RATERTA, NOEL JR, C.
T143
BSIT-3A

So each letter of the alphabet is consistently replaced by another letter. In my code, I created a mapping based on (frequency table) that defines how each letter corresponds to another.

**Limitation of the Substitution Cipher**

- **Letter Frequency** - In any given language, certain letters appear more frequently than others. For example, in English, letters like 'E', 'T', 'A', and 'O' are among the most common.
- **Common Words and Patterns** - Common words (e.g., "the," "and," "is") and letter patterns (like double letters) can provide clues. For example, if a letter appears twice in a row in the ciphertext, it might represent a double letter like 'LL' or 'EE'.
- **Static Key** - A substitution cipher uses a static key, meaning that the same substitution is applied throughout the entire message.
- **Limited Key Space** - The number of possible keys for a substitution cipher is limited compared to more complex ciphers.
- **Lack of Diffusion** - Substitution ciphers do not provide significant diffusion, meaning that changing one letter in the plaintext will only affect that letter in the ciphertext.
- **Easier to Analyze with Longer Texts** - The longer the text, the more reliable the frequency analysis becomes.

**How Attackers Could Break a Substitution Cipher Using Letter Frequency Analysis**

- **Frequency Counting** - An attacker would start by counting the frequency of each letter in the ciphertext.
- **Comparison with Known Frequencies** - The attacker then compares the frequency of letters in the ciphertext with the known

frequency distribution of letters in the target language (e.g., English).

- **Identifying Common Words** - By looking for common patterns and single-letter words (like 'A' and 'I'), the attacker can start to fill in some of the substitutions.
- **Finding Patterns** - The attacker can look for patterns like common digraphs (two-letter combinations) such as 'TH', 'HE', 'IN', and 'ER'.
- **Trial and Error** - As the attacker builds a partial key through educated guesses, they can test different combinations and refine their key based on the resulting plaintext.
- **Use of Cryptanalysis Tools** - Modern attackers may use software tools that automate frequency analysis and pattern recognition, significantly speeding up the decryption process and making it easier to break simple substitution ciphers.