**1. Assume an attacker knows that a user's password is either abcd or bedg. Say the user encrypts his password using the shift cipher, and the attacker sees the resulting ciphertext. Show how the attacker can determine the user's password, or explain why this is not possible.**

> According to shift cipher, all letters are shifted by k places. Therefore, if the resulting ciphertext is in alphabetical order, the password is *abcd*. Otherwise, the password is *bedg*.

**2. The shift, substitution, and Vigenere ciphers can also be defined over the 128-character ASCII alphabet (rather than the 26-character English alphabet). Provide a formal definition of each of these schemes in this case.**

> **Shift:**
>
> Encryption of the message $m = m_1 \cdots m_l$ (Where $m_i \in \{0, \ldots, 127\}$) using key $k$ is given by
>
> $$Enc_k(m_1 \cdots m_l) = c_1 \cdots c_l, \text{where } c_i = [(m_i + k) \bmod 128]. \tag{1}$$
>
> Decrytion of a ciphertext $c = c_1 \cdots c_l$ using key $k$ is given by
>
> $$Dec_k(c_1 \cdots c_l) = m_1 \cdots m_l, \text{where } m_i = [(c_i - k) \bmod 128]. \tag{2}$$
>
> **Substitution:**
>
> Given a permutation $k$ of length 128 that maps character to other character and can be reversed. For example, $map_k(a) = X$ and $map_k(X) = a$.
>
> Encryption of the message $m = m_1 \cdots m_l$ (Where $m_i \in \{0, \ldots, 127\}$) using key $k$ is given by
>
> $$Enc_k(m_1 \cdots m_l) = c_1 \cdots c_l, \text{where } c_i = map_k(m_i). \tag{3}$$
>
> Decrytion of a ciphertext $c = c_1 \cdots c_l$ using key $k$ is given by
>
> $$Dec_k(c_1 \cdots c_l) = m_1 \cdots m_l, \text{where } m_i = map_k(c_i). \tag{4}$$
>
> **Vigenere:**
>
> Assume $Dis(a, b)$ is the distance between character $b$ and $a$. For example, $Dis(a, c) = 2$.
>
> Encryption of the message $m = m_1 \cdots m_l$ (Where $m_i \in \{0, \ldots, 127\}$) using key $k = k_1 \cdots k_l$ is given by
>
> $$Enc_k(m_1 \cdots m_l) = c_1 \cdots c_l, \text{where } c_i = [(m_i + Dis(k_i, a)) \bmod 128]. \tag{5}$$
>
> Decrytion of a ciphertext $c = c_1 \cdots c_l$ using key $k$ is given by
>
> $$Dec_k(c_1 \cdots c_l) = m_1 \cdots m_l, \text{where } m_i = [(c_i - Dis(k_i, a)) \bmod 128]. \tag{6}$$

**3. Encrypt the message "cryptography" using the Vigenere cipher with the key "google" (repeated).**

> *Shift for g: 6*
>
> *Shift for o: 14*

> *Shift for l: 11*
>
> *Shift for e: 4*
>
> Result is "IFMVESMFOVSC".