Problem 10. «AES-GCM»

Alice is a student majoring in cryptography. She wants to use AES-GCM-256 to encrypt the communication messages between her and Bob (see the next page for a description of AES-GCM-256). The message format is as follows:

However, Alice made some mistakes in the encryption process since she is new to AES-GCM. Your task is to attack the communications.

Q1 You intercepted some messages sent by Alice. You can find these messages in the directory "Task_1".

Moreover, you know that the plaintext (unencrypted payload) of the first message (0.message) is "**Hello, Bob! How's everything?**" (without quotes, encoded in UTF-8).

Try to decrypt any message in the directory "Task_1".

Q2 In this task, you further know that the AAD (additional authenticated data) used by Alice in each message is Header || Initialization Vector:

You want to tamper some messages in the directory "Task_2".

You pass this task if you can modify at least one bit in some message so that Bob can still decrypt the message successfully.

Q3 Alice has noticed that the messages sent by her have been tampered with. So she decides to enhance the security of her encryption process.

Instead of using Header || Initialization Vector as the additional authenticated data (AAD), Alice further generates 8 bytes data X by some deterministic function f and the AES secret key K, where

$$X = f(K).$$

In each message, she uses Header || Initialization Vector || X as the AAD.

You also intercepted some messages sent by Alice, see these messages in the directory "Task_3". Try to tamper any message!

Q4 **Bonus problem (extra scores, a special prize!)**

You have successfully tampered with the messages in Q2. However, the attacks will be easy to detect if the tampered message cannot be decrypted to some meaningful plaintext.

In this task, try to tamper the messages in Q2 so that the tampered message can still be decrypted to some plaintext that people can understand. **Remark:** Tampering with the Header or Initialization Vector of a message will not be accepted as a solution, you need to tamper with the encrypted payload to produce some other ciphertext which did not appear in any message included.

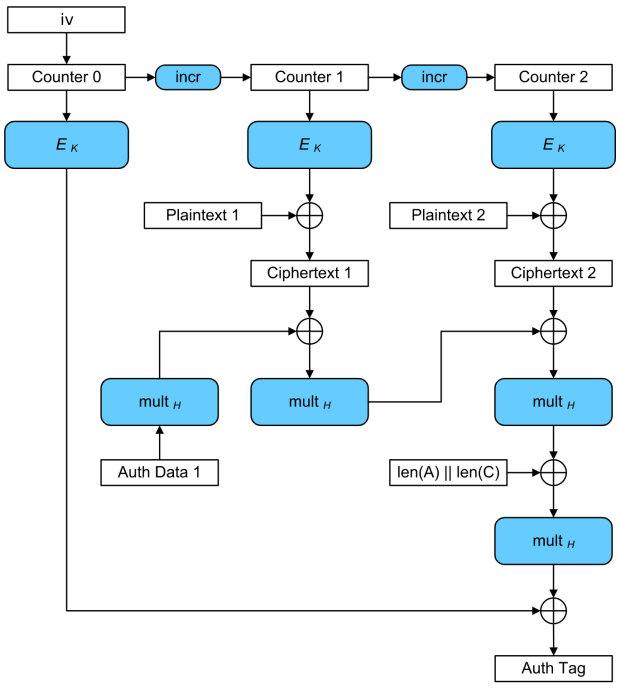
Turn to the next page.

Remark. In cryptography, Galois/Counter Mode (GCM) is a mode of operation for symmetric-key cryptographic block ciphers widely adopted for its performance.

The operation is an authenticated encryption algorithm designed to provide both data authenticity (integrity) and confidentiality.

Let us describe the AES-GCM algorithm. First, let us describe some notations used:

1. IV (Initializaton Vector) is a block of 96 bit; Alice arbitrarily chooses it before the encryption;
2. E_K is an AES-256 encryption function, operating on the blocks of 128 bits and encrypting them using the key K;
3. $mult_H$ is the multiplication operation. It multiplies an input block and a block H of 128 bits as numbers in a Galois field of order 2^{128}; the result is a 128-bit block;
4. H is the result of an AES-256 encryption of the 128-bit all-zero vector;
5. $incr$ is a certain (non-secret) increment function, which transforms blocks of 128 bits into blocks of 128 bits;



The *encryption* is performed as follows:

1. First, Alice chooses IV and splits the plaintext P into the blocks of 128 bits: $P = P_1||P_2||\dots||P_{n-1}||P_n$. The last block is not padded, let us denote the length of it by r;
2. The vector IV is transformed into a 128-bit block CB_0 (Counter 0 on the picture);
3. For $i = 1, \dots, n$, the block CB_{i-1} is incremented into the block CB_i; the latter is then encrypted with AES encryption E_K and summed with the block P_i of the plaintext using bitwise XOR operation. The result is the block C_i of the ciphertext;
4. For the last block, only the r leftmost bits of the encrypted block CB_n are summed with P_n;
5. The resulting ciphertext is the concatenation of the obtained blocks: $C := C_1||C_2||\dots||C_{n-1}||C_n$.

The *Authentication Tag* is obtained as follows:

1. The block of Additional Authentication Data is multiplied with $mult_H$, resulting in a block Y_0;
2. For $i = 1, \dots, n$, the block C_i of the ciphertext is summed with the block Y_{i-1}; the sum is then multiplied using $mult_H$ again, resulting in a block Y_i;
3. The block Y_n is summed with the block $len(A)||len(C)$, which consists of the encoded lengths of the AAD and of the ciphertext C; the result is once again multiplied using $mult_H$ and then summed with the AES-encrypted block CB_0; this gives us the Authentication Tag.

For more details of GCM, we refer to [1].

[1] Dworkin M. Sp 800-38d. Recommendation for block cipher modes of operation: Galois/counter mode (GCM) and GMAC. National Institute of Standards & Technology, 2007.