MATH 314 Spring 2018 - Class Notes
04/02/2019
Scribe:Amanuel Challa

Summary: Todays topic covered are Meet-in-the-Middle attack on DES, 2DES and how a brute force attack would work and ADES introduction

Known Plain Text Attack

- Eve Knows Plaintext(p) and Ciphertext(c)
- $C = E_{k2}(E_{k1}(p))$ 2DES
- Eve can Brute-Force $DES(2^{56} operation)$
- but she cant do $2^{112} operations$
- So she creates two tables one for Encryption and Decryption

Our Goal is to find entries that show up in both tables:$E_{k1}(p), D_{k2}(c)$

Encryption Table	Decryption Table
$E_{k1}(p)$	$D_{k2}(c)$
For all k_1 and s	For all possible k_2,s

- How many pairs does Eve encrypt to find the keys ?
- Pretend each entry is a random string of bites(each string has 64 bits)
- Take a string from the encryption table and one from decryption table
- Find the probability they are equal
- Probability 2 bits are equal = $1/2^{64}$
- Total pair of entries = $2^{56} * 2^{56} = 2^{112}$
- Expected outcome $2^{112} * 1/2^{64} = 2^{48}$
- Eve does this again with new p_2 and c_2 , $c_2 = E_{k2}(E_{k1}, (p_2))$
- What is the expected number of pairs of keys for the second round?
- Expected outcome = $2^{48} * 1/2^{64} = 1/65536$
- We know there is at least one valid pair exists

- Almost always after 2 tries Eve obtains k1 and k2
- How many computation is this?
- We have 2^{56} computation for encryption and 2^{56} ... decryption table
- 2DES has only 57 bits for security only 1 more then DES
- Double encryption is vulnerable to meet-in-the-middle-attack
- because C = Ek2[Ek1(P)] and P = Dk1[Dk2(C)]
- Braking it requires 2^{57} operations

1. 3DES: if we use DES 3 times

- k_1, k_2, k_3
- $c = E_{k3}(E_{k2}, (E_{k1}(p)))$
- $D_{k3}(c) = (E_{k2}, (E_{k1})(p))$
- $D_{k2}(D_{k3}(c)) = ((E_{k1})(p))$
- 3DES is not vulnerable to meet in the middle attack like 2DES
- we use $c = E_{k1}(D_{k2}(E_{k1})(p))$ to encrypt
- we use $p = D_{k1}(E_{k2}(p_{k1})(c))$ to decrypt
- 3DES is still used in practice especially in the financial industry

NIST decided in the 90's it was time to replace DES put out a call for replacement
The chosen design was an algorithm Rijndael "pronounced rain-dahl"
became the official replacement of DES called "ADES"
Advanced Encryption Standard
Faster and more secure than DES as well as it dosent have a back door