Task 1. «WaterMarking Cipher»

Special Prize from the Program Committee!

Let X, Y and K be the sets of plaintexts, ciphertexts and keys respectively, where $X = Y = \{0,1\}^n$ and $K = \{0,1\}^m$ for some integer n and m. Recall that two functions $E : X \times K \to Y$ and $D : Y \times K \to X$ are called *an encryption algorithm* and *a decryption algorithm* respectively if for any $x \in X$, $k \in K$ it holds $D(E(x,k),k) = x$. Together E and D form *a cipher*.

Let us call a cipher *watermarking* if for any key $k \in K$ and any subset $I \subseteq \{1,2,\ldots,n\}$ there exists a key k_I such that for any $x \in X$ it holds

$$D(E(x,k),k_I) = x',$$

where x' is obtained from x by changing all bits with coordinates from I.

A simple example of such a cipher. Let $m = n$ and encryption and decryption algorithms be the following:

$$E(x,k) = x \oplus k \quad \text{and} \quad D(y,k) = y \oplus k.$$

For any set I and any key k we can easily get the key k_I that is obtained from k by changing all bits with coordinates from I. The main disadvantage of such a cipher that every key should be used only once.

How can we use a watermarking cipher? Suppose you own some digital products (for example, videos), which you want to sell. Let x represent a binary code of a product. For each customer of x you choose the unique set I of coordinates and send to him the encrypted with the key k copy y and the correspondent key k_I. Then after receiving y and k_I the customer decrypts y and gets x'. The difference between the original x and x' is not significant; thus the customer does not know about it. If someone illegally spreads on the Internet bought by him product, you can easily understand who do it because you choose the unique set I for each customer!

Summarize the ideas we need to construct a cipher that has to put into the video something like a «watermark». Lets try! So, the task is to construct a watermarking cipher. Please think about easy usage of it for an owner and a customer.