Amrita Vishwa Vidyapeetham, Amritapuri

Department of Computer Science and Engineering

22AIE314 Computer Security

Lab Sheet 1

Classical Encryption Methods

1. Implement Caesar cipher.
   a) Given plaintext "DEFEND THE EAST WALL" and a shift key 3, encrypt the message using the Caesar Cipher.
   b) Decrypt the given ciphertext "WKH HDJOH LV LQ SODFH" assuming shift key 3.
2. Implement Monoalphabetic Cipher
   a) Encrypt the plaintext "HELLO WORLD" using a random substitution key.
   b) Decrypt the given ciphertext "XUBBE MEHBT" using the provided key mapping: {H: X, E: U, L: B, O: E, W: M, R: H, D: T}.
3. Implement Playfair Cipher.
   a) Encrypt the plaintext "MEET ME AT THE PARK" using the Playfair Cipher with key "SECURITY".
   b) Decrypt the given ciphertext "GATLMZ CLRSPB" assuming the same Playfair key.
4. Implement Hill Cipher (Use a 3x3 matrix for encryption)
   a) Encrypt the plaintext "ACT" using a 3x3 key matrix:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

   b) Decrypt the ciphertext "POH" using the inverse of the given key matrix.

5. Implement Polyalphabetic Cipher (Vigenère Cipher) -Use a repeating key to encrypt the message.
   a) Encrypt the plaintext "ATTACK AT DAWN" using the key "LEMON".
   b) Decrypt the ciphertext "LXFOPV EF RNHR" using the same key.
6. Implement One-Time Pad Cipher
   a) Encrypt the plaintext "HELLO" using the one-time pad key "XMCKL".
   b) Decrypt the ciphertext "EQNVZ" using the same key