All Contests > BITS F463 Cryptography PA-1 (2024) > The Enigmatic Heirloom

The Enigmatic Heirloom

Problem Submissions Leaderboard Discussions

In the mysterious world of cryptography, you find yourself immersed in a captivating tale of secrets and legacies. Imagine you are a skilled codebreaker entrusted with unraveling the enigma surrounding an ancient family heirloom – a peculiar encrypted message passed down through generations. The year is 1875, and you receive an urgent letter from a reclusive noble family known for their eccentricities. Lord Archibald Cunningham, the current custodian of the family's ancestral estate, seeks your expertise to decipher a cryptic message discovered in the hidden chambers of the manor. Legend has it that this encrypted message holds the key to a long-lost family treasure, and the fate of the Cunningham lineage rests upon your ability to unlock its secrets. The method used to encrypt the message is a mysterious cipher known as the Baconian cipher, a system with origins shrouded in secrecy. Lord Cunningham, a fervent admirer of cryptography, was known to employ unconventional methods to protect the family's most cherished secrets. As you examine the faded parchment, you realize that only a skilled codebreaker like yourself can uncover the hidden message within. Your task is clear – decode the Baconian cipher and reveal the message that has eluded generations of Cunninghams. The stakes are high, and the clock is ticking. The future of the family's legacy hangs in the balance, awaiting the expert touch of a cryptographer to bring forth the long-buried truth. Delve into the intricate world of Baconian cryptography and let your analytical prowess shine as you strive to unveil the secrets concealed within this ancient artifact. The fate of the Cunningham estate and its legacy lies in your hands.

About the algorithm:

- This algorithm is an example of a substitution cipher. More specifically, it's a type of steganography, where a message is encoded within another message. The algorithm is roughly explained as follows:
- Convert each letter to its binary representation.
- Each binary bit is then substituted with either SecretCharacter1 (SC1) or SecretCharacter2 (SC2), based on its value.
- Refer to this link for a detailed explanation with example.

Input Format

The input consists of 2 lines where:

- 1. The first line contains SC1 followed by SC2, separated by a space.
- 2. The second line contains the ciphertext to be decrypted.

Constraints

- The input string will pertain to the language {SC1, SC2}.
- You are not allowed to use libraries like cryptography available in python.

Output Format

Print the plaintext in uppercase string format.

Sample Input 0

Sample Output 0

CRYPTOGRAPHY

Explanation 0

- In the aforementioned example, SC1 corresponds to 'C' and SC2 corresponds to 'G' respectively. However, for this particular question, any character can be used in their place.
- Employ distinct encoding for each character; for instance, utilize separate values for 'I' and 'J' as specified in the provided link.

