill blocks
Only if length is prime
Only if length is even
Answer: No, it requires padding to fill blocks
Explanation: Plaintext length must be a multiple of the block size, so padding is used if necessary.

Q13. What kind of mathematical object is used as the key in Hill Cipher?
Vector
Matrix
Scalar

Polynomial
Answer: Matrix
Explanation: The key is a square matrix used for linear transformations of plaintext blocks.

Q14. Is Hill Cipher a symmetric or asymmetric cipher?
Symmetric, uses same key for encryption and decryption
Asymmetric, uses different keys
Symmetric, but keys are public
Asymmetric, based on matrix factorization
Answer: Symmetric, uses same key for encryption and decryption
Explanation: Hill Cipher is symmetric since encryption and decryption use the same key matrix and its inverse.

Q15. Why can Hill Cipher be vulnerable if the key matrix is small?
Small keys are slow to compute
Small matrices make brute force feasible
They cannot be inverted
They encrypt less text
Answer: Small matrices make brute force feasible
Explanation: Small key sizes reduce complexity, making it easier to attack via brute force or known-plaintext attacks.