Lei Chen 1206139983

CSE 539 Applied Cryptography HW1

# Block encryption.

The block encryption process is 32-bit based and takes three steps, substitution, XOR with the key and then permutation. The process is described in the following figure.

32 bit data

Substitution

32 bit key

32 bit data

XOR

32 bit data

Permutation

32 bit Cipher data

# Find weakness and try to break

The weakest point of this encryption method is the length of the key, which is only 32 bits. A brute force program running on an average PC can try all the possible keys in a short period of time.

Since the key is short and no chaining mechanism is used, if the plain text is English sentences or any data with particular pattern, the pattern can also be found in the cipher text. And we can use the frequency of each repeated pattern to guess what the pattern means. For example, using my algorithm, “day day day” will be encrypted to a binary data as “C6E9 45BA C6E9 45BA C6E9 45BA”, we can clearly see that “C6E9 45BA” repeats for 3 times.

# Brute Force Decoder.

Since the real brute force decoder need to have the ability to decide whether the decrypted data makes sense, which is not achievable for this project. We will instead assume that we know the plain text and brute force to find the key.

On my computer, based on a relatively short input string, the brute force decoder can find the key in less than 30 min on average. Code can be found at https://github.com/leochen4891/AppliedCryptography539.git