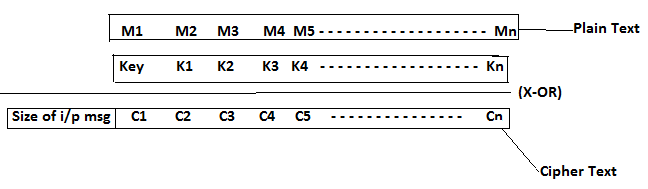
**Home Work -**2 **Jaya Venkata Maneswara Rao Vutukuri - 1208568461**

**Ishan Vyas -1208819504**

**1)Algorithm Used in**  **Encryption**

Input Message is divided into M1, M2, M3, - - - - - - Mn are such that all the blocks are of 32 bit length. If Mn is not 32 bits add padding to Mn

****

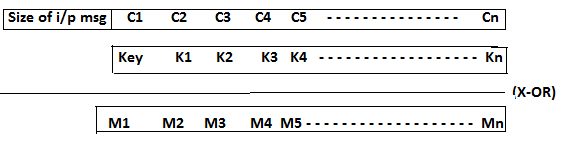
Here K1 is Hash(Key) and K2 is Hash(K1) and so on ... (MD 5 is used for hashing).

Key, K1, K2 - - - are of 32 bit size

C1=M1^Key ; C2=M2^K1 ; C3=M3^K2 ; and so on ..

Key is generated from system entropy.

**Algorithm Used in Decryption**



**2)** Brute forced the keys for the given encrypted files and found keys.

Key for img-encr file is **c9034bf4**

Key for pdf-encr is **1739d398**

Key for text-encr is

**3) Weakness of Cipher Design**

* If the type of the encrypted file is known we can get the key and plain text in one attempt
* Cannot check for Integrity
* If attacker knows some part of message then he can find original message to its right in one attempt
* Attacker can get a range of keys because plain text contains only some range of characters. Range of keys << 2^32 .So Attacker can brute force with less number of keys.

**4)**  **We already know the type of the file. Calculating keys using this weakness**

**PNG :** For png image starting 32 bits are always 474e5089 (hex) and the first 32 bits of encrypted image file is 8e4d1b7d (hex). On doing a simple X-OR of these 2 values can get the key in one attempt. Key is c9034bf4 (hex)

**PDF :** For pdf starting 32 bits are always 46445025(hex) and the first 32 bits of encrypted pdf file is 517d83bd (hex). On doing a simple X-OR of these 2 values can get the key in one attempt. Key is 1739d398(hex)

**Text File:** we have encrypted file and we know plain text will only contain characters, numbers, and some special characters based on it we can minimize key space to find the plain text

To have plain text in a-z key should be in range (c2c92eb8 -- d9d235a3)

To have plain text in A-Z key should be in range to get Z (e2e90e98 -- f9f21583)

9a9176e0 -- to get "