CSS322 – Block Ciphers and DES Notes

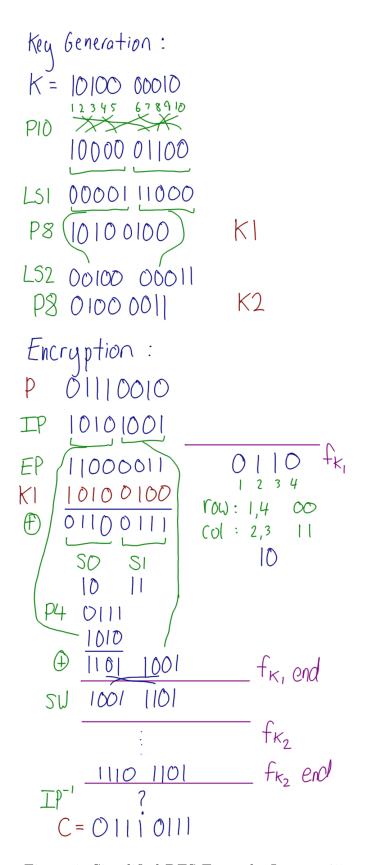


Figure 1: Simplified DES Example; Lecture 05

Plaint ext: 64 bits

Ciphertext: 64 bits

$$P_1$$
 P_2

DES J
 K_1
 C_1
 C_2
 C_1 , C_2

differ in 32 bits

Figure 2: Expect half of bits to be different between two ciphertext; Lecture 06

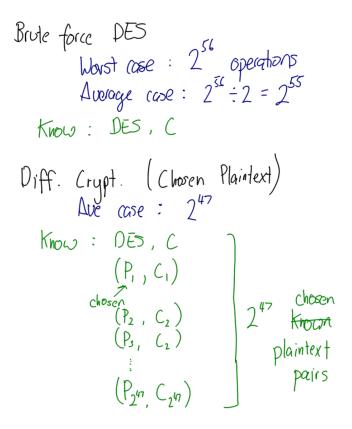


Figure 3: Chosen Plaintext Attack on DES; Lecture 06

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

$$E P_{1} = 01|0| K_{1} = 001 \underbrace{X = 0011}_{C_{1}} K_{2} = 100 \underbrace{X = 0011}_{C_{1}} K_{2} = 100 \underbrace{X = 0011}_{C_{1}} K_{2} = 100 \underbrace{X = 0011}_{C_{1}} K_{1} = 001 \underbrace{X = 0011}_{C_{1}} K_{1} = 001 \underbrace{X = 0011}_{C_{1}} K_{1} = 00101$$

Figure 5: Double Cipher Encrypt showing same X; Lecture 07