Impact Factor:	ISI (Dubai, UAE) = 0.829 GIF (Australia) = 0.356	SIS (USA) = 0.912 РИНЦ (Russia) = 0.179 ESJI (KZ) = 1.042 SJIF (Morocco) = 2.031	ICV (Poland)	= 6.630
SOI: <u>1.1/T</u>	AS DOI: <u>10.15863/TAS</u>		Alexandı	Shevtsov
International Scie	entific Journal		ididate of technica	,

- 1 244 STE (UEA)

candidate of technical sciences, member of PILA (USA), Department of «Mathematics», Deputy Director on Science of FITAT, Taraz state University named after M.Kh. Dulati, Kazakhstan Shev_AlexXXXX@mail.ru

Bakyt Turmakhanovich Bayeshov candidate of technical sciences, associate Professor, Taraz state University named after M.Kh. Dulati, Kazakhstan

ON ONE ALGORITHM FOR HOMOMORPHIC ENCRYPTION

Abstract: This paper discusses the implementation issues of homomorphic encryption algorithm in Delphi. The resulting algorithm allows to create a probability matrix of the ciphertext. The developed algorithm is efficient and test on the texts.

Key words: matrix, homomorphic encryption algorithm, encryption, delphi. Language: English

ISDA (India)

e-ISSN: 2409-0085 (online)

Theoretical & Applied Science

SECTION 2. Applied mathematics. Mathematical

Volume: 30

http://T-Science.org

Issue: 10

p-ISSN: 2308-4944 (print)

Published: 30.10.2015

Year: 2015

modeling.

Citation: Shevtsov AN, Bayeshov BT (2015) ON ONE ALGORITHM FOR HOMOMORPHIC ENCRYPTION. ISJ Theoretical & Applied Science 10 (30): 1-3. Soi: http://s-o-i.org/1.1/TAS-10-30-1 Doi: crosse http://dx.doi.org/10.15863/TAS.2015.10.30.1

Homomorphic encryption is a form of encryption that allows you to perform mathematical operations with the ciphertext and obtain an encrypted result that matches the result of operations performed in plaintext. For example, one person could add two encrypted numbers and then another person could decrypt the result, without using any of them. Homomorphic encryption would allow to unite in one whole a variety of services, without providing data for each service. Distinguish partially homomorphic and fully homomorphic cryptosystem. While partially homomorphic system allows only one operation — addition or multiplication, a fully homomorphic cryptosystem supports the simultaneous execution of both operations, which allows holomorphe to compute arbitrary Boolean circuits. [1-8]

The basic steps in the encryption:

- Imagine that we want to encrypt the number x (a small natural number).
- We will choose a random vector v (it will be our secret kev).
- Possible to find a row of the matrix A that will be true $A_i v = x$, i.e., the multiplication of A on v will give the number x.
- If we want to encrypt a new number y, then again you will find a row of the matrix A, such that $A_i v = y$. Thus we can, with only one secret key v, and encrypt any number of numbers where the code of each number is a string matrix.
- To decode the number, we multiply the matrix by the vector v secret.

		• •							
	(a_{11})	a_{12}	a_{13}	a_{14}	 a_{1j}		a_{1n}	(v_1
	a ₂₁	a_{22}	a_{23}	a_{24}	 a_{2j}		a_{2n}		<i>v</i> ₂
	<i>a</i> ₃₁	a_{32}	<i>a</i> ₃₃	<i>a</i> ₃₄	 a_{3j}		a_{3n}		<i>v</i> ₃
Λ —	a ₄₁	a_{42}	a_{43}	<i>a</i> ₄₄	 a_{4j}	••	a_{4n}	V =	v_4
					 •••			v –	
	a_{i1}	a_{i2}	a_{i3}	a_{i4}	 a_{ij}			-	v_j v_j v_n
	a_{m1}	a_{m2}	a_{m3}	a_{m4}	 		a_{mn})		(v_n)

It is obvious that the homomorphism for works not executed. Because with the algorithm of encryption is partially homomorphic. Due to the fact that the algorithm is being built with private key,

then you first need the secret key. The key length nmay vary depending on the desired strength. The interval [a,b] is also random.



1

	ISRA (India) = 1.344	SIS (USA) = 0.912	ICV (Poland)	= 6.630
Impost Easton	ISI (Dubai, UAE) = 0.829	РИНЦ (Russia) = 0.179		
Impact Factor:	GIF (Australia) = 0.356	ESJI (KZ) = 1.042		
	JIF = 1.500	SJIF (Morocco) = 2.031		

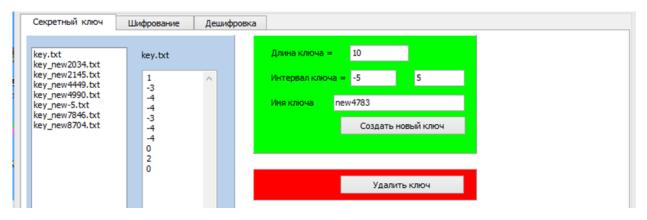


Figure 1 – Creating a secret key.

Секретный ключ	Шифрование	Дешиф	ровка	3												
ext — копия.txt ext.txt	Text.txt												Cou	int =	874	
	получать за Например, о Гомоморфно Различают В то время и	ашифрован один челов ое шифрова частично г как частич	ный р ек мо ание г омомо но гол	резуль г бы с позвол орфны моморо	лат, к ложит пило б е и по фная (соторы ть два ы объю олност	а позв	тветст рован ть в од юморо	нных ч дно це рные н произ	резуль исла, пое ра срипто водит	а зате азличн систе ь одн	операций, в м другой ч ые услуги, ны. овременно	ённые математи зыполняемых с с еловек мог бы р не предоставля только одну из обеих операций	откры асши ая дан опера	ітым те фроваті іные дл іщий — і	,
ASC	ш	Вероятн	юстн	ый инт	гервал	٦	-	-			-i		Name	_xx	x	
1095	^	-1000		1000				Заши	фрова	ть		874		-		
1089			-558	750	710	-559	-558	86	-443	-72	178	578			ок	
1080			-											^	on	
32			232	-824	980	-676	-371	462	-455	-62	-765	-967				
1082 1086			246	-805	-935	938	-113	-50	203	572	-645	-364				
1085		3	566	771	191	-357	979	117	-910	-280	966	573				
			400	379	-127	-529	-651	791	-103	-461	-1	465				
1091			100	575												
1091 1088 1099					-713	-425	856	388	-219	484	485	388				
1091 1088	Ţ		903 120	699 -556	400	-506	138	-134	736	-837	848	-725				
1091 1088 1099	~		903 120 -658	699 -556	400	-506 -447		-134 494	736 819	-837 -121		-725 -121				

Figure 2 – Enter the source text. The transformation of the original text according to the ASCII table and encrypted text in the matrix.

Conclusion

As a result of the studied encryption algorithms based on the homomorphic properties and the conducted research we can draw the following conclusions:

• The existing encryption algorithms are not perfect, fully homomorphic encryption algorithm is still not created.

• Our proposed algorithm encryption has homomorphic properties of probabilistic addition of encrypted matrices.

• The proposed algorithm is implemented and aprobirovany on a computer in Delphi environment.

• When increasing the length of the secret key, the cryptographic strength is increased more than the increase in the probability interval.



Impact Factor:

ISRA (India)

ISI (Dubai, UAE) = **0.829**

GIF (Australia) = **0.356**

екре	тный	ключ		Шифр	овани	e	Деш	ифров	ка						
ode ode	XXX ke XXX ke XXX ke XXX ke XXX b	y.txt. y_nev	txt v4449.	txt		Cod	e_XXX	key_n	ew444	9.txt			key.txt key_new2034.txt key_new2145.txt key_new4449.txt key_new4490.txt key_new-5.txt key_new7846.txt		ASCII 1077 1089 1082 1080 1077 32
	747	-797	606	535	-240	-633	-787	25	-924	-887	990	^	key_new8704.txt key_new4449.txt		1082 1086 1085
	-419	-878	278	30	595	812	-911	74	-218	608	508		-39		1090
	69	-488	999	516	585	284	722	907	-149	-775	771		-34 -34	Дешифровать	1091 1088
	867	11	-793	29	51	822	-26	616	763	-691	-813		-3 -45	дешлфровать	1099 46
	-43	-44	-102	686	-780	-574	-581	-869	-445	-790	698		-46		
	298	-5	-863	934	964	-203	-761	618	-252	55	872		-44 -5		
	-437	-798	676	-307	-238	-775	-299	218	-326	667	-495		3 -46	Гомоморфное шифро	
	-156	-688	-497	974	640	-252	-278	-885	856	-176	264		-41 -5	форма шифрования, позволяющая произ	водить
			307								587		-49	определённые мате действия с зашифро	
			-558					522					-38 -40	текстом и получать зашифров	
		932						-256		349			-6 -13	результат, который	i
	-993				-920			-490		-500			-44	соответствует резу. операций, выполняе	
	276	340	163	-189	187	726	-969	691	587	-852	-564	5	-20 -14	открытым текстом.	

= 1.344

SIS (USA)

ESJI (KZ)

РИНЦ (Russia) = **0.179**

= 0.912

= 1.042

Figure 3 – Decoding of the source text using the correct key.

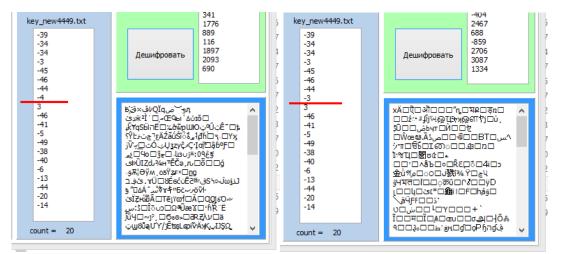


Figure 4 – Error decoding data when the error in the secret key.

References:

- 1. Burris SN, Senkeppenever KP (1981) Kurs v Universal'noy algebre. Springer-Verleg.
- 2. Kokorin AI (1972) Lineyno uporyadochennye gruppy: monografiya.- M.: Nauka, 1972.-199 p.
- 3. Kopytov VM, Mamaev II (1968) Absolyutnaya vypuklost' nekotorykh podgrupp uporyadochivaemoy gruppy. Algebra i logika. -Novosibirsk, 1968.-T.7.-№2.-pp.20-26.
- Menezes AJ, Oorschot PS, Vanstone SA (2015) 4. The ElGamal signature scheme // Handbook of applied cryptography.
- 5. Venbo Mao (2005)Sovremennaya Kriptografiya. Teoriya i Praktika. - Spb.: Vil'yams, 2005.

- 6. (2015) Kriptograficheskie algoritmy. Available: http://www.codenet.ru/progr/alg/crypt.php (Accessed: 20.10.2015).
- 7. (2015) Zadachi kriptografii. Ponyatie stoykosti kriptograficheskogo algoritma. Available: http://allrefs.net/c39/38j2b/ (Accessed: 20.10.2015).
- Nil's Fergyuson, Bryus Shnayer (2004) 8. Prakticheskaya kriptografiya = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. - Moscow: Dialektika, 2004. — 432 p.



= 6.630

ICV (Poland)