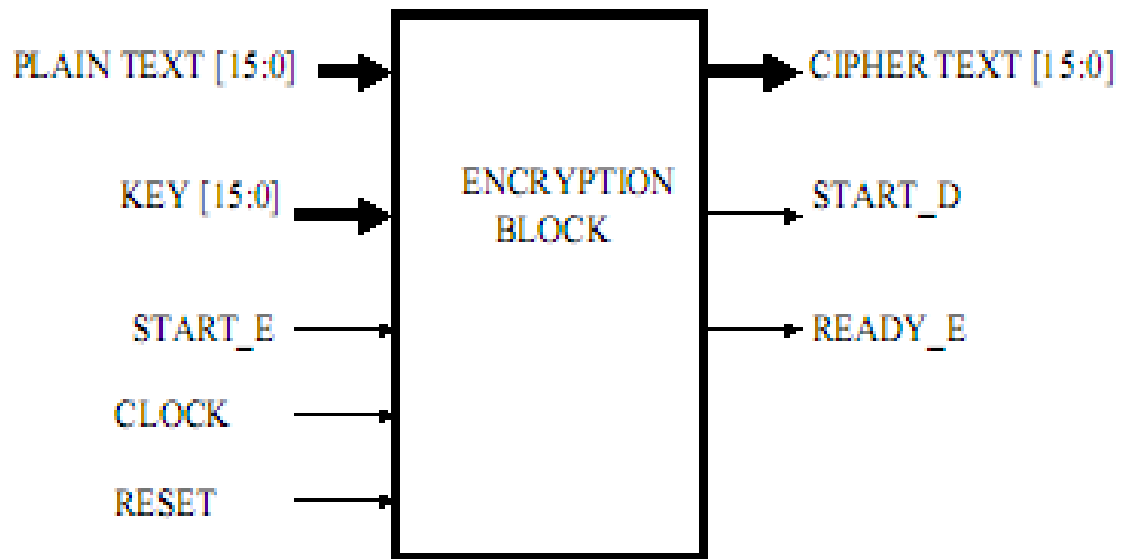
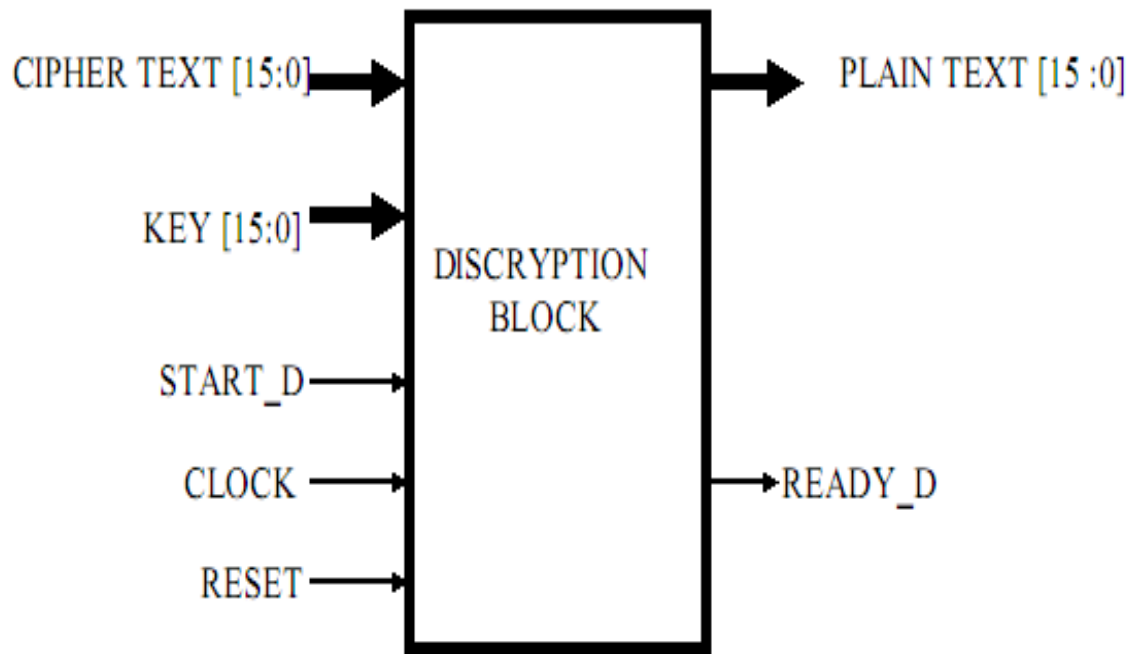


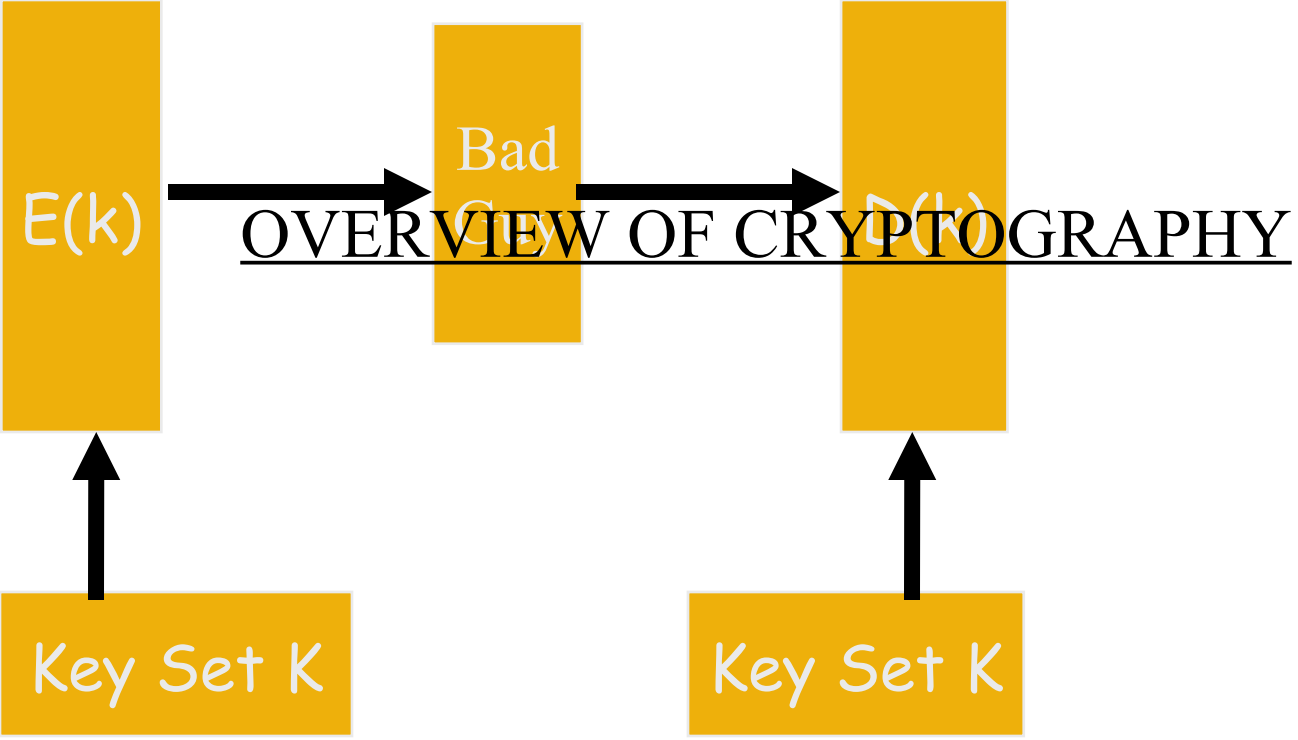
CRYPTOGRAPHY

INPUT BLOCK

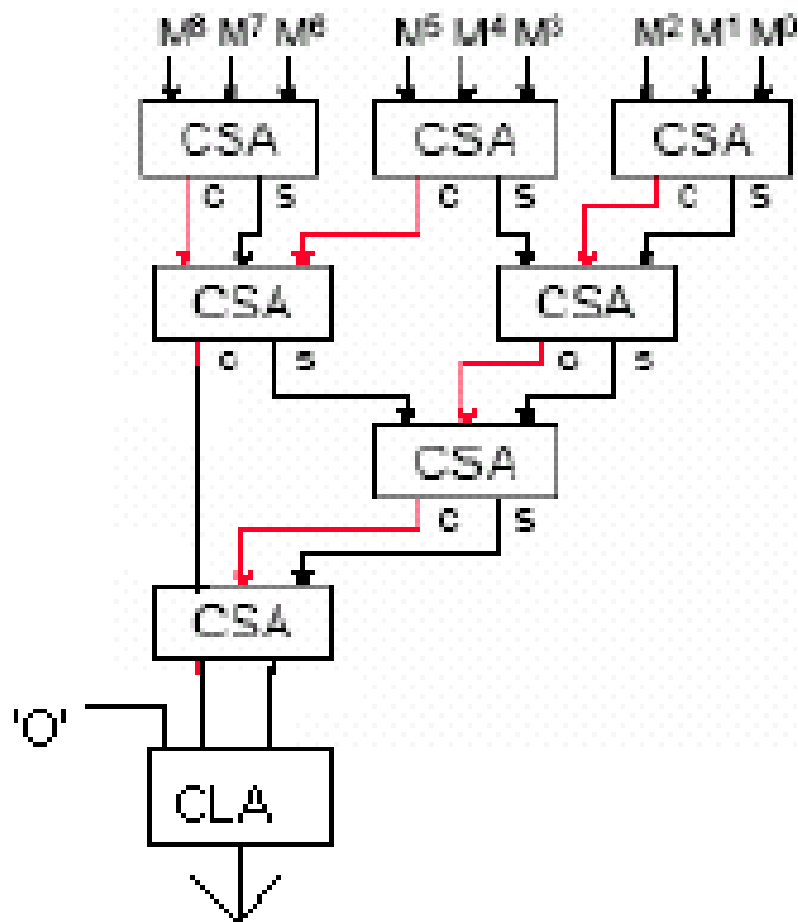


OUTPUT BLOCK

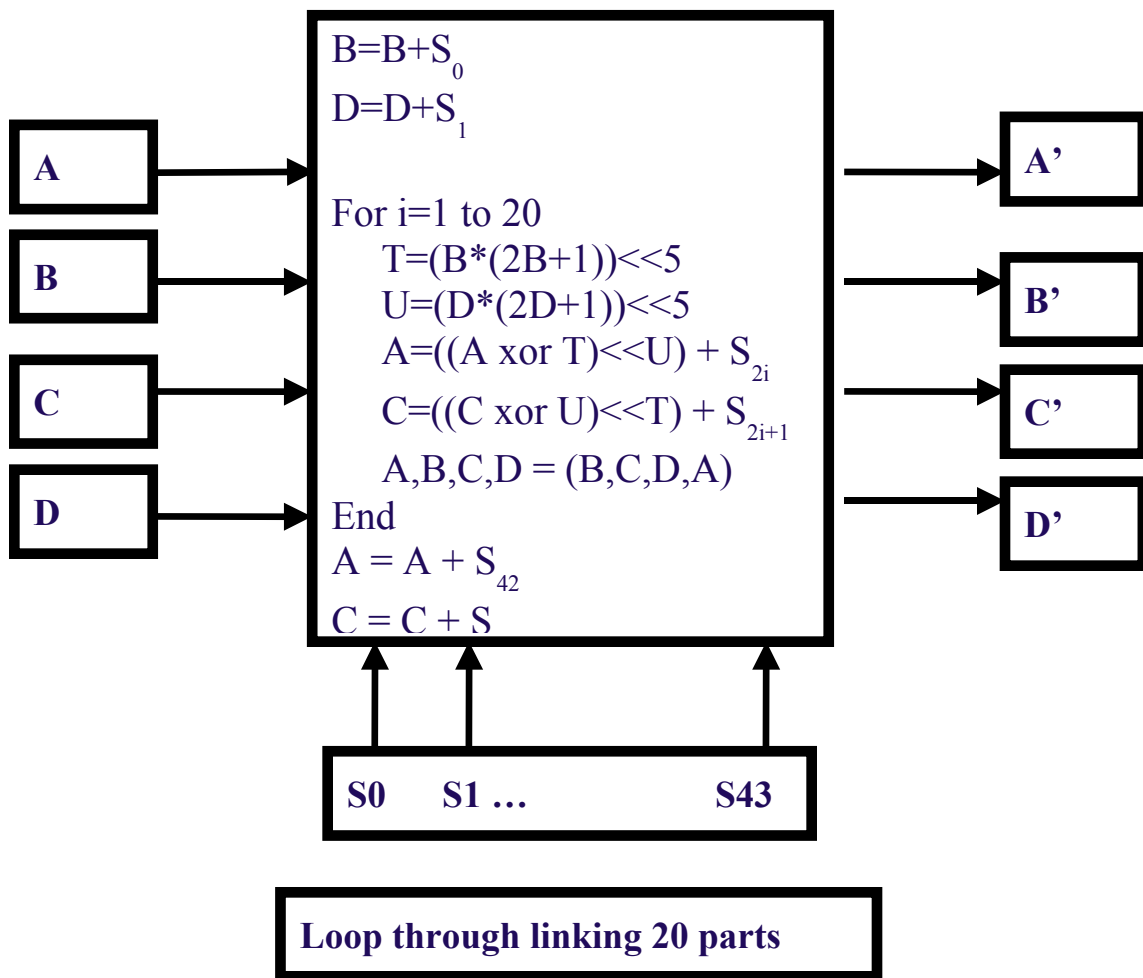




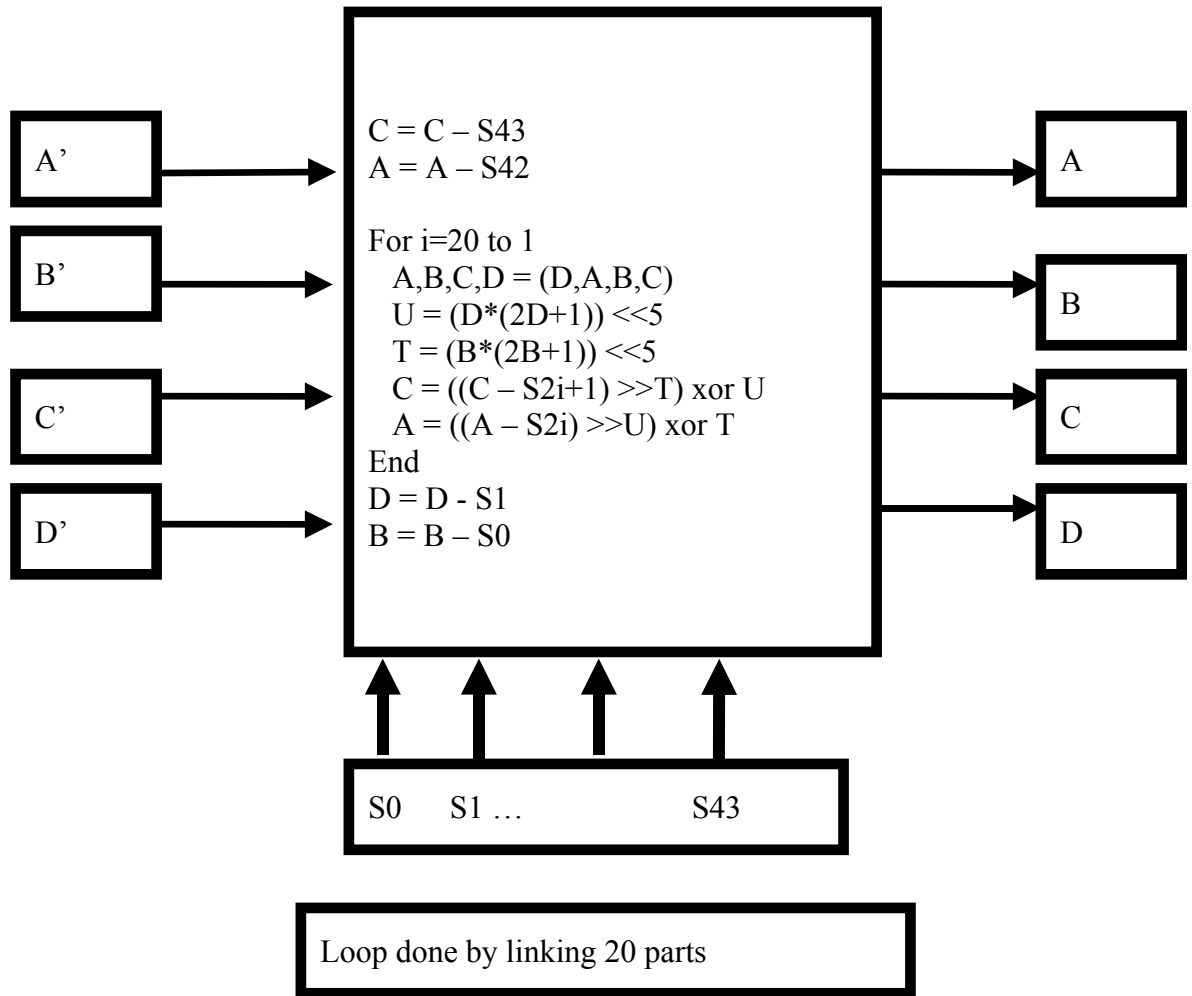
WALLACE TREE



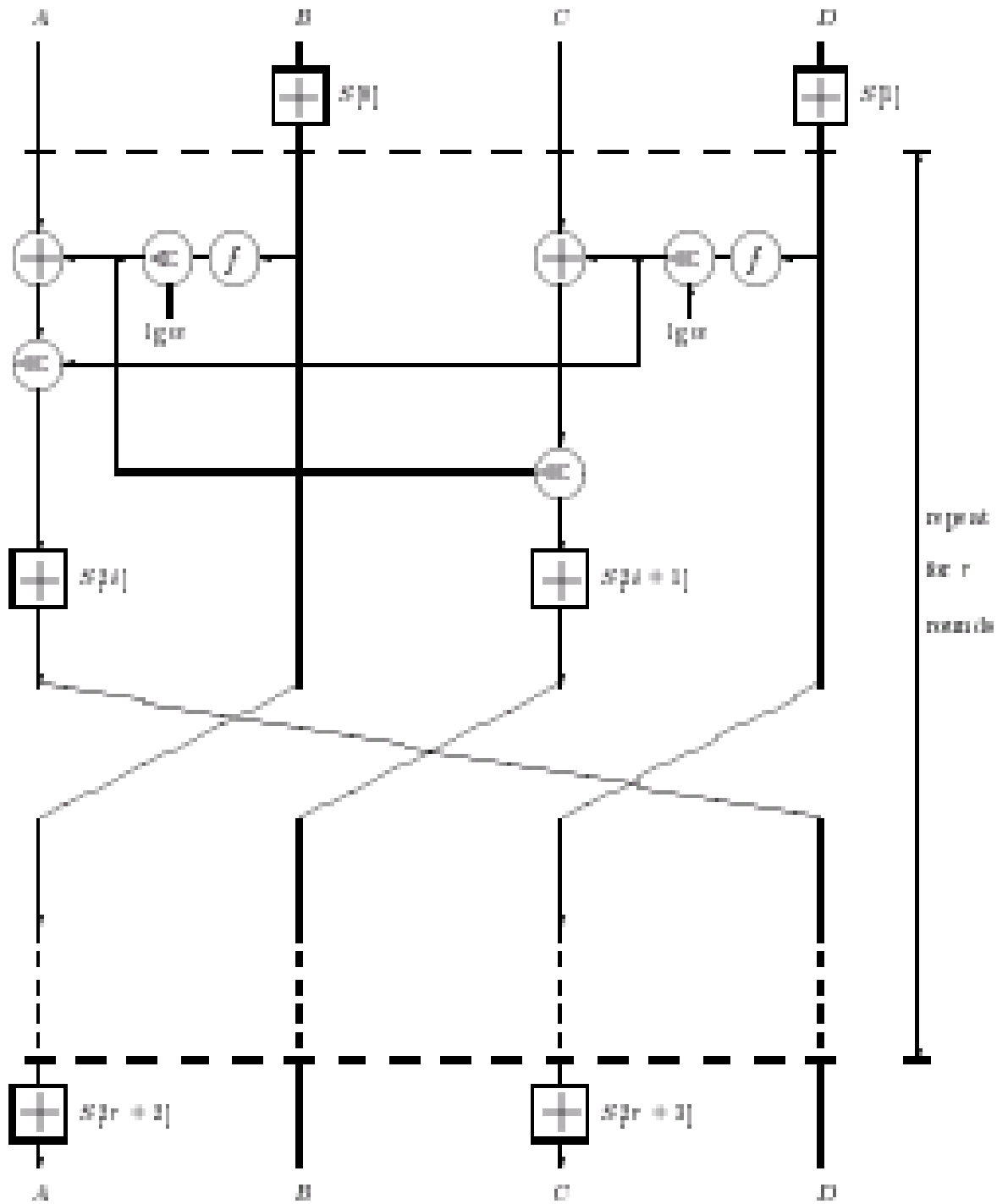
ENCRPTION ALGORITHM



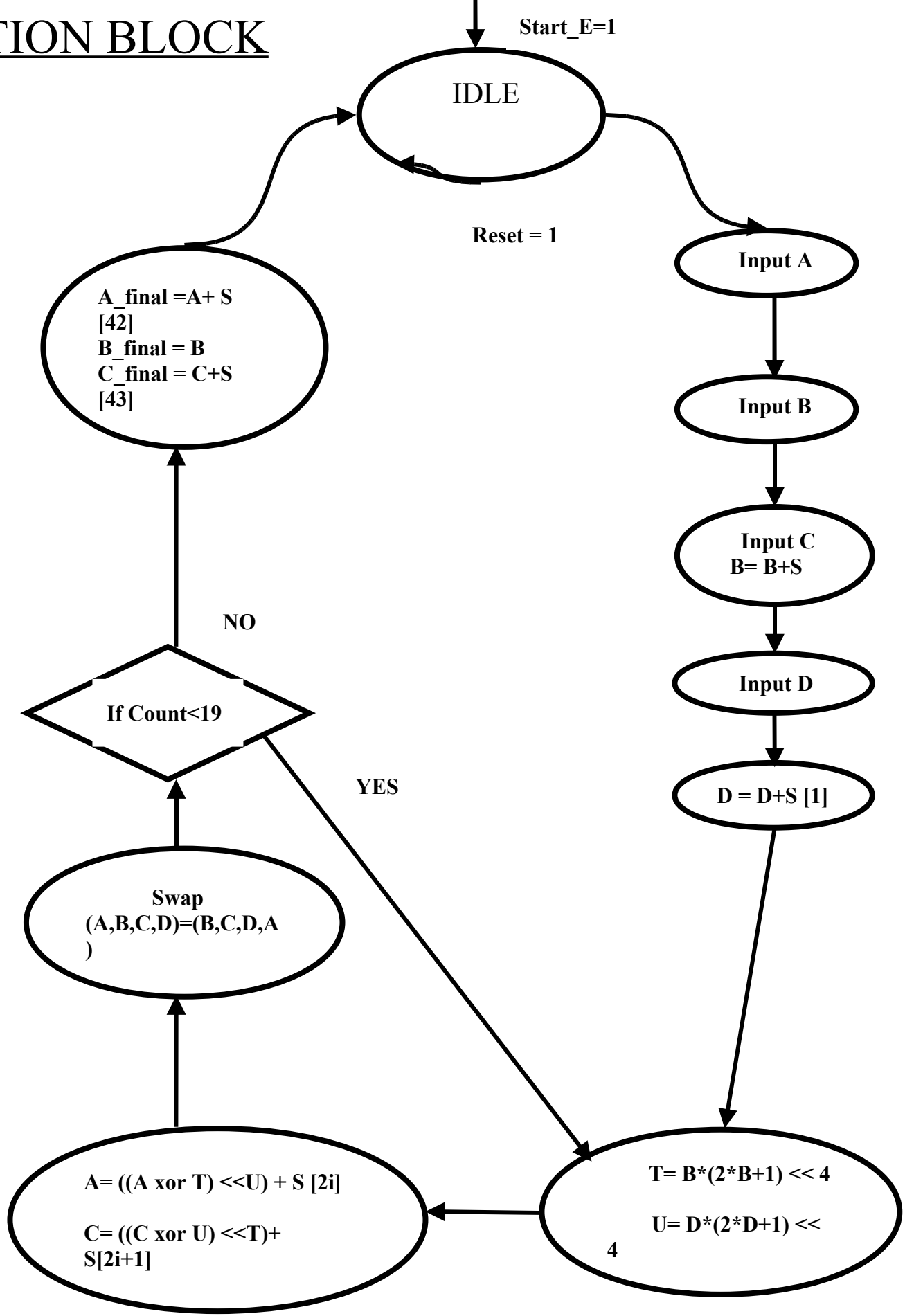
DISCRYPTION ALGORITM



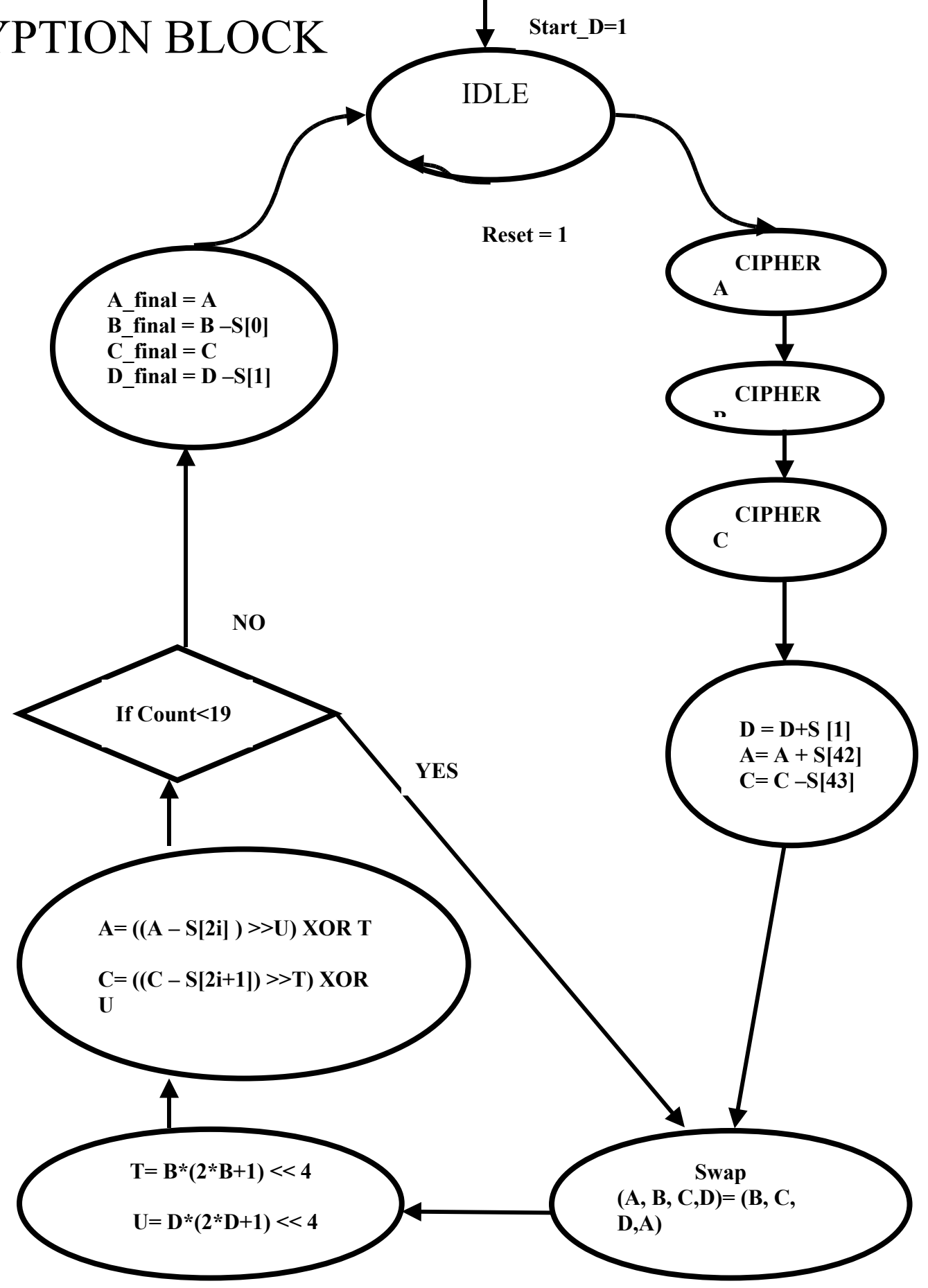
FLOW CHART



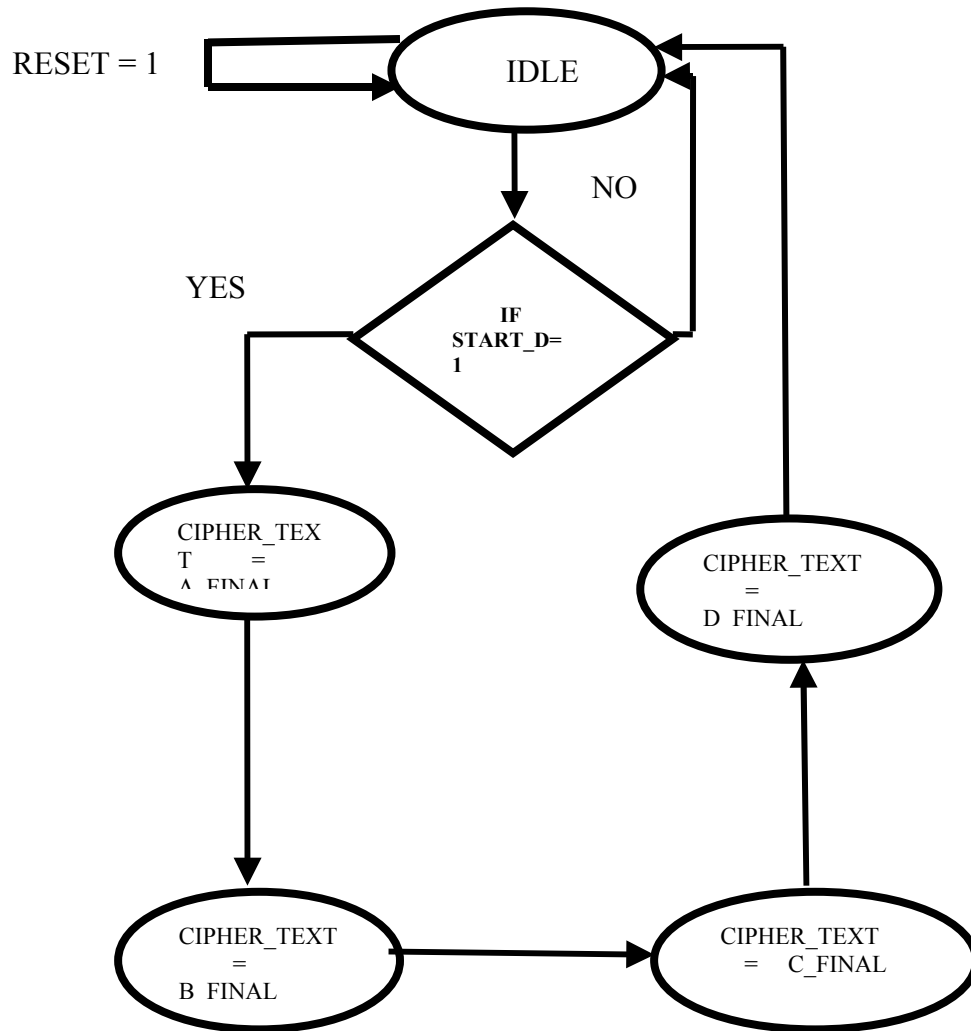
ENCRYPTION BLOCK



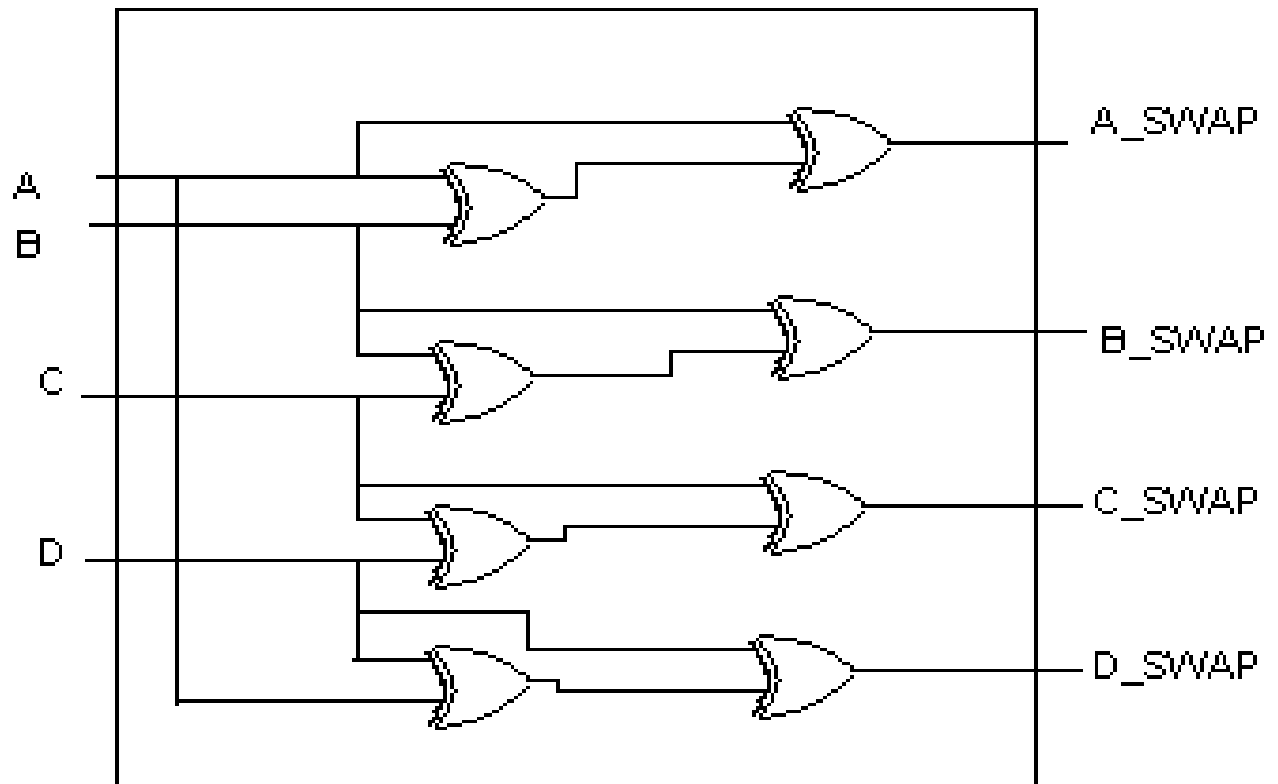
DISCRIPTION BLOCK



OUTPUT FSM



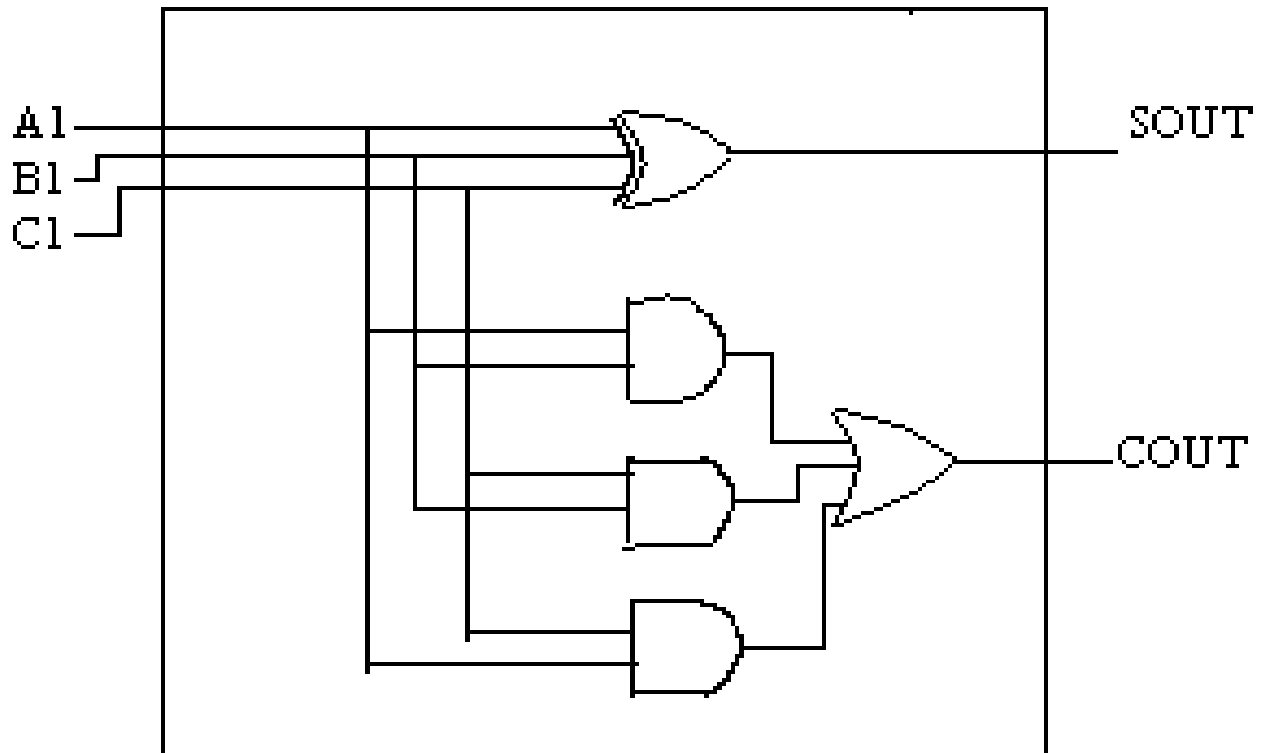
INTENAL BLOCK



SWAP OPERATION

INTENAL BLOCK

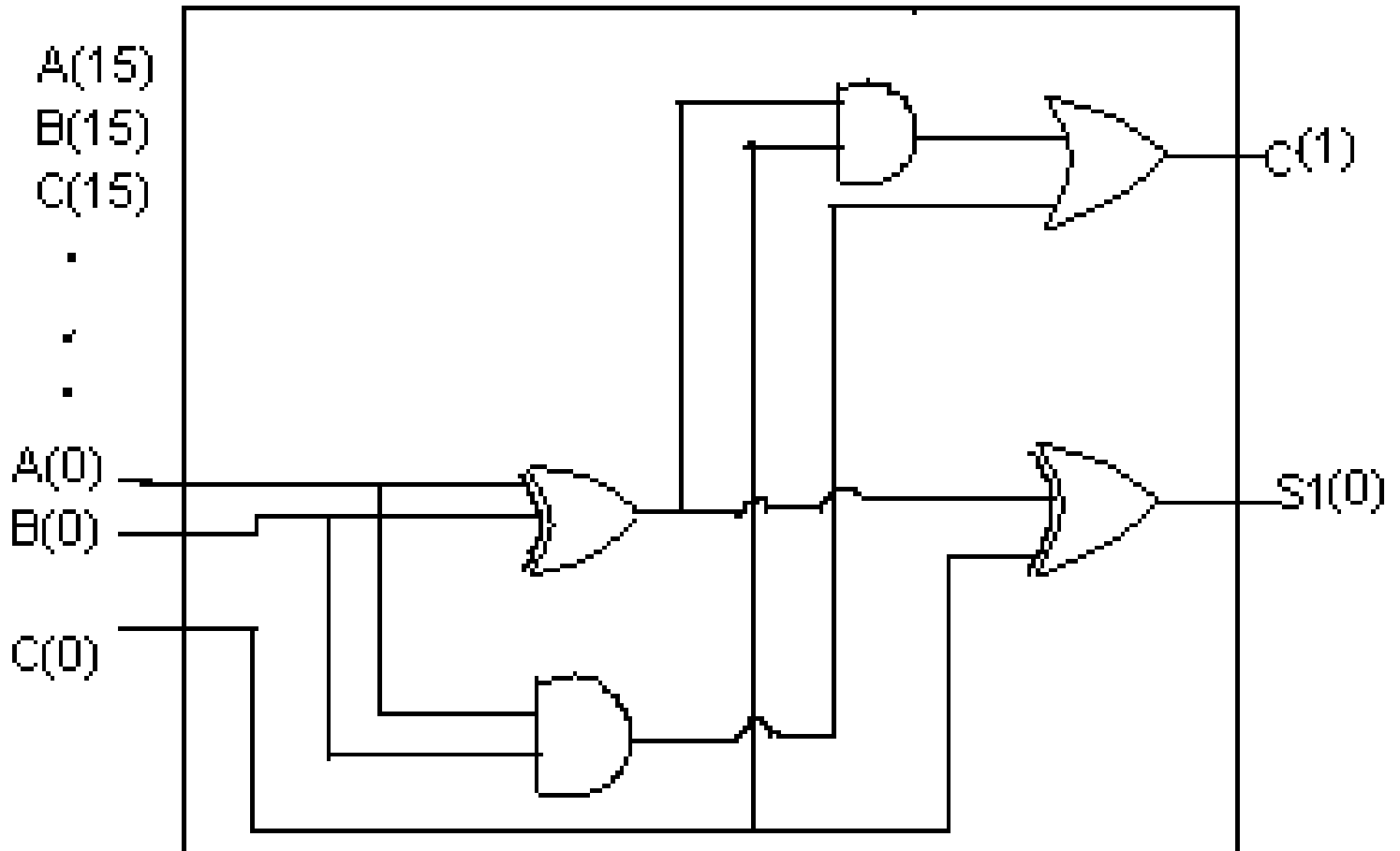
CARRY SAVE



CARRY SAVE

INTERNAL BLOCK

CARRY LOOK AHEAD



ENCRYPTOR O/P FSM

KEY SCHEDULING FOR RC6-w/r/b

Inputs:

User-supplied b byte key preload into the c-word array L[0,.....,c-1]
Number r of rounds

Output :

w-bit round keys S[0,.....,2r+3]

Procedure:

$s(0) \leftarrow P$;

-- initialize constant array

$l(0) \leftarrow (\text{round_keyse} + s(0))$;

$s(1) \leftarrow (l(0) + s(0) + q)$;

$l(1) \leftarrow (l(0) + s(1))$;

In general:

$S(i) = l(i-1) + s(i-1) + q$;

$L(i) = l(i) + s(i)$;