

No.

Date

1. plaintext

0100101 01000010 1101000 0111000 0111010
0111001 010

key

0101000 0110011 0100101 0101000 0011110 0110010
0001101 0010001 1001101 0010000 0100100

cipher:

CF910

3. CBC

$$Funct = 1000$$

$$IV = 1001$$

Plaintexts : Aye

A	y	e
0000	0001	0111
0001	0111	0001

$$P_1 = 0100$$

$$IV = 1001$$

$$K = 1000$$

$$C = 0101$$

$$P_2 = 0001$$

$$IV = 0101$$

$$K = 1000$$

$$C = 1100$$

$$P_3 = 0111$$

$$IV = 1100$$

$$K = 1000$$

$$C = 0011$$

$$P_4 = 1001$$

$$IV = 0011$$

$$K = 1000$$

$$C = 0010$$

$$P_5 = 0110$$

$$IV = 0010$$

$$K = 1000$$

$$C = 1100$$

$$P_6 = 0101$$

$$IV = 1100$$

$$K = 1000$$

$$C = 0001$$

$$C = 0101 \quad 1100 \quad 0011 \quad 0010 \quad 1100 \quad 0001$$

No.

Date

2. ECB

Plaintiff: Aye

Defendant: 1100

	A		y		e				
P	0100		0001	0111		1001	0110		0101

10	=	1100	1100	1100	1100	1100	1100
----	---	------	------	------	------	------	------

0	=	1000	1101	1011	0101	1010	1001
---	---	------	------	------	------	------	------