

MATH 314 - Class Notes

3/28/2017

Scribe: Matt Stillwell

Summary: We learned how SDES works.

Notes: Feistel System $L_{i+1} = R_i$, $R_{i+1} = f(R_i, K_i) \text{ XOR } L_i$. To encrypt perform this operation n times. To decrypt perform this operation n times in reverse (swap L_i , R first). DES has 16 rounds and 64 bits at a time. SDES (simple DES) has 3 rounds and 12 bits at a time. Round key obtained from master key (9 bits) by taking 8 bits at a time starting at $i-1$. For the function $f(R_i, K_i)$, you take R_i (6 bits) and pass it to the expander function. In the expander function $E(abcdef) = abcdcef$ (8 bits). You then XOR that With the round key R_i . Split the first half (4 bits) and pass it to SBOX1 (3 bits). Take the second half (4 bits) and pass it to SBOX2 (3 bits). Concatenate the first half with the second half (6 bits). Take this and XOR it with L_i to get the new R_i . SBOX1 looks like ((101, 010, 001, 110, 011, 100, 111, 000), (001, 100, 110, 010, 000, 111, 101, 011)). SBOX2 looks like ((100, 000, 110, 101, 111, 001, 011, 010), (101, 011, 000, 111, 110, 010, 001, 100)). To understand what SBOX will return the first digit of the 4 digit sequence is decides whether it is on top (0) or on bottom (1). Then the rest of the digits decide which option to choose (if the binary is 2, choose the 3rd one). The randomness of the SBOX causes confusion. The expander function helps with diffusion.

Examples: message = 101101110101, master key = 111010110
key1 = 11101011, key2 = 11010110, key3 = 10101101

Round 1

$L_0 = 101101$	$R_0 = 110101$
.....	EXPANDER(110101) = 11101001
.....	XOR key1 = 0000 0010
.....	$S_1(0000) = 101$ $S_2(0010) = 110$
.....	101 110 = 101110
$L_1 = R_0 \dots$	101110 XOR $L_0 = 000011$
$L_1 = 110101$	$R_1 = 000011$

Round 2

$L_1 = 110101$	$R_1 = 000011$
.....	EXPANDER(000011) = 00000011
.....	XOR key2 = 1101 0110
.....	$S_1(1101) = 111$ $S_2(0110) = 001$
.....	111 001 = 1110001
$L_2 = R_1 \dots$	1110001 XOR $L_1 = 001100$
$L_2 = 000011$	$R_2 = 001100$

Round 3

L2 = 000011	R2 = 001100
.....	EXPANDER(001100) = 00111100
.....	XOR key3 = 1001 0001
.....	S1(1001) = 100 S2(0001) = 000
.....	100 000 = 100000
L3 = R2...	100000 XOR L2 = 100011
L3 = 001100	R3 = 100011

Ciphertext: L3 || R3 = 001100100011