Signal Cryptography

Sidhath Mohla (ES16BTECH11020)
Sushant Meena (ES16BTECH11021)

March 8, 2019

Overview

Introduction

What is cryptography

Cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages.

Applications

Various aspects in information security such as data confidentiality, data integrity, communication and authentication .

Why we choose this project

We want to deliver a FPGA based implementation so that it can be trusted right from the bottom up (no backdoors at hardware or software level).

Systems considered for implementation

Classic

1. Caesar cipher: Simple shifting by some number. Easily brute forced.
2. Vingere cipher: Introduce the idea of shifting using a key. Easily broken by statistical analysis.

Note: Attacks based for text data.

Modern

1. RC4: Rivest Cipher 4; Permutes input according to a key; Not as simple to attack as the Classical ones yet is fast and not very resource intensive. Was used in WEP.

RC4 Algorithm

Key Scheduling algorithm

- Initialization: S goes from 0 to 255, T[0:255] is filled with K repeating it if necessary.
- Use T and S to swap values in S to get a generator. Key is useless now.

Pseudo-random generation algorithm

- Repeatedly use S to perform more swaps to generate a stream of seemingly random numbers.

Generating encrypted signals

XOR the PRNG generated with the text to encrypt it, and XOR the key again to decrypt it.