MATH 314 Fall 2018 - Class Notes

10/17/2018

Scribe: Brandon Potter

Summary: Today in class we covered the differences between DES and SDES. As well as differential cryptanalysis

Notes:

SDES:

- 3 Rounds
- 12 bit Plaintext
- 9 bit Master Key

DES:

- 16 Rounds
- 64 bit Plaintext
- 56 bit Master Key

Differential cryptanalysis is faster than brute fors on DES with 15 or fewer rounds but with sixteen rounds it is faster to brute force every possible key.

During the mid 90s there was a foundation that created a super computer with the sole reason of brute forcing DES encryption. The machine took 24 hours to crack the system.

This gave rise for a need of longer keys.

Unlike other encryption systems with DES, if you encrypt plaintext with DES twice it isn't equivalent to any form of encrypting one time with DES, like how with Ceasar cipher if you shift 2 then shift 1 it is the same as shifting 3. Although this encrypts the plaintext further this type of encryption is vulnerable to meet in the middle attack.