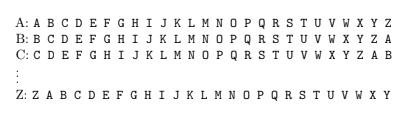
Describe some of the components that comprise modern day block ciphers. In particular, describe with the aid of an example the Vignère Cipher. [8 marks]

All modern day block ciphers contain a key denoted by K, that can take on many possible values.

The Vigenere Cipher can protect against possible attacks of identifying recurring characters and domain specific buzzwords etc. as the Vigenere Cipher is a poly-alphabetical cipher.To encode a letter, go to it’s row and across by the index of the letter in the key.



For example,

Plaintext: ATTACKATDAWN

Key: LEMON -> LEMONLEMONLE

Ciphertext: LXFOPVEFRNHR

With the aid of an example, show why the electronic code book (ECB) mode is susceptible to substitution attacks. Describe the cipher block chaining (CBC) mode and how it can provide probabilistic encryption which overcomes the deterministic features of ECB mode. [10 marks]

ECB mode is susceptible to a substitution attack as an attacker can intercept blocks once the key mapping the plaintext Xi -> Yj is known.

For example with an electronic bank transfer, if the attacker can repeatedly send 1 dollar transfers to an account and can intercept the blocks he can record the senders Bank account number, the bank name, his bank name and then replaces all other transactions that he intercepts with his bank account number by substitution and can send all the transactions to his bank account.

In CBC mode, each block of plaintext is XOR’d with the previous ciphertext block being before encrypted. Each ciphertext block depends upon all plaintext blocks up to that point.

Define a cyclic group G. [2 marks]

What is the primitive element or generator of the group G? [2 marks]

Check if a=2 is a primitive element of ℤ\*11. [2 marks]

Is the group ℤ\*11 a cyclic group? [2 marks]

* A Group G which contains an element *a* with maximum order *ord(a) = |G|* is said to be cyclic.
* The primitive element or generator of the group G **NEED ANSWER**
* **NEED ANSWER**

**Is a=2 a primitive element?**

A1 = 2

A2 = 2\*2%11 = 4

A3 = 4\*2%11 = 8

A4 = 8\*2%11 = 5

A5 = 5\*2 = 10%11 = 10

A6 = 10\*2%11 = 9

A7 = 9\*2%11 = 7

A8 = 7\*2%11 = 3

A9 = 3\*2%11 = 6

A10 = 6\*2%11 = 1

Yes a=2 is a primitive element & group is cyclic

* **NEED ANSWER**