Central Washington University

Introduction to Computer Security

Spring 2019

Project 1 Report

Author:
Hermann Yepdjio

Instructor:
Dr. Razvan Andonie

April 17, 2019

Contents

1 Results

1.1 Part 1

After the 32 iterations we have:

- X = 0001101000000000000
- Y = 1111101010101010101010
- Z = 01101010111100001010101
- 32 keystream bits: 10000011011100000111100000011001

1.2 Part 2

- Plain text before encryption: 0123456789ABCDEF.
- Cipher text: BD2B2FA555AE7017.
- Plain text after encryption and decryption: 0123456789ABCDEF.

2 Observations

The implementation of part 2 was straightforward while part 1 was a little harder to implement. Given the simplicity of both algorithms, my guess is that they can not be used to encrypt really important confidential data.