CS181 HW3
Xiaoming Huang

1.

a) Codes in 1a.cpp

b) *Codes in 1b.cpp*

ciphertext in binary: 1 0 0 0 0 1 0 1 0 0 1 0 0 1 1 1 0 1 1 0 0

c) Codes in 1c&d.cpp

keystream:
181 210 86 5 165 245 93 50 124 85 172 216 184 91 155 127 193 164 7 131 207 15 52 13

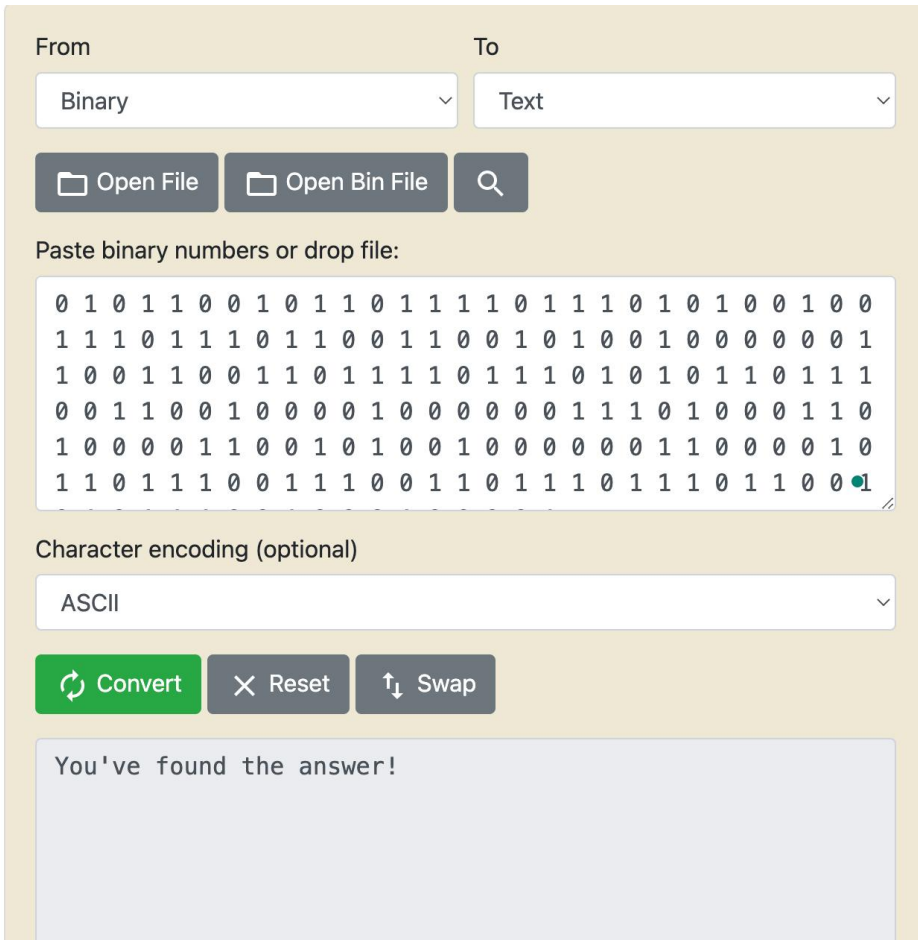
Keystream in binary:
1 0 1 1 0 1 0 1 1 1 0 1 0 0 1 0 0 1 0 1 0 1 1 0 0 0 0 0 0 1 0 1 1 0 1 0 0 1
0 1 1 1 1 1 0 1 0 1 0 1 0 1 1 1 0 1 0 0 1 1 0 0 1 0 0 1 1 1 1 1 0 0 0 1 0 1
0 1 0 1 1 0 1 0 1 1 0 0 1 1 0 1 1 0 0 0 1 0 1 1 1 0 0 0 0 1 0 1 1 0 1 1 1 0
0 1 1 0 1 1 0 1 1 1 1 1 1 1 1 1 0 0 0 0 0 1 1 0 1 0 0 1 0 0 0 0 0 0 0 1 1 1
1 0 0 0 0 0 1 1 1 1 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 1 1
0 1

d) Codes in 1c&d.cpp

plaintext in binary after ciphertext XORing with keystream:

```
0 1 0 1 1 0 0 1 0 1 1 0 1 1 1 1 0 1 1 1 0 1 0 1 0 0 1 0 0 1 1 1 0 1 1 1 0 1
1 0 0 1 1 0 0 1 0 1 0 0 1 0 0 0 0 0 0 1 1 0 0 1 1 0 0 1 1 0 1 1 1 1 0 1 1 1
0 1 0 1 0 1 1 0 1 1 1 0 0 1 1 0 0 1 0 0 0 0 1 0 0 0 0 0 0 1 1 1 0 1 0 0 0 1
1 0 1 0 0 0 0 1 1 0 0 1 0 1 0 0 1 0 0 0 0 0 0 1 1 0 0 0 0 1 0 1 1 0 1 1 1 0
0 1 1 1 0 0 1 1 0 1 1 1 0 1 1 1 0 1 1 0 0 1 0 1 0 1 1 1 0 0 1 0 0 0 1 0 0 0
0 1
```

Convert to ASCII using online translator:
plaintext:
You've found the answer!



2.
a)

- As decryption only requires Mi = Ci + Ek(Ci−1), so if C2 is wrongly transmission, then, it will have effect on M2, and M3 which use Ek(C2);

- So Bob can still decrypt M1, M4, ... , M10 correctly, since they do not use C2 to decrypt.

- M2 will have 2 bits off, since it's XORing the C2 with other stuff, as C2 has two bits off, M2 is gonna also has 2 bits off.

- M3 seems to be completely off, since some slight change in the input of the Ek() can have great effect on the output, so Ek(C2) is gonna be huge off even if C2 is just 2 bits off, and then the decrypted M3 will also be huge different.

b)
If the CBC uses the same IV, it will be deterministic, which means that same plaintext will always be mapped to the same ciphertext. It is not save aginst CPA attack because the attacker can test on whether some specific plaintext map to some ciphertext he knows or not.

For Eve, as she know M and M', and their corresbonding C and C'. She can basically ask Bob to encrypt one of the M's. And since the encryption is deterministic, it will definitely output one of the C's. And based on the result, she can see the ciphertext of M and M'.

Reference:
https://www.rapidtables.com/convert/number/binary-to-ascii.html