MATH 314 - Class Notes

10/11/2016

Scribe: Ben Alden

Summary: Todays class covered the introduction to DES and the general format for a Feistel System.

Notes:

DES- Data Encryption Standard
It was a form of Encryption used for almost all digital communication from the 70's till around 2000.
It is still used today in legacy applications, mainly banking.

History: In 1972 NBS (now NIST) put out a request for a new Cryptosystem. IBM Submitted their system (LUCIFER). NSA made changes to LUCIFER and the result was published in 1975 as DES. In 1990 Biham and Shamir published a technique called differential cryptanalysis that could crack a DES like system using 15 rounds (DES uses 16).

Overall Philosophy: Diffusion and Confusion

- Diffusion: Small changes in the plaintext have big changes on the ciphertext. Ideally changing one bit of the plaintext should change about half the digits of the ciphertext.
- Confusion: Every bit of the ciphertext should depend on the entire key in a way that is hard to predict.

Simplified DES (SDES):

DES is a Feistel System:

- We work with bits(F_2)
- Use $\oplus$ to denote bitwise addition in F_2
- Write our plaintext in binary and split it into two halves $->$ L_0 and R_0 (have m bits each)
- Choose n different keys $(k_0, k_1, ...k_n)$ n=number of rounds

Define a function(R_i, k_{i+1}) that outputs m bits.
Encryption: Get the i^{th} step from the $i-1^{th}$ step.

$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$

R_{i-1} becomes L_i
$L_{i-1} \oplus f(R_{i-1}, k_i)$ becomes R_i

Repeat this process n times.

Decryption:
Key fact is that in F_2 $(x \oplus y) \oplus y = x$
Swap L_n and R_n
Repeat encryption steps with keys: $k_n, k_{n-1}, ...k_1$
Repeat n times

$L_n = R_{n-1}$
$R_n = L_{n-1} \oplus f(R_{n-1}, k_n)$

SDES

- Messages will have 12 bits
- L_0, R_0 will have 6 bits
- Master key: 9 bit string
- Keys k_i is the 8 bits of the master key starting with bit i and wrapping around.

Examples: $k = 101100110$
$k_1 = 10110011$
$k_2 = 01100110$
$k_3 = 11001101$
$k_4 = 10011010$

Define $f(R_{i-1}, k_1)$:

First: Need an expander function (Diffusion Step) $E(x)$ function that takes in 6 bits and outputs 8.

123456 turns into:
12434356

Ex: $E(101011) : 10010111$

Second: S-Box (Confusion Step)
S-Box takes in 4 bits and outputs 3 bits

$S_1 =$
(0) 101 010 001 110 011 100 111 000
(1) 001 100 110 010 000 111 101 011

$S_2 =$
(0) 100 000 110 101 111 001 011 010
(1) 101 011 000 111 110 010 001 100

The first bit determines the row to use in the S-box
The last 3 bits (that number) describes which column to use

Example:
$S_1(1110)$ The first deterimes that it is the second row. The 110 is in Decimal 6 meaning the 6^{th} (or 7^{th} when starting with the first row being 1) meaning the output is 101.

R_{i-1} which is 6 bits is fed into the expansion function, making it 8 bits. It is then $\oplus$ with k_i which would still be 8 bits. Then that is split in half, with the upper left most half being fed into S_1 and lower fed into S_2. After that they are both put together as the output.

Try yourself with Message[100001111000] and Master Key: 110010110 using the formula:
$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$

$k = 110010110$
$k_1 = 11001011$
$k_2 = 10010110$
$k_3 = 00101101$

$L_0 = 100001$ $R_0 = 111000$
$L_1 = 111000$ $R_1 = L_0 \oplus f(R_0, k_1)$

$E(111000) = 11010100$
$11010100 \oplus 11001011 = 00011111$
$S_1(0001) = 010$
$S_2(1111) = 100$

Output $= 010100$

Finally $R_1 = 100001 \oplus 010100 = 110101$

Repeat until $n = 4$