

## Problem 6. «CPA game»

Suppose we have a system for the encryption of binary messages. The system has the following characteristics:

- Every message is divided into blocks of length n that are called plaintexts (it is supposed that the length of messages is divisible by n).
- The system employs a block cipher with the encryption function E in cipher block chaining (CBC) mode (see the picture below). A block, an initialization vector IV and a key lengths are equal to n. The result of encryption of the message is a concatenation of IV and the ciphertexts of all plaintexts it consists of.
- The IV for the first message is chosen randomly by using a secure pseudorandom number generator. The last ciphertext block of the i-th message is used as the IV for the (i+1)-st message.

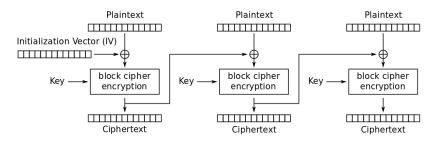
Let Alice be an honest user of the system. Victor, an adversary, convinced her to play chosen—plaintext attack game (CPA game) with him.

The game is the following:

- **1.** Alice selects a key  $k \in \{0,1\}^n$  and chooses a bit  $b \in \{0,1\}$ .
- **2.** Victor submits a sequence of q queries to Alice. For  $i = 1, 2, \ldots, q$  repeat
  - (a) Victor chooses a pair of messages,  $m_{i,0}, m_{i,1}$  of the same length.
  - (b) Alice encrypts  $m_{i,b}$  with the key k and gets  $c_i$  (the sequence of corresponding IV and ciphertexts). She sends  $c_i$  to Victor.
- **3.** Victor outputs a bit  $b^* \in \{0, 1\}$ .

Let W be the event that Victor guesses the bit, that is  $b^* = b$ . We define Victors's advantage with respect to E as CPAadv :=  $|\Pr[W] - 1/2|$ . Victor wins the game if he can build an efficient algorithm such that CPAadv is not negligible.

**Task**. Construct an efficient probabilistic polynomial-time (PPT) algorithm that wins the CPA game against this implementation with an advantage close to 1/2.



Cipher Block Chaining (CBC) mode encryption