Brian Cullinan

CS 499

10/4/2010

Project 1

1. I took a brute force approach to the first problem. I circulated through all the offsets for 25 letters, then check to see which offset had the most valid words. The first problem was easy to crack because there are only 26 possibilities. I rotated through each offset, and checked the number of valid words. The results were returned instantly.
2. The mono-alphabetic cipher can be solved by calculating the average frequency of characters and word segments found in the English language. For example, “QPS” appears 3 times in the encrypted text, and “PQ” appears once. This will provide a huge advantage to minimizing the possible keys.
3. The Vigenere cipher can be solved in a similar way, using a dictionary and finding frequency of characters. Since the key is only 8 characters and the text is much larger, there will be intersecting segments of words. For example, “TS” is encrypted to “GF”, this makes the exact same step for the two characters, which means the key must be the same letter “N”.
4. Ceasar cipher simply uses a single offset for each character, rotating each character in the text by a certain number of characters.

Mono-alphabetic cipher replaces each letter A through Z with a new letter A through Z. This cipher has 26! possibilities.

Vigenere is similar to Ceasar cipher, but each character of the key provides a new index for rotation. This cipher is vulnerable to statistics using a dictionary.

Vigenere has the largest number of possibilities, making it the strongest cipher. However, all of these ciphers are vulnerable to a dictionary and statistics. The mono-alphabetic cipher also has a very large set of possible keys (4x10^26).

1. The 4-byte RC4 implementation is limited to only being able to encrypt with a small set of keys.

Original message: cs499

Encrypted message: bp4:9

Decrypted message: cs499

