**Encryption Equations:**

Ai**’** = P(Ai ⊕ K1) ⊕ S(Bi ⊕ K2)

Bi**’** = S(Ci ⊕ K3)

Ci**’** = S(Bi ⊕ K2)

Di**’** = P(Di⊕K4) ⊕ S( Ci ⊕ K3)

Ri**’** = Ai**’**Bi**’**Ci**’**Di**’**interpreted as 32-bit sequence

Ri+1 = Ri**’**⊕ Hash (Key)

Ai+1 = 1st 8 bits of Ri+1

Bi+1 = 2nd 8 bits of Ri+1

Ci+1 = 3rd 8 bits of Ri+1

Di+1 = 4th 8 bits of Ri+1

**Decryption Equations:**

Ai = P-1(Ai**’**⊕ Ci**’**) ⊕ K1

Bi = [S-1(Ci**’**)] ⊕ K2

Ci = [S-1(Bi**’**)] ⊕ K3

Di = P-1(Di**’** ⊕ Bi**’**) ⊕ K4

Ri’ = Ri+1 ⊕ Hash(Key)

Ai**’**= 1st 8 bits of Ri**’**

Bi**’**= 2nd 8 bits of Ri**’**

Ci**’**= 3rd 8 bits of Ri**’**

Di**’**= 4th 8 bits of Ri**’**

**Cipher Block Chaining Mode:**

Chaining adds a feedback mechanism to the block cipher. The results of encryption of previous blocks are added to the encryption of current block, i.e, the plain text is XORed with the previous cipher text before its encrypted which makes the plain text patterns concealed.

**Initialization Vector:**

This block of random data makes each message unique. It prevents identical plaintext messages to encrypt to different cipher text messages.

**Key:**

We split the 32-bit key into 4 8-bit keys. We also protect the key by hashing it as h(k). Every 8-bit sub key is passed into a set of functions .

