CSS322 – Block Ciphers and DES Notes

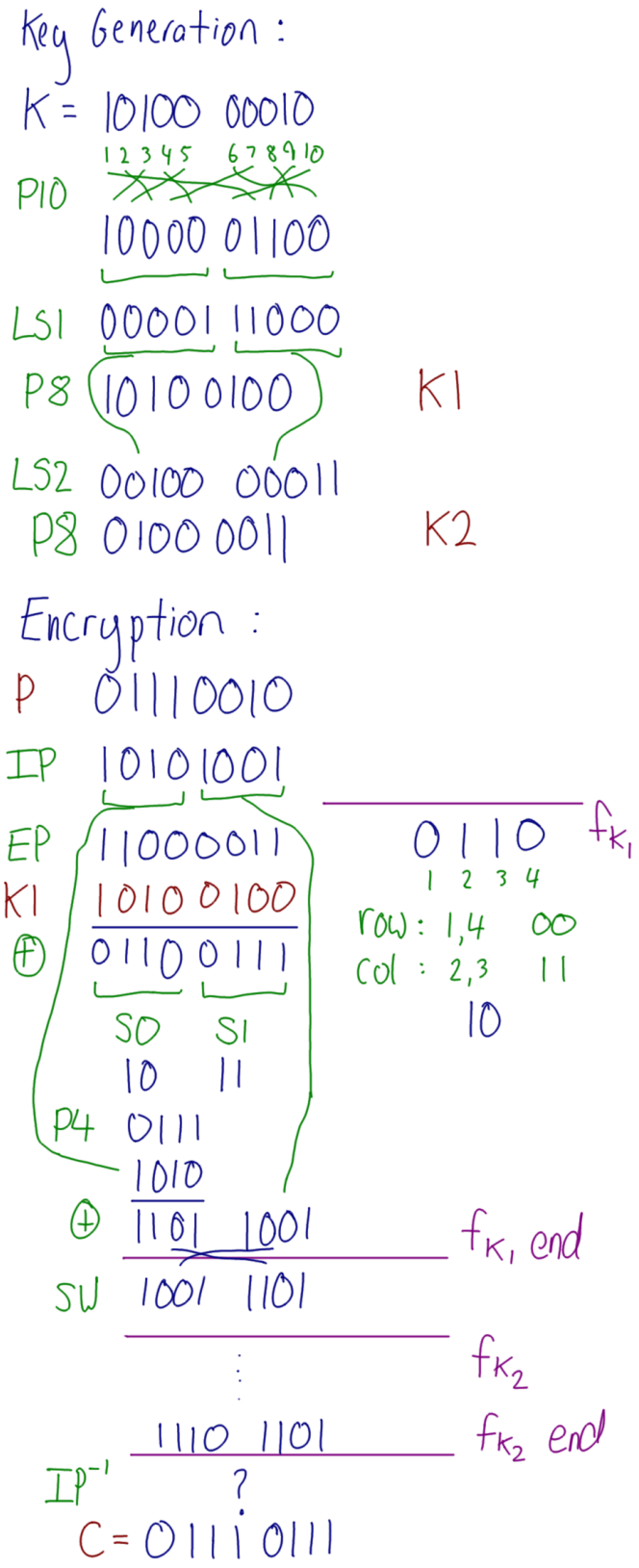

Figure 1: Simplified DES Example; Lecture 05

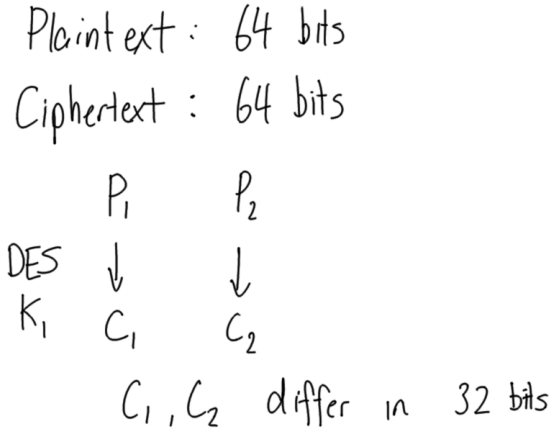

Figure 2: Expect half of bits to be different between two ciphertext; Lecture 06

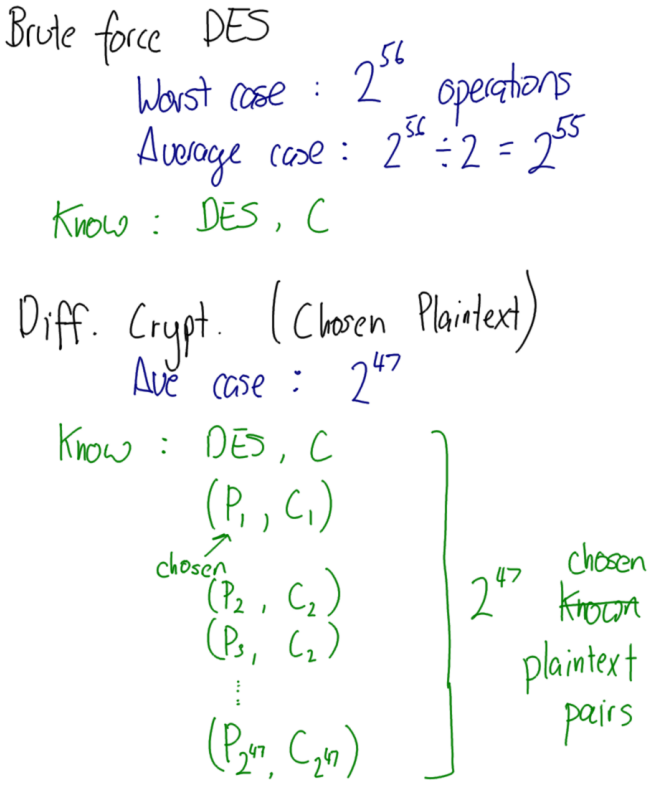

Figure 3: Chosen Plaintext Attack on DES; Lecture 06

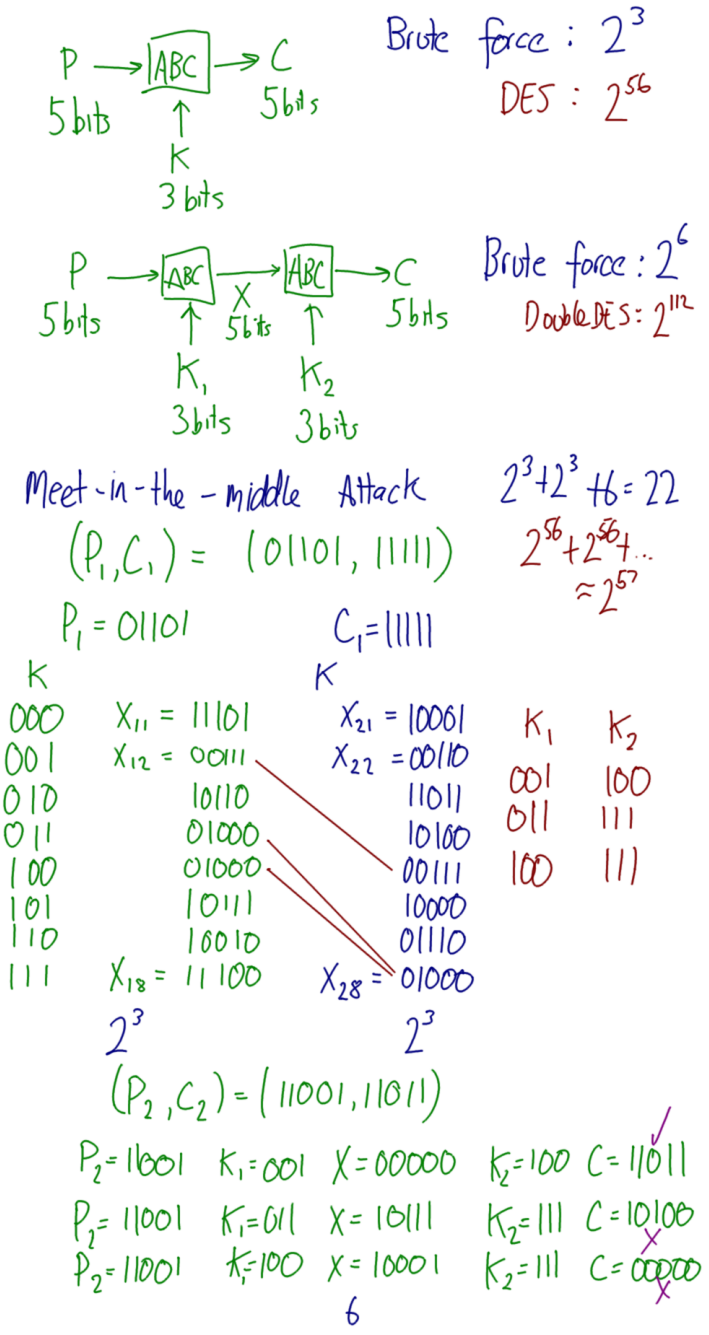

Figure 4: Meet-in-the-Middle Attack on Double Cipher; Lecture 06

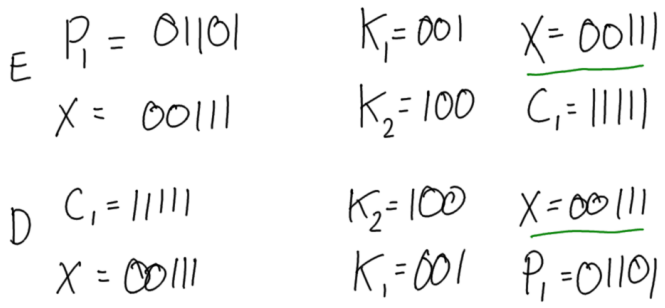

Figure 5: Double Cipher Encrypt showing same X; Lecture 07