MATH 314 Spring 2019 - Class Notes

Scribe: Sean Smith

03/12/2019

Summary: In this class we will start talking about more modern Cryptosystems. Specifically, we will focus on DES (Digital Encryption Standard), but more specifically on SDES (Simplified Digital Encryption Standard).

Before we start: There are two goals of modern Cryptography:

- **Confusion:** Where each bit of the Ciphertext should depend (in a complicated way) on lots of bits of the key.
- **Diffusion:** Where each bit of the Ciphertext should depend on the entire Plaintext. Changing one bit of the Plaintext should change about half of the Ciphertext bits.

Feistel Ciphers: are a framework for a Cryptosystem. The Plaintext gets split into two halves, right and left, doing the same operation (round) many times.

A Feistel Cipher works with any function *f(R,k)* (where R is the Right half of the Plaintext, and k is the key) we need to pick a function that gives us lots of confusion and diffusion to create a strong Ciphertext.

To create a Feistel Cipher, we need to specify:

- The size of the Plaintext (Block size)
- The number of rounds
- The function *f(R,k)*
- How to get k

DES (Digital Encryption Standard): In 1972, the National Bureau of Standards (NBS) (which would later become the National Institute of Standards and Technology, NIST) needed a common Cryptosystem since computers were rapidly on the rise.

The NBS put out a call for proposals for this system. They eventually ended up picking a system developed at IBM called *LUCIFER*, it was then given to the NSA to make changes to it (without saying why).The result became the Digital Encryption Standard (DES).

The DES has notable components such as:

- 64-bit Plaintexts
- 16 rounds
- Complicated f functions involving S-boxes

S-boxes: are just a function that takes in some number of bits and outputs a very different string of bits, which in turn produces lots of confusion.

We'll be mainly talking about SDES since it has all the same ideas as DES, but less complicated.

SDES:

- 12-bit Plaintexts
- 3-4 rounds
- 9-bit master key
- Each round will have have a different round key of 8-bits each
- Round 1 will contain the first 8-bits of the master key
- Round 2 will contain the next 8-bits starting with the second bit of the master key
- Round 3 will contain the next 8-bits starting with the third bit of the master key, wrapping around and ending with the first bit of the master key

Example:

Suppose you have the master key:

$$M_k = 101100011$$

Then:

$$k_1 = 10110001$$

$$k_2 = 01100011$$

$$k_3 = 11000111$$

$$k_4 = 10001110$$

Reminder: the master key is 9-bits, and the round key is 8-bits.

SDES function:

$$f(R_i, k_i)$$

Where R_i is 6-bits and k_i is 8-bits

- R_i is taken to the Expander and is turned into 8-bits from 6-bits
- Then it is moved through a $\oplus(XOR)$ function using the 8-bits from k_i
- Those 8-bits are then split into two different 4-bits
- One of the 4-bits is put through S-box 1, and the other is put through S-box 2
- The S-boxes both spit out 3-bit each and then are moved to the output
- The output combines the two 3-bit strings into one 6-bit string

Expander: takes in 6-bits B_1, B_2, B_3, B_4, B_5, B_6 and creates 8-bits composed of: B_1, B_2, B_4, B_3, B_4, B_3, B_5, B_6,