ASSIGNMENT 4

1. Distinguish the following techniques: Caesar, hill, row-column transportation, Rail fence, Affine and monoalphabetic ciphers.

2. Given the encryption function E(x) = 67x + 50 mod 128. Find the decryption function. By referring to ASCII table(128), encrypt: It is not allowed to come in class. Decrypt your result to verify the accuracy of the algorithm.

3. Given the key matrix, K = $[10\ 9\ 7\ 12]$ mod 128. Find the decryption key. By referring to ASCII table(128) encrypt: “Rwanda is Rwandaful”. Decrypt the ciphertext to verify the accuracy of the algorithm.

Solution

Substitution Techniques

Caesar Cipher

- **Type:** Simple substitution (shift by fixed number).
- **Similarity:** Uses fixed letter-to-letter substitution.
- **Weakness:** Only 25 keys => trivially brute-forced.

Monoalphabetic Cipher

- **Type:** General substitution (arbitrary mapping).
- **Similarity:** Still 1-to-1 letter mapping like Caesar.
- **Weakness:** Vulnerable to **frequency analysis** despite huge keyspace.

Hill Cipher

- **Type:** Polygraphic substitution using matrix multiplication over mod 26.
- **Similarity:** Still substitution, but on **blocks** of letters.
- **Weakness:** If the matrix is small (2×2 or 3×3), it can be cracked via **known-plaintext attacks** and linear algebra; completely breaks if ciphertext-only but enough statistics exist.

Affine Cipher

- **Type:** Algebraic substitution (a*x + b mod 26).
- **Similarity:** Like Caesar but with multiplication + addition.
- **Weakness:** Only 12 possible “a” values => small keyspace; easily broken with frequency analysis.

Transposition Techniques

Rail Fence Cipher

- **Type:** Simple transposition using zig-zag pattern.
- **Similarity:** No letter substitution - only rearranges characters.
- **Weakness:** Very low security; few key options; patterns easily detectable.

Row-Column Transposition Cipher

- **Type:** Rearrangement via writing in rows and reading by columns (or vice versa).
- **Similarity:** Pure transposition like Rail Fence.
- **Weakness:** More secure than Rail Fence but still vulnerable to **anagramming** and pattern attacks.

Summary Table

Cipher	Type	Keyspace	Vulnerability
Caesar	Substitution	Very small	Brute-force
Monoalphabetic	Substitution	Large	Frequency analysis
Affine	Substitution	Small	Frequency + algebraic attacks
Hill	Polygraphic substitution	Medium	Linear algebra attacks
Rail Fence	Transposition	Very small	Pattern detection
Row-Column	Transposition	Moderate	Anagramming / pattern