Task-3 (LDES)

Task-3 (LDES)

Ⅰ

C

rotate left

A_0	B_0

f ← K_2

$+$

A_1	B_1

f ← K_1

$+$

A_2	B_2

B_2	A_2

rotate right

M (4 bits)