CSS322 – Block Cipher Examples

1 Example Block Cipher

Consider a 4-bit block cipher, called *Steve's Simple Cipher* or SSC for short, shown in the table below. The table gives the ciphertext C produced when encrypting the plaintext P with one of the four keys.

P	C (K=00)	C (K=01)	C (K=10)	C (K=11)
0000	0110	1100	0001	0010
0001	1101	0100	1010	0000
0010	0010	0001	1111	1011
0011	0100	1101	0011	1001
0100	1100	0111	1001	0011
0101	1111	0101	0010	1000
0110	0000	0011	0111	1111
0111	0111	1011	1101	0001
1000	1010	1001	1000	0100
1001	0001	0000	1110	0111
1010	1001	0110	0110	1100
1011	1110	0010	1011	1101
1100	1011	1111	0000	0101
1101	1000	1010	0100	1110
1110	0011	1110	1100	0110
1111	0101	1000	0101	1010

2 Meet-In-The-Middle Attack

Consider a block cipher, *Double-SSC*, which involves applying the block cipher SSC two times (e.g. encrypt the plaintext to obtain a temporary value, then encrypt the temporary value to obtain the ciphertext), each time using a potentially different 2-bit key.

Show how the meet-in-the-middle attack works by applying it against Double-SSC. Use the attack to find the key used if the attacker already knows the (plaintext, ciphertext) pairs: (1101, 1100) and (1001, 1101).

3 Modes of Operation

Encrypt the plaintext `1100101011001111` using *SSC* and key `00` (and where necessary IV/nonce/counter `1100`) using the following modes of operation: ECB, CBC, CFB, OFB, Counter.