

Alice

Bob

KSES

9.5

A6

D8

7B

A xor B

1010 xor 1011

0001 = 1

6 xor 7

0110 xor 0111

0001 = 1

$$Y_A = eK_A(KSES) = 11$$

D xor B

1101 xor 1011

0110 = 6

8 xor 7

1000 xor 0111

1111 = F

$$Y_B = eK_B(KSES) = 6F$$

11 xor A6

1 xor 6

0001 xor 0110

0111 = 7

1 xor A

0001 xor 1010

1011 = B

$$K_A = 7B$$

6F xor D8

6 xor D

0110 xor 1101

1011 = B

F xor 8

1111 xor 1000

0111 = 7

$$K_B = 7B$$