1) cipher: CPC. ↓ mpwf zpu. bmjdf

plain: bob. I love you. alice

cipher: nan. u xahq kag. mxuoq

plain: ~~x~~bhb. t ~~fhmz~~ ohl aftrz } bob. I love you. Alice
or jmj

2) Plain: This is an easy problem

cipher: uqsi si mj cmiw lokn gch

cipher: rmij'st uamu xyj

plain: wasn't that fun

4. Find ciphertext for 010 - 110 - 001 - 111 for the mapping:

XOR Truth Table

| Input A | B | Output |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

| input | output |
|---|---|
| 000 | 110 |
| 001 | 111 |
| 010 | 101 |
| 011 | 100 |
| 100 | 011 |
| 101 | 010 |
| 110 | 000 |
| 111 | 001 |

| $P_i$ | $C_i$ |
|---|---|
| 010 | 101 |
| 110 | 000 |
| 001 | 110 |
| 111 | 001 |

Ciphertext: 101 - 000 - 110 - 001

Using CBC and the mapping:

a) Encrypt Plaintext: 010-110-001-110 given IV = 110

| P(1) | P(2) | P(3) | P(4) |
|---|---|---|---|
| 010 | 110 | 001 | 110 |

| C(0) | C(1) | C(2) | C(3) | C(4) |
|---|---|---|---|---|
| 110 | 011 | 010 | 000 | 101 |

XOR Truth Table

| Input A | B | Output |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

010 / 110 → KS(100) → 011 → 100

110 / 011 → 101 → KS(001) → 010 → 011

KS(100) → 011 → 000 → 110

b) Decrypt cipher from A: 110-011-010-001

| C(0) | C(1) | C(2) | C(3) | C(4) |
|---|---|---|---|---|
| 110 | 011 | 010 | 000 | 101 |

C(0) = 110 → 100 → 010 → C(2)

| C(0) | C(1) | C(2) | C(3) | C(4) |
|---|---|---|---|---|
| 010 | 110 | 110 | 001 | 001 |
| | 000 | 000 | 111 | 111 |
| 010 | 010 | 010 | 010 | 101 |
| | 010 | 101 | 010 | |

encrypt

IV = 010

| P(1) | P(2) | P(3) | P(4) |
|---|---|---|---|
| 010 - 110 - 001 - 110 | | | |

| C(0) | C(1) | C(2) | C(3) | C(4) |
|---|---|---|---|---|
| 010 - 110 - 110 - 001 - 001 | | | | |

| | | | |
|---|---|---|---|
| 110 | 110 | 110 | 001 |
| 110 | 110 | 001 | 110 |
| 000 | 000 | 111 | 111 |
| KS(000) → 110 | KS(000) → 110 | KS(111) → 001 | KS(111) → 001 |

WRONG

| P(1) | P(2) | P(3) | P(4) |
|---|---|---|---|
| 010 - 110 - 001 - 110 | | | |

| C(0) | C(1) | C(2) | C(3) | C(4) |
|---|---|---|---|---|
| 110 - 011 - 010 - 100 - 101 | | | | |

| | | | |
|---|---|---|---|
| 110 | 011 | 010 | 100 |
| 010 | 110 | 001 | 110 |
| 100 | 101 | 011 | 010 |
| 011 | KS(101) → 010 | KS(011) → 100 | KS(010) → 101 |