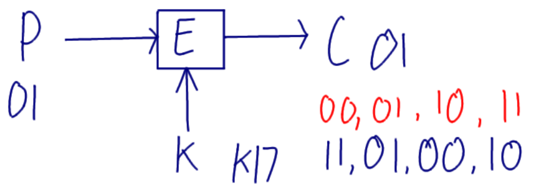
CSS322 – Block Ciphers and DES Notes

P	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11	K12
00	00	00	00	00	00	00	01	01	10	10	11	11
01	01	01	10	10	11	11	00	00	00	00	00	00
10	10	11	01	11	01	10	10	11	01	11	01	10
11	11	10	11	01	10	01	11	10	11	01	10	01

P	K13	K14	K15	K16	K17	K18	K19	K20	K21	K22	K23	K24
00	01	01	10	10	11	11	01	01	10	10	11	11
01	10	11	01	11	01	10	10	11	01	11	01	10
10	00	00	00	00	00	00	11	10	11	01	10	01
11	11	10	11	01	10	01	00	00	00	00	00	00

2 bit block

$2^2 = 4$ possible plaintexts



Ideal: n-bit block, $2^n!$ mappings

key length $n2^n$

Feistel: n-bit block, 2^k mappings

Key length k

Figure 1: Ideal Block Cipher Example; Lecture 04

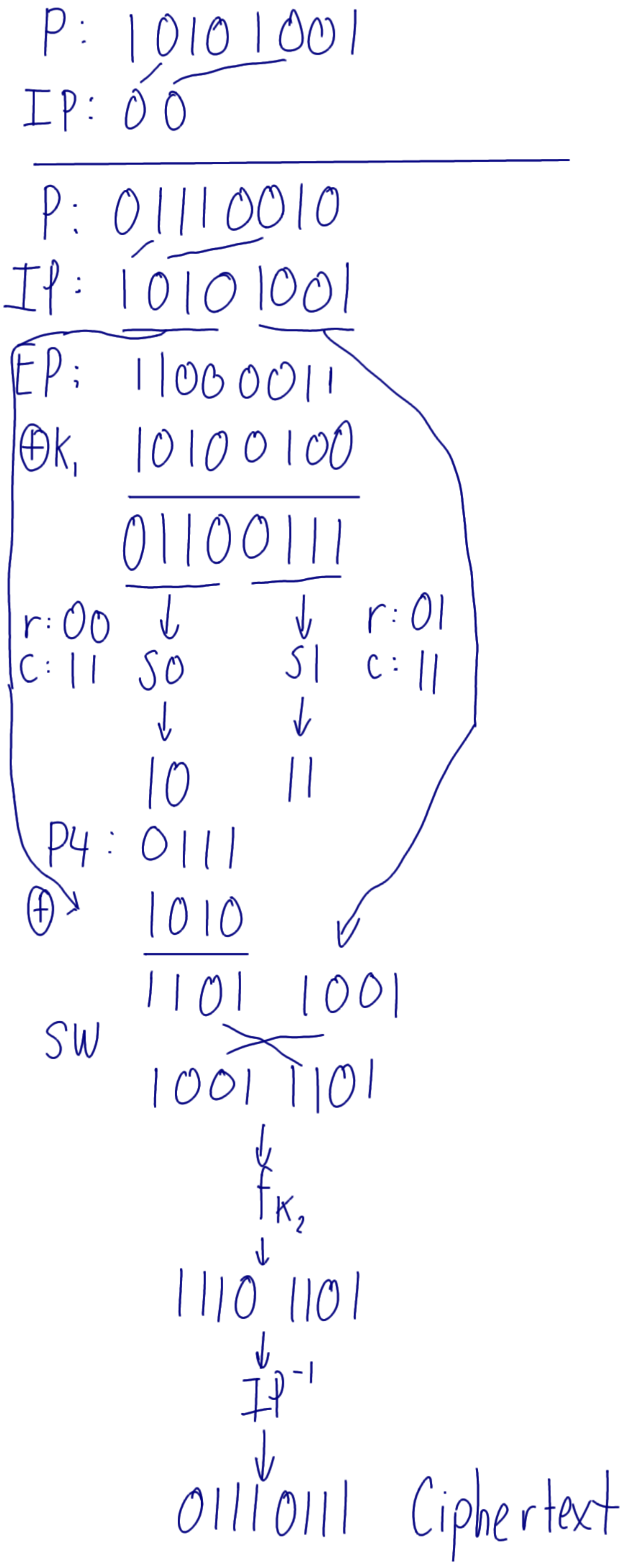


Figure 2: Simplified DES Example; Lecture 05

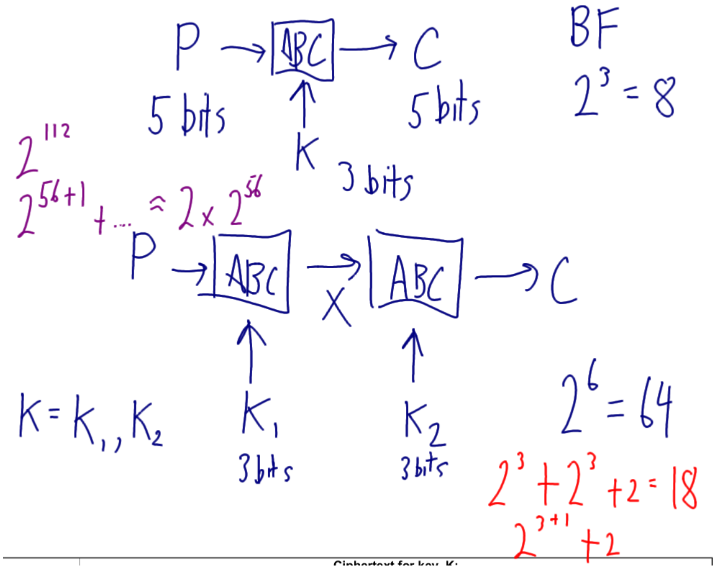


Figure 3: Single Encryption vs Double Encryption; Lecture 06

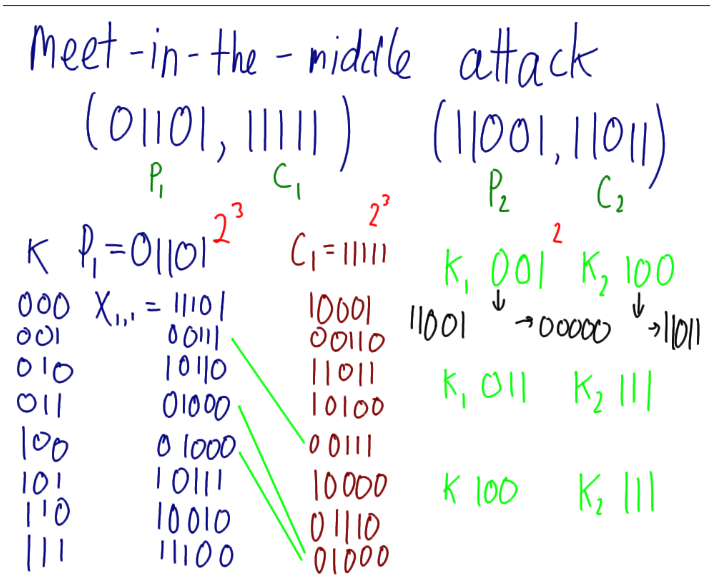
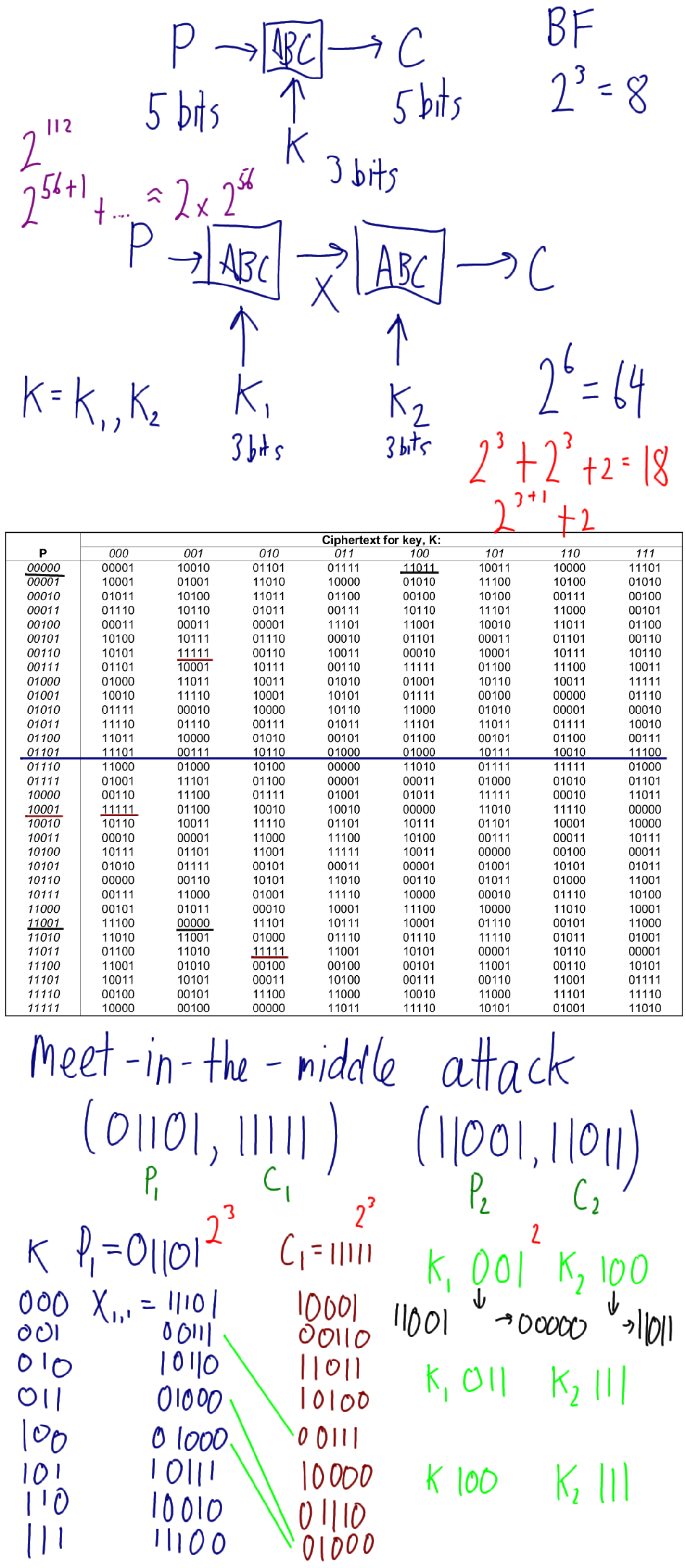


Figure 4: Meet-in-the-Middle Attack on Double Encryption; Lecture 06



P	Ciphertext for key, K:							
	000	001	010	011	100	101	110	111
00000	00001	10010	01101	01111	11011	10011	10000	11101
00001	10001	01001	11010	10000	01010	11100	10100	01010
00010	01011	10100	11011	01100	00100	10100	00111	00100
00011	01110	10110	01011	00111	10110	11101	11000	00101
00100	00011	00011	00001	11101	11001	10010	11011	01100
00101	10100	10111	01110	00010	01101	00011	01101	00110
00110	10101	11111	00110	10011	00010	10001	10111	10110
00111	01101	10001	10111	00110	11111	01100	11100	10011
01000	01000	11011	10011	01010	01001	10110	10011	11111
01001	10010	11110	10001	10101	01111	00100	00000	01110
01010	01111	00010	10000	10110	11000	01010	00001	00010
01011	11110	01110	00111	01011	11101	11011	01111	10010
01100	11011	10000	01010	00101	01100	00101	01100	00111
01101	11101	00111	10110	01000	01000	10111	10010	11100
01110	11000	01000	10100	00000	11010	01111	11111	01000
01111	01001	11101	01100	00001	00011	01000	01010	01101
10000	00110	11100	01111	01001	01011	11111	00010	11011
10001	11111	01100	10010	10010	00000	11010	11110	00000
10010	10110	10011	11110	01101	10111	01101	10001	10000
10011	00010	00001	11000	11100	10100	00111	00011	10111
10100	10111	01101	11001	11111	10011	00000	00100	00011
10101	01010	01111	00101	00011	00001	01001	10101	01011
10110	00000	00110	10101	11010	00110	01011	01000	11001
10111	00111	11000	01001	11110	10000	00010	01110	10100
11000	00101	01011	00010	10001	11100	10000	11010	10001
11001	11100	00000	11101	10111	10001	01110	00101	11000
11010	11010	11001	01000	01110	01110	11110	01011	01001
11011	01100	11010	11111	11001	10101	00001	10110	00001
11100	11001	01010	00100	00100	00101	11001	00110	10101
11101	10011	10101	00011	10100	00111	00110	11001	01111
11110	00100	00101	11100	11000	10010	11000	11101	11110
11111	10000	00100	00000	11011	11110	10101	01001	11010

Figure 5: Double Encryption and Meet-in-the-Middle with Demo Cipher; Lecture 06