MATERIALS OF XI JUNIOR RESEARCHERS' CONFERENCE

ITC, Electronics, Programming

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.

x	Expon	entLog	×
Файл Операции Помощь			
a1 20 a2 7.0 a3 0.0	Key parameters: 51 52 10.0 53 3.0	c1 4.0 c2 50 c3 6.0	k 2 1 2
Input text	Coding text	Base of data	Decoding text
Progress:	Result:		
Coding	Clear	Decoding	Cancei

Figure 1. – Program interface

2019

MATERIALS OF XI JUNIOR RESEARCHERS' CONFERENCE

2019

ITC, Electronics, Programming

Файл Операции Помощь a1 b1 c1 k; 20 3.0 4.0 c2 a2 b2 c2 c2 7.0 10.0 5.0 a3 b3 c3 0.0 3.0 8.0 Input text Coding text Base of data Decoding text 3auu4ppoe3aretush Texct 32.3747151112874576 32.27 991941472 5b555187768749513 38.8153719200771548 32.27 991941472 43381 793075371 Cphertext 55.055318776824951 50 665538968182133 20 39148 37781205637 21 5735775 22 5735777822986 .	ς.	Expo	nentLog	×
a1 b1 c1 k; 20 30 40 2 a2 b2 c2 - 70 10.0 50 - a3 b3 c3 - 0.0 30 60 - Input text Coding text Base of data Decoding text 322.3747151112874576 32.3747151112874576 32.374715111 - 38237<9919414727046387 55 655318776 32.374715111 Cphertest 32.6575878819513 32.374715111 - 39148.377812056 33148.377812056 - - 39148.3778120562715788489 50 866590924 - 50 866590924 - - - 50 866590924 - - - 39148.377812056 42 57335757 - - 4557.06602284118/07793 - - - - 4557.06602284118/07793 - - - - 4557.06602284118/07793 - - - -	Файл Операции Помощь			
20 30 4.0 2 a2 b2 c2 7.0 10.0 5.0 a3 b3 c3 0.0 30 6.0 Input text Decoding text 3auxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx		Key parameters: b1		
a2 b2 c2 7.0 10.0 5.0 a3 b3 c3 0.0 3.0 6.0 Input text Coding text Base of data Decoding text 3auxHoppoBaHHbiR Tek cr 32.3747151112874576 32.374715111 Decoding text 3auxHoppoBaHHbiR Tek cr 32.3747151112874576 32.374715111 Decoding text 3auxHoppoBaHHbiR Tek cr 32.3747151112874576 32.37 991341472 Decoding text 3auxHoppoBaHHbiR Tek cr 32.3747151112874576 382.37 991341472 Decoding text Set Sister Si	2.0	3.0	4.0	2
7.0 10.0 5.0 a3 b3 c3 D.0 3.0 6.0 Input text Coding text Base of data Decoding text 3auHx4ppoBaHHbiRTekct 32.3747151112874576 38237 991941472 56553187765 3b2 Sof	a2	b2	c2	200
a3 b3 c3 D.0 3.0 B.0 Input text Coding text Base of data Decoding text Jauxuxopposarineian rekort Ciphertext 32,3747151112874576 38237,9919414727046387 55,66553187769749513 38,8153719200711548 48381,7990763715788489 50,68865909242554091 37,6867588681829133 39148,377812056 32,374715111 0 Jauxuxopposarineian rekort Ciphertext 32,3747151112874576 38237,991941472 32,374715111 0 Saturite rekort Ciphertext 32,3747151112874576 38237,991941472 32,374715111 0 0 Progress: Result: 33,9148,377812056 37,5400918805730797 44557,0660228411870776 32,57335757 37,540091880 33,9148,377812056 37,540091880 33,9148,377812056 32,57335757 Progress: Result: Длл отключена! Длл отключена!	7.0	10.0	5.0	0404 <u>0</u>
0.0 3.0 6.0 Input text Coding text Base of data Decoding text Зашикфрованный текст 32.3747151112874576 32.374715111 38237 931941472 Decoding text Зашикфрованный текст 32.3747151112874576 38237 931941472 Decoding text Decoding text Зашикфрованный текст 38.2153719200771548 38237 931941472 Decoding text Decoding text S6.6553187769749513 36.8153719200771548 38231 7990763715708489 Decoding text Decoding text S6.8655092425540913 37.6867588680 39148.3778120566 42.57335757 S148.3778120566 42.57335757 S148.3778120566 42.57335757 S148.3778120566 42.5736727 S148.377812056 44557.660228411 Decoding text Deco	a3	63		
Input text Coding text Base of data Decoding text Зашинфрованный текст 32,3747151112874576 38237,9919414727046387 55,6553187769749513 36,815371920071548 48381,7990763715788489 50,6866909242554087 37,68657888681829133 39148,377812056 37,5400918805730797 44557,0660228411870776 322,374715111 38237,991941472 55,655318776 36,815371920 Decoding text Progress: Result Длл отключена! 1	0.0	3.0	6.0	
Зашинфрованный текст Ciphertext 32.3747151112874576 38237.9919414727046387 55.6553187763749513 36.8153719200771548 48381.7990763715788493 50.6866909242554087 37.6867588681829133 39148.3778120562710683 42.057357577682998 37.5400918805730797 44557.0660228411870776 32.374715111 38237.991941472 55.655318776 36.815371920 48381.799076371 50.6866590924 37.866758868 39148.377812056 42.57335757 37.540091880 44557.66022841 Progress: Result: Длл.отключенаl	Input text	Coding text	Base of data	Decoding text
Progress: Result: Для отключена!	Зашифрованный текст Ciphertext	32.3747151112874576 38237.9919414727046387 55.6553187769749513 36.8153719200771548 48381.7990763715788489 50.6865909242554087 37.6867588681829133 39148.3778120552710683 42.0573357577682998 37.5400918805730797 44557.0660228411870776	32 374715111 38237 991941472 55 655318776 36 815371920 48381 799076371 50 686580924 37 686758868 39148 377812056 42 57335757 37 540091880 44557 66022841	
	Progress:	Result:	Длл отключенаl	
Loding Clear Decoding Cancel	Coding	Clear	Decoding	Cancel

Figure 2. – Encryption Interface

	Ex	ponentLog	
айл Операции Помощи	5		
	Key parameters: b1		
2.0	3.0	4.0	2
a2	b2	c2	200
	10.0	5.0	<i>n</i> m H
a3	b3	c3	A Com
	3.0	6.0	
Input text	Coding text	Base of data	
Зашнфрованный текст Ciphertext	 32.3747151112874576 38237.9919414727046387 55.6553187769749513 36.8153719200771548 48381.7990763715788489 50.6865909242554087 37.6867588681829133 39148.3778120562710683 42.0573357577682998 37.5400918805730797 44557.0660228411870776 	32 374715111 38237 991941472 55 655318776 36 815371920 48381 799076371 50 686590924 37 686758868 39148 377812056 42 57335757 37 540031880 44557 66022841	Зашифрованный текст 🧖 Ciphertext
Progress:	Result	Длл отключенаl	
Coding	Clear	Decoding	Cancel

Figure 3. – Decryption Interface

MATERIALS OF XI JUNIOR RESEARCHERS' CONFERENCE

ITC, Electronics, Programming TexponentLog Файл Операции Помощь -62 a2 c2 Base of data Decoding text Input text Coding text ашифрованный текст Ciphertext Заїифовінн й Іекіл SiUheTteQt ~ ~

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 placed 10^{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.
- Конанович, Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. Киев : МК-Пресс, 2006. – 288 с.