CIPHER Circuit
Specification

Specification:

The **CIPHER** circuit is specified below using its:

1. Pseudocode
2. Table of input/output ports
3. Timing requirements.

1. Pseudocode:

```
A = I3; B = I2; C = I1; D=I0
B = B + S[0]
D = D + S[1]
for i = 1 to r do
{
        T = (B*(2B + 1)) <<< k
        U = (D*(2D + 1)) <<< k
        A = ((A ⊕ T) <<< U) + S[2i]
        C = ((C ⊕ U) <<< T) + S[2i + 1]
        (A, B, C, D)  =  (B, C, D, A)

}
A = A + S[2r + 2]
C = C + S[2r + 3]
O = (A, B, C, D)
```

Notation:

w: word size, e.g., w=8 (constant)
k: $\log_2(w)$ (constant)
A, B, C, D, U, T: w-bit variables
I3, I2, I1, I0: Four w-bit words of the input I
r: number of rounds (constant)
O: output of the size of 4w bits
S[j] : 2r+4 round keys stored in two RAMs. Each key is a w-bit word. The first RAM stores values of S[j=2i], i.e., only round keys with even indices. The second memory stores values of S[j=2i+1], i.e., only round keys with odd indices.

Operations:
⊕ : XOR
+ : addition modulo 2^w
– : subtraction modulo 2^w
* : multiplication modulo 2^w
X <<< Y : rotation of X to the left by the number of positions given in Y
X >>> Y : rotation of X to the right by the number of positions given in Y
(A, B, C, D) : Concatenation of A, B, C, and D.

2. Table of input/output ports:

Port	Width	Meaning
clk	1	System clock.
reset	1	System reset – clears internal registers.
I	4w	Input block.
write_I	1	Synchronous write control signal for the input block I. After the block I is written to the CIPHER unit, the encryption of I starts automatically.
Sj	w	Round key S[j] loaded to one of the two internal memories.
write_Sj	1	Synchronous write control signal for the round key S[j].
j	m	Index of the round key S[j] loaded using input Sj.
O	4w	Output block.
DONE	1	Asserted when the output O is ready.

Note:
m is a size of index j. It is a minimum integer, such that $2^m - 1 \geq 2r+3$.

3. Timing Requirements:

Assume that

- **2r+4 clock cycles are used to load round keys to internal RAMs**
- **r+2 clock cycles are used for encryption of a single message block of the size of 4w bits.**

Task 1

Draw a block diagram of the Datapath of the CIPHER circuit. Use medium complexity components corresponding to the operations used in the pseudocode.
Clearly specify

- **names, widths and directions of all buses**
- **names, widths and directions of all inputs and outputs of the logic components.**

Assume that one round of the main for-loop of the pseudocode executes in one clock cycle.

Minimize the number of control signals to be generated by Control Unit.

Mark the most likely critical path in your circuit.

Task 2

Draw an interface of the CIPHER circuit with the division into Datapath and Controller.