UDC 004.021

DESIGNING GUI SYSTEM FOR HIDING INFORMATION USING HYPERBOLIC FUNCTIONS

ALIAKSEI SMALIAK, DMITRY PASTUKHOV
Polotsk State University, Belarus

This article discusses designing the GUI system for hiding information using hyperbolic functions. The analysis of the degree of suitability of a container for modifications, modeling and determination of resistance to them.

Need for hiding information from mankind appeared very long ago. However, with the advent of the need for hiding information, and the need for breaking ciphers. The Cryptology, the science of creating and breaking ciphers.

The interface of the program should possess a number of characteristics: naturalness, consistency, friendliness, simplicity, flexibility, aesthetic appeal.

«ExponentLog» is an application to hide information. In the interface presented 3 encryption key for each key has 2 functions, parameter 3 to choose from: hyperbolic cosine (1) and hyperbolic sine (2).

To hide messages you will need to type in the text for encryption in the fieldInputtext, choose the encryption keys and 9 function k, click Coding. After clicking filling status bar appears and the text will be encrypted.

When the buttonDecoding is clicked, decoding the message occurs.

However, if you change at least 1 of 9 decryptedkey message will be changed.

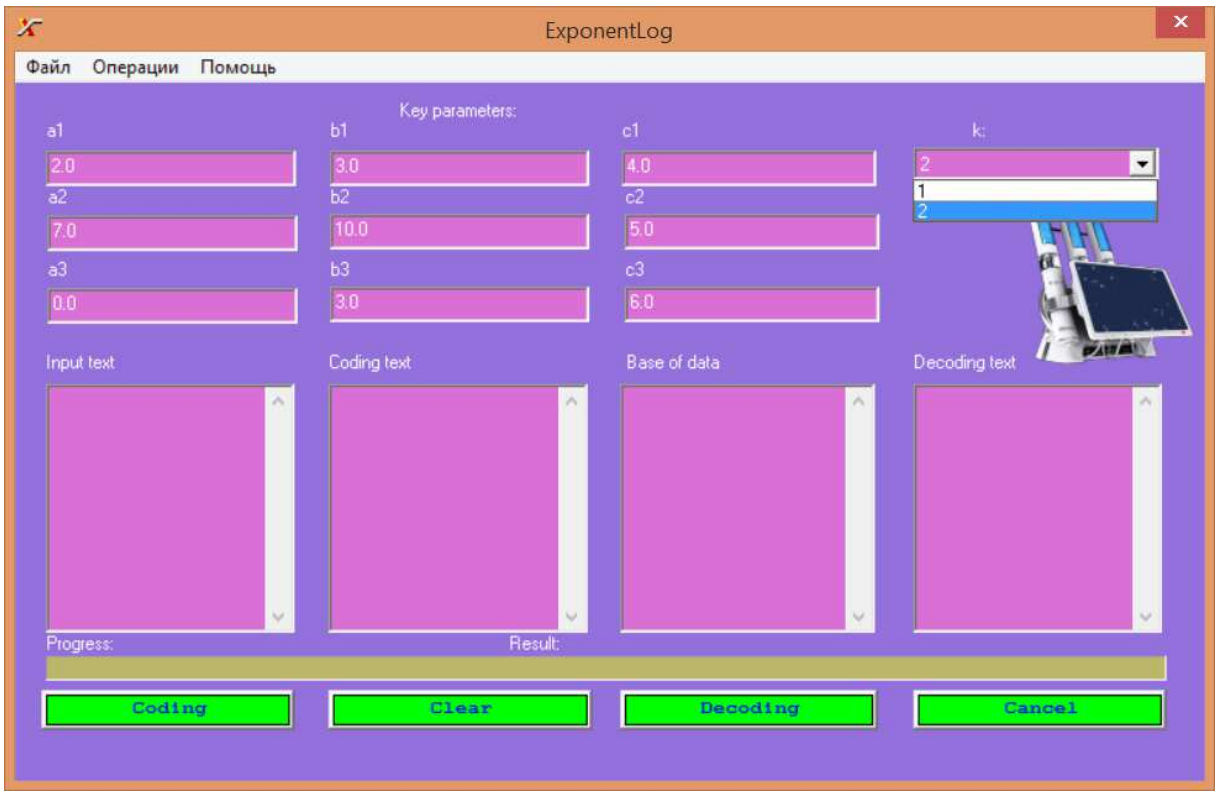

Figure 1. – Program interface

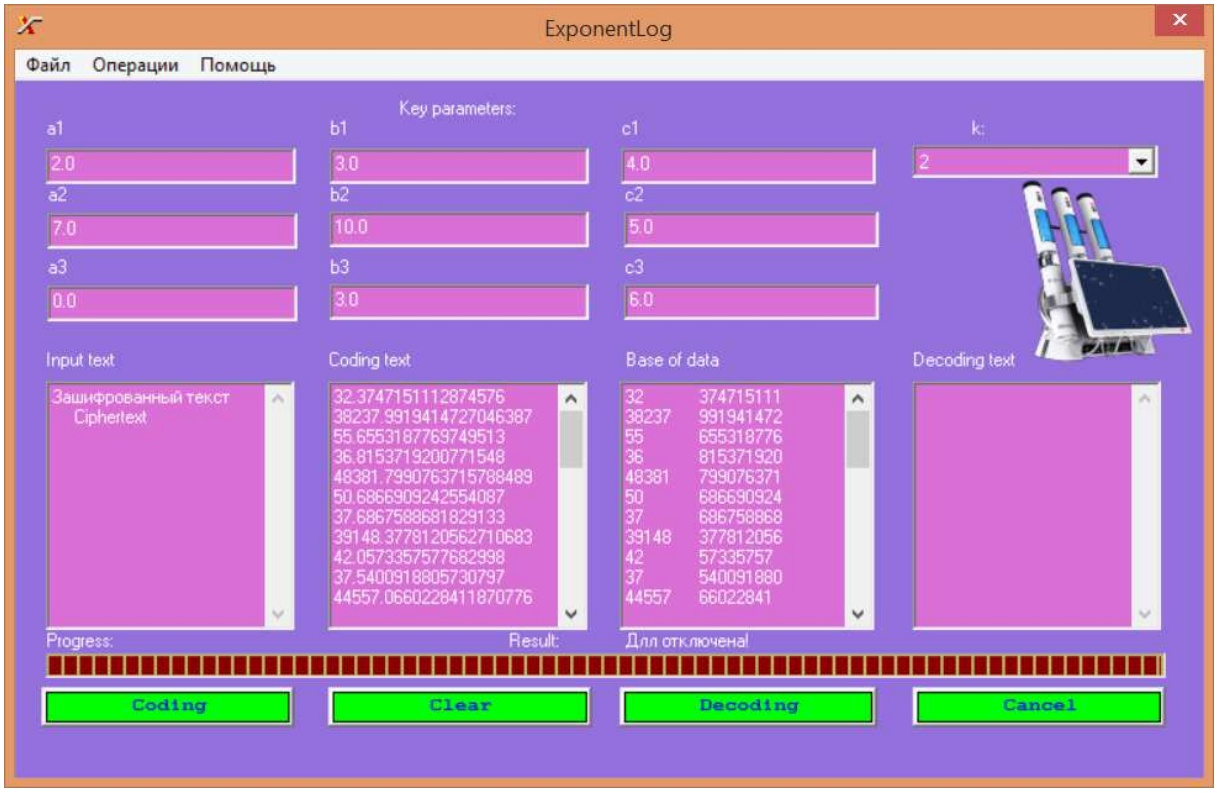

Figure 2. – Encryption Interface

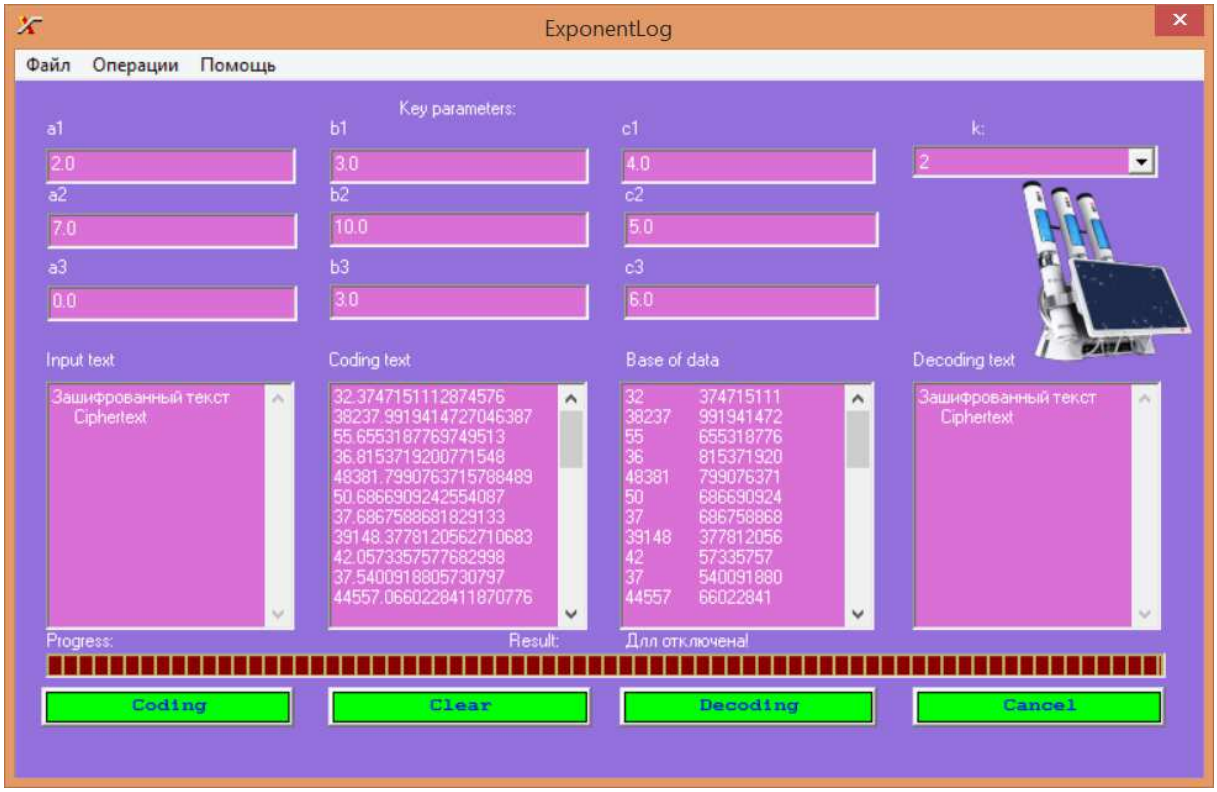

Figure 3. – Decryption Interface

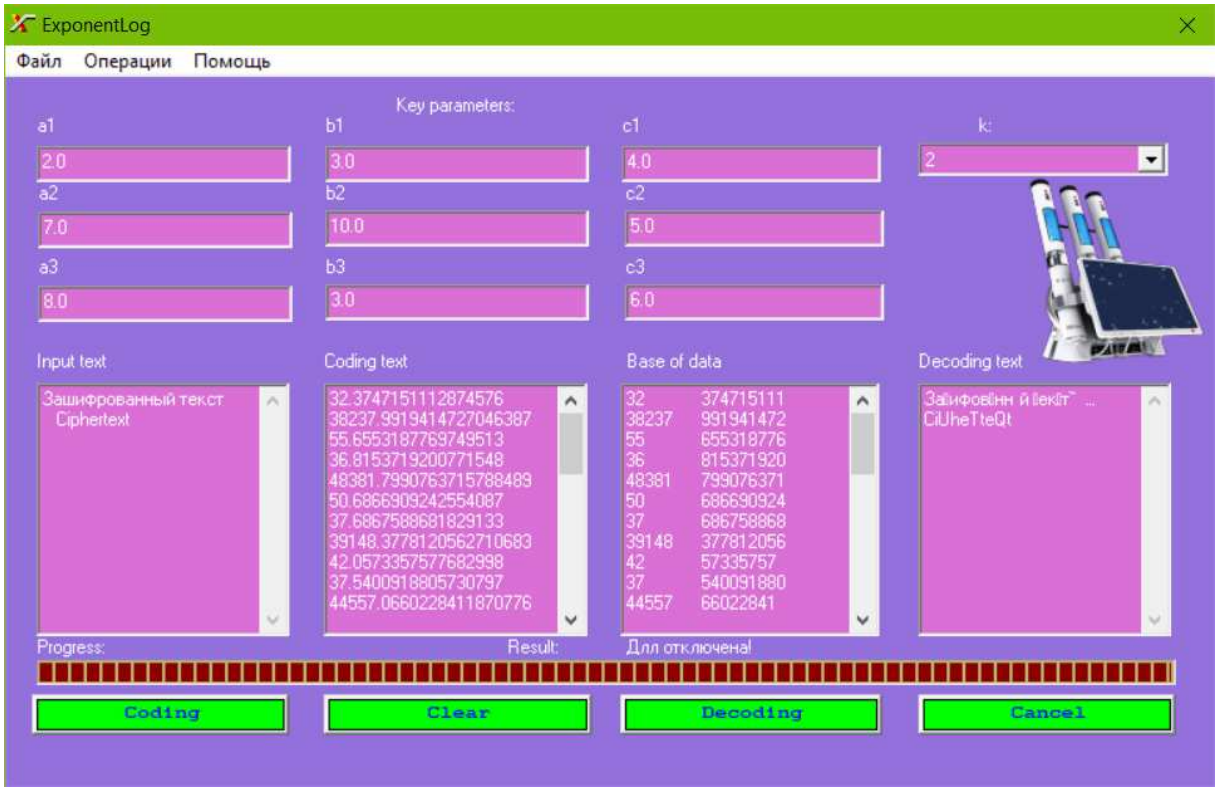

Figure 4. – Error in decrypted text if you change key parameters

Incrediblygreatciphersensitivityrelativelysmall$10^{-10}-10^{-12}$keychanges $(Left, raight, a), (left, raight, n)$, provides greater dimensionality of space distribution of the keys. If the supercomputer cryptanalyst picked up the keys to the fixed code nonlinear functions with speed$10^9 \frac{1}{sec}$, would require hacking time, exceeds the lifetime of the Earth (more than 5 billion years old). Such a large dimension is guaranteed by the use of double-precision (double) for the arguments and nonlinear functions. Indeed, a single range of one key parameter can be placed10^{16}different ciphers. Strong encryption of nonlinear functions is ensured by two reasons: big dimension key space, a large set of nonlinear functions with "floating" scoped-line, which allows on the one hand increase key space, and on the other hand increase the strong encryption.

Thereare 2 classesofnon-linear functions. They were used in this application: the hyperbolic sine and hyperbolic cosine. Applied algorithms in the program can be used to store passwords in the database with a length of up to several hundred-thousand characters. Adding randomization algorithms to encrypt nonlinear functions makes applied algorithms invulnerable to cryptanalyst.

In this article, you learned how to build a graphical interface of the system on the basis of information hiding nonlinear functions, proved on analysis of the reliability of non-linear encryption functions.

REFERENCES

1. Матюшик, В.Н. Методы и средства стеганографии для защиты графических образов / В.Н. Матюшик. – Минск :БГУР.
2. Грибунин, В.Г. Цифровая Стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М. : СОЛОН-Пресс, 2002. – 272 с.
3. Конанович, Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – Киев : МК-Пресс, 2006. – 288 с.