MATH 314 Spring 2019 - Class Notes

3/29/2019

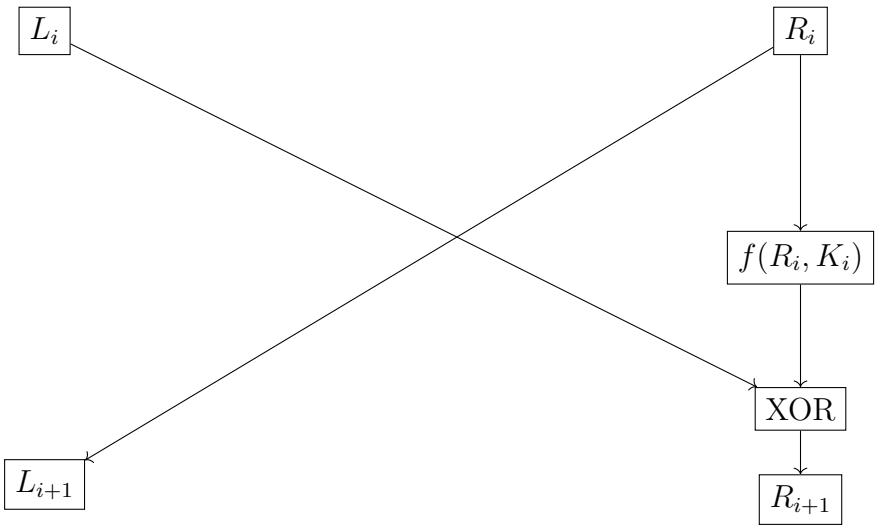
Scribe: Russell Carter

Summary: Today we went over DES and Feistel Systems, and revisited SDES in more depth with an example.

Recall: DES

General picture of the Feistel Cipher

Round i:



How do you decrypt a feistel cipher?

- Swap right and left sides
- Perform all the round using the round keys in reverse order
- Swap right and left side one final time
- Recover the plaintext

SDES

- 12 bit plaintexts
- 9 bit master key
- 8 bit round key, starting with $(i-1)$st (wrap around if necessary)
- Recover the plaintext

S1:

101	010	001	110	011	100	111	000
001	100	110	010	000	111	101	011

S2:

100	000	110	101	111	001	011	010
101	011	000	111	110	010	010	100

```
Expander: 1 2 3 4 5 6
          1 2 4 3 4 3 5 6
```

SDES F-function

$f(R_i, K_i)$
$R_i = 6$ bits
$K_i = 8$ bits

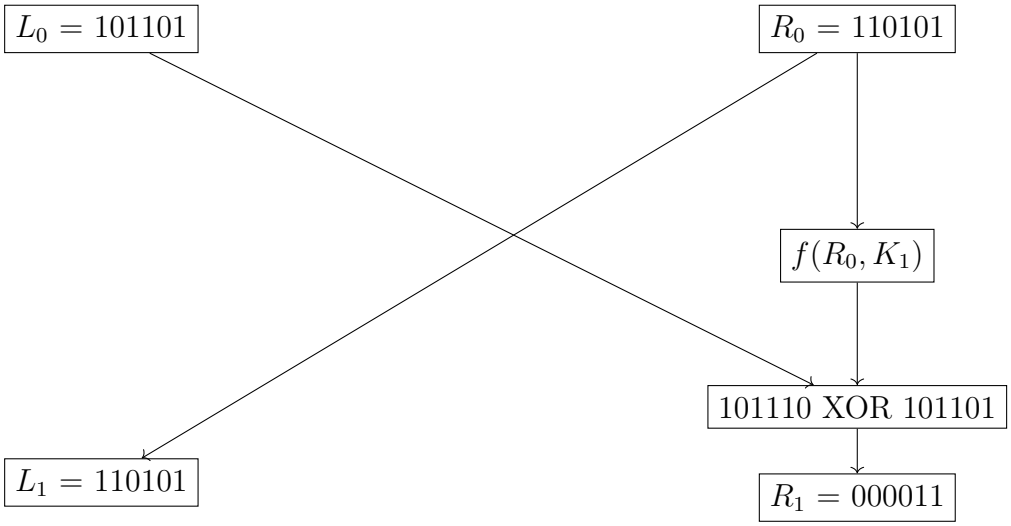
F function in steps:

- Ri gets expanded into 8 bits with the Expander above
- The expanded 8 bits then gets XOR'ed with K_i
- The 8 bits then gets split into 4 and 4
- The first 4 bits are compared with Sbox 1
- The last 4 bits are compared with Sbox 2
- The Sboxes will produce 3 bits each which together will give us our ciphertext

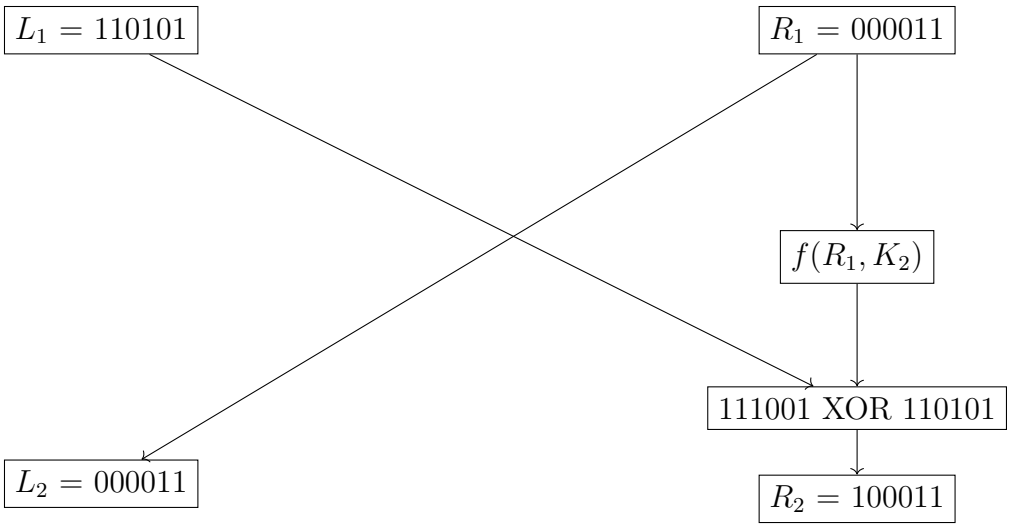
SDES Example (3 rounds):

Master Key = 111 010 110
Encrypt P = 1011 0111 0101
3 round keys:
$K_1 = 11101011$
$K_2 = 11010110$
$K_3 = 10101101$

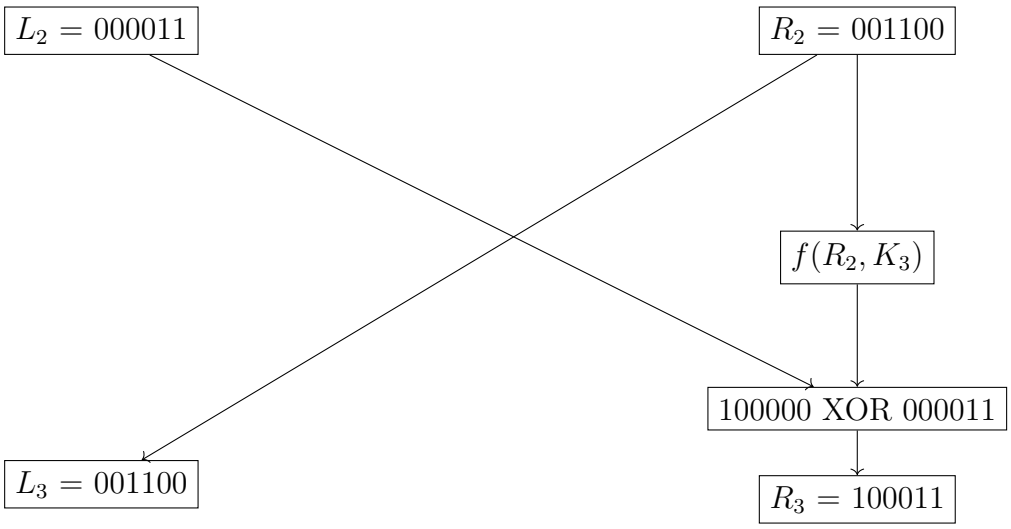
Round 1



Round 2


$L_1 = 110101$
$R_1 = 000011$
$f(R_1, K_2)$
111001 XOR 110101
$L_2 = 000011$
$R_2 = 100011$

Round 3



When we combine L_3 and R_3 to get the ciphertext 001100100011