CSE 539 – Homework 1 **Spring 2015**

Author 1: Mukund Manikarnike (1208597425)

Author 2: Lakshmi Srinivas (1208635554)

Introduction

The aim of the homework was to design a cryptographic algorithm. This report contains a description of the approach towards building the algorithm, the details of the algorithm and the brute force attack.

Approach

The approach used towards designing the algorithm is described in the following few points

1. For any encryption algorithm, the desire is
   a. To build an algorithm that with very little change to it can be reversed for decryption provided the key is available.
   b. An algorithm which results in many changes in bits in the cipher text for small changes in bits in the plain text or key.
2. Typically, encryption is done at the byte level no matter what the input is and bitwise operators come into action when we talk of byte-wise operations. This meant that we had to choose bit-wise operators that could be easily reversible.
3. Hence, Circular shift and XOR operations were chosen to build an algorithm which would take the plain text and key as input, circular shift the plain text as a function of the input and XOR it with the key and carry on for multiple rounds.

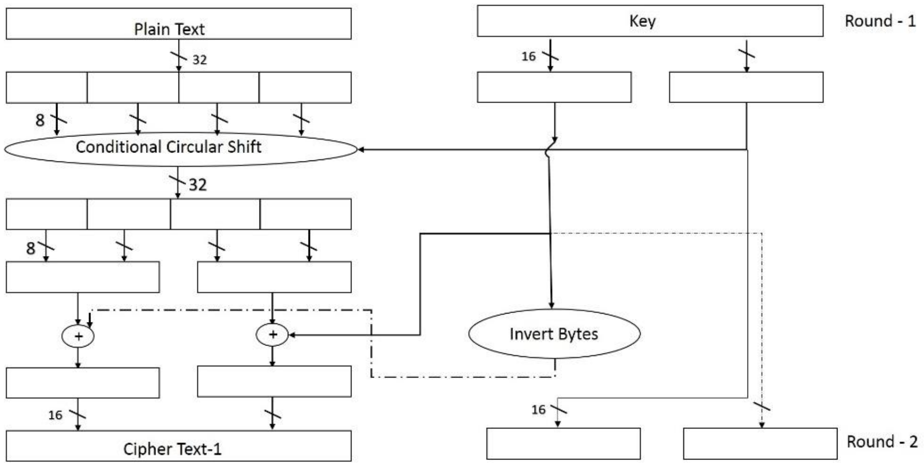
Algorithm

The algorithm consists of 2 phases and 7 rounds, the details of which are explained below.

Description

1. The first phase performs a permutation of the plain text as a function of the key. The least significant word of the key is used for this permutation.
2. The second phase performs an XOR operation of the key on the permuted output from the first phase. The most significant word of the key is used for the XOR operation.

A block diagram for one round of the algorithm that follows provides more information.



Definitions

This section contains some of the definitions of the functions used in the block diagram

- **Conditional Circular Shift**

  Each of the 2 16-bit keys derived for both the phases would be treated as 4 nibbles and each nibble right/left circular shifts the corresponding byte of plain text according to the following definition

BIT3	BIT2	BIT1	BIT0
0 – Left Shift	Shift Value (x bytes)		
1 – Right Shift			

- **Invert bytes**

  Swaps the bytes of the input

Analysis

Theoretical

1. The algorithm permutes the input using a circular shift and XORs with different combinations of the key at different phases and rounds. If the key were to be one of the values 0 or 2^32, the cipher-text produced would be same as the plain-text which is the only weakness in the algorithm.
2. Other than that the algorithm uses all 32 bits of the key for encryption and performs confusion and diffusion as is the desirable property of any cryptographic algorithm and it wouldn't be possible to break the algorithm apart from a brute-force attack.

Statistical

In addition to the theoretical analysis, a test program was written to calculate minimum, maximum and average bit changes in the cipher text for one bit changed in the key/plain-text, the statistics of which computed over a smaller set of keys (0 – 0xFFFF) are shown below

Minimum	Maximum	Average
0	14	2

Brute Force Attack

The brute force attack is a straight-forward algorithm which tries decryption of plain-text using all keys from 0 – 0xFFFFFFFF. The complexity in a brute-force attack is to decide when to stop.

In order for a brute force attack to decide whether the attack was successful or not, the algorithm would need a way to say whether the obtained plain-text is the right one. This decision can be made through an integrity check. The algorithm chosen for an Integrity check is CRC-32. This algorithm has been implemented using the reference [A PAINLESS GUIDE TO CRC ERROR DETECTION ALGORITHMS] http://www.zlib.net/crc_v3.txt