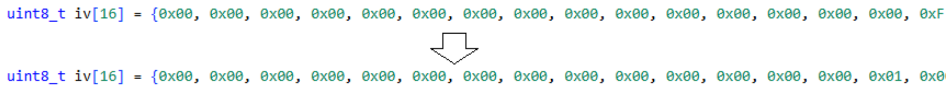
Lab 5 exercises

June 26, 2025

1. Implement missing AES cipher modes (from previous lab).

2. Working with big numbers.

    a. In cryptography, working with big numbers that exceeds usual data types size is common. Even simple operations have to be performed on buffers. Implement a function that increments a counter on 16 bytes.



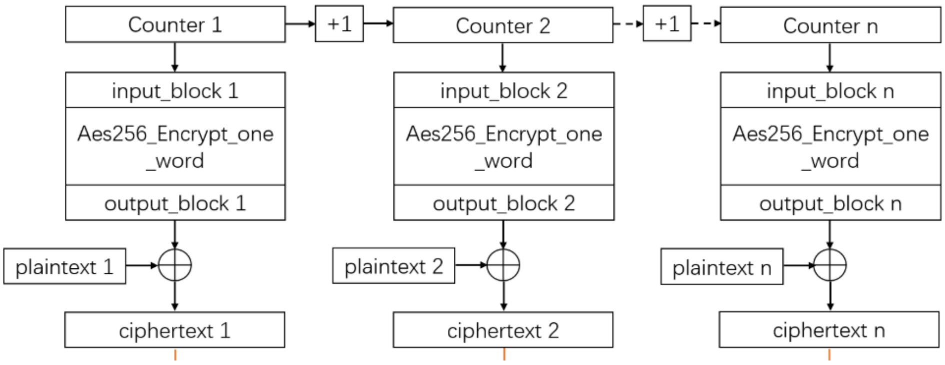
```
uint8_t iv[16] = {0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xF

uint8_t iv[16] = {0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x01, 0x0
```

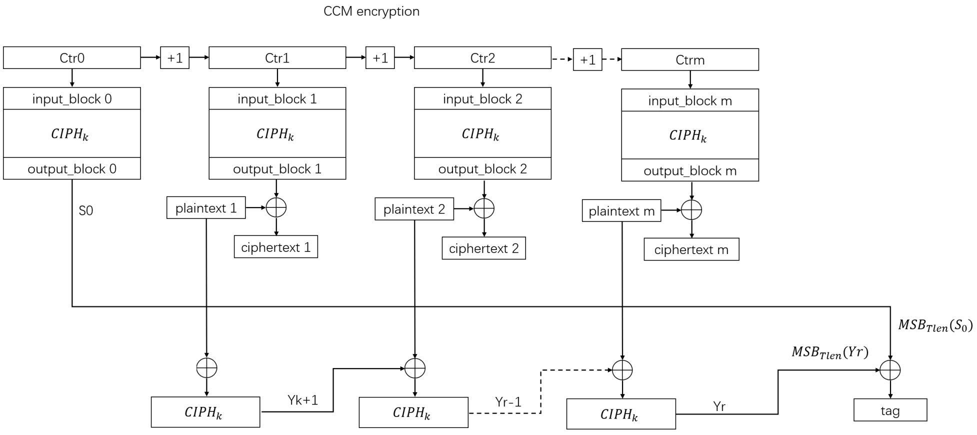
    b. Create test scenarios to check the implementation. What happens at overflow?

    c. Optional: Implement big number multiplication (find a way to multiply numbers on e.g. 30 bytes each).

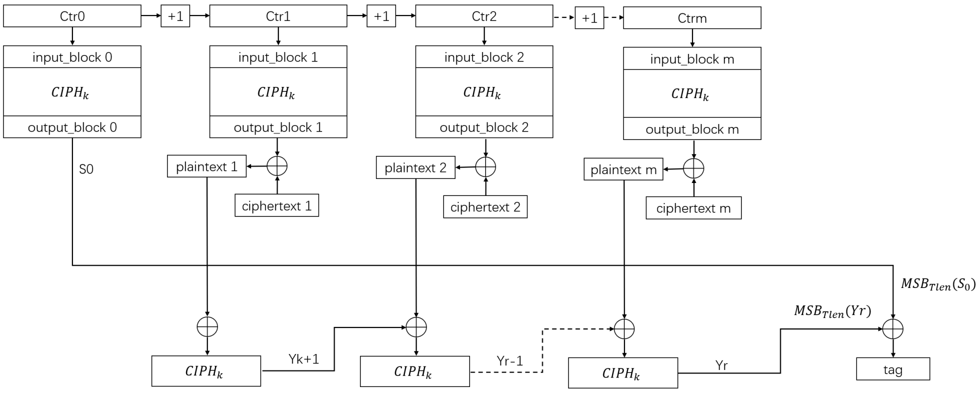
3. Implement CTR mode of operation. CTR (Counter) mode uses a counter value that is encrypted with a block cipher. The resulting ciphertext is then XORed with the plaintext to produce the final encrypted output. The counter is incremented for each block of plaintext.



4. Using the already implemented Cipher, implement the AES CCM (simplified) operation mode presented below.



CCM decryption


Ctr0
+1
Ctr1
+1
Ctr2
+1
Ctrm
input_block 0
$CIPH_k$
output_block 0
input_block 1
$CIPH_k$
output_block 1
input_block 2
$CIPH_k$
output_block 2
input_block m
$CIPH_k$
output_block m
S0
plaintext 1
ciphertext 1
plaintext 2
ciphertext 2
plaintext m
ciphertext m
$MSB_{Tlen}(S_0)$
$MSB_{Tlen}(Yr)$
$CIPH_k$
Yk+1
$CIPH_k$
Yr-1
$CIPH_k$
Yr
tag