|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | Shift Cipher  **History and Description**  In the first century B.C., Julius Caesar developed the shift cipher. Based on a shift key, each letter in the alphabet is replaced by the new shifted letter. The message which is enciphered by replacing the corresponding new letter is called plaintext, and the new message which is produced by the substitution is called ciphertext. The key gives the number of letters the alphabet is shifted between plaintext and ciphertext.  **Example**  **Encipher** Given: The shift key is 5 Plaintext: I AM A STUDENT  The corresponding ciphertext letter is computed for each letter in the plaintext as follows I + Shift(5) = N  A + Shift(5) = F M + Shift(5) = R  A + Shift(5) = F  S + Shift(5) = X T + Shift(5) = Y U + Shift(5) = Z D + Shift(5) = I E + Shift(5) = J N + Shift(5) = S T + Shift(5) = Y  Therefore, the ciphertext is NFRFXYZIJSY.  **Decipher** We decipher NFRFXYZIJSY. by computing the corresponding plaintext letter for each letter in the ciphertext as follows N - Shift(5) = I  F - Shift(5) = A R - Shift(5) = M  F - Shift(5) = A  X - Shift(5) = S Y Shift(5) = T Z - Shift(5) = U I - Shift(5) = D J - Shift(5) = E S - Shift(5) = N Y - Shift(5) = T  Therefore, the plaintext is IAMASTUDENT.  **Disadvantages**  As there are 26 letters in alphabet, each letter can be shifted up to 25 places. To break the ciphertext, we can list all the possible plaintext and choose the most reasonable message.  For example, if we have the ciphertext which is NFRFXYZIJSY, possible corresponding plaintexts are:   |  |  | | --- | --- | | **Shift** | **Plaintext** | | 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 | MEQEWXYHIRX LDPDVWXGHQW KCOCUVWFGPV JBNBTUVEFOU IAMASTUDENT HZLZRSTCDMS GYKYQRSBCLR FXJXPQRABKQ EWIWOPQZAJP DVHVNOPYZIO CUGUMNOXYHN BTFTLMNWXGM ASESKLMVWFL ZRDRJKLUVEK YQCQIJKTUDJ XPBPHIJSTCI WOAOGHIRSBH VNZNFGHQRAG UMYMEFGPQZF TLXLDEFOPYE SKWKCDENOXD RJVJBCDMNWC QIUIABCLMVB PHTHZABKLUA OGSGYZAJKTZ |   By locating the only reasonable message, we can decide that the shift key is 5 and the plaintext is IAMASTUDENT. | |
|  |