In HIS name

Instructor : Vahid Amin-Ghafari
Ali Sheikh Attar

Cryptography - HW3

➔ **Q1 -** Decrypting Ciphertext Generated Using the Vigenere Cipher:

Decrypting ciphertext generated by the Vigenere cipher requires knowing the key used during encryption. The process involves the following steps:

1. First, identify the length of the key. This can be done using methods like the Kasiski Examination or Frequency Analysis.
2. Once the key length is known, divide the ciphertext into substrings, where each substring corresponds to the letters encrypted by a single letter of the key (stream).
3. Next, treat each substring as being encrypted by a Caesar cipher, which can be decrypted by shifting each letter back by the value corresponding to the letter in the key (or X-Or with key).
4. Apply the reverse shift (subtraction instead of addition or X-or) for each letter, based on the corresponding key letter.
5. Combine the decrypted substrings to reconstruct the original plaintext.

More in-detail explanation:

Look at every 14th character of the ciphertext,
starting with the first
– Call this the first “stream”
• Let some alpha be the most common character appearing in this stream
• Most likely, alpha corresponds to the most common character of the plaintext (i.e., ‘e’)
– Guess that the first character of the key is alpha - ’e’
• Repeat for all other positions
• This is somewhat haphazard … and does not use all the available informationA better attack
• Let pi (0 ≤ i ≤ 25) denote the frequency of the ith English letter in normal English plaintext
– One can compute that alpha some of pi^2 roughly equals to 0.065
• Let qi denote the observed frequency of the ith letter in a given stream of the ciphertext
• If the shift for that stream is j, expect qi+j == pi for all i

– So expect some of pi * qi+j roughly equals to 0.065
    • Test for every value of j to find the right one
– Repeat for each stream

- What if we didn't know the key length:
    • When using the correct key length, the ciphertext frequencies {qi} of any stream will be shifted versions of the {pi}

– So qi2 pi2 0.065
    • When using an incorrect key length, expect (heuristically) that ciphertext letters are uniform

– So qi2 (1/26)2 = 1/26 = 0.038
    • In fact, good enough to find the key length N that maximizes qi2 for some stream

- When the guess key is correct:

– All bytes in the plaintext stream will be between 32 and 126(ascii value)
– Frequency of space character should be high
– Frequencies of lowercase letters (as a fraction of all lowercase letters) should be close to known English-letter frequencies
    • Tabulate observed letter frequencies p'0, …, p'25 (as fraction of all lowercase letters) in the candidate plaintext
    • Should find p'i pi pi2 0.065, where pi corresponds to English-letter frequencies
    • In practice, take B that maximizes p'i pi, subject to caveats above (and possibly others)

➔ **Q2 -** Brute Force Attack:

A brute force attack in cryptography is a trial-and-error method used to decipher encrypted data, such as a password or ciphertext, by exhaustively trying all possible keys or passwords until the correct one is found.

In the context of encryption algorithms like the Vigenere cipher, brute force would involve trying every possible key (with every possible length) until the correct plaintext is discovered. Brute force attacks can be time-consuming and resource-intensive, especially as the length of the key or the complexity of the encryption increases.
The effectiveness of a brute force attack is influenced by factors such as the key length, the size of the keyspace (number of possible key combinations), and the computational power available.