ՀՏԴ 681.3

Ա.Կ. ՍԱՂԱԹԵԼՅԱՆ, Ա.Հ. ՀԱՄԱԶԱՍՊՅԱՆ, Ա.Գ. ՔԱՄԱԼՅԱՆ

ՎԻԺԵՆԵՐԻ ԱԼԳՈՐԻԹՄՈՎ ԳԱՂՏՆԱԳՐՈՂ ՍԱՐՔԻ ԱՊԱՐԱՏԱՅԻՆ ԻՐԱԿԱՆԱՑՈՒՄԸ ԵՎ ԳՆԱՀԱՏՈՒՄԸ

Ուսումնասիրվում են Վիժենների ալգորիթմով գաղտնագրող սարքի ապարատային իրագործման հարցեր: Ներկայացված է ալգորիթմի մաթեմատիկական հիմնավորումը, մշակված են Վիժենների քառակուսու մտապահման համար մշտական հիշող սարքի կառուցվածքը և տեքստի ու բանալու տառերի ներմուծման ճշգրտված ալգորիթմի բլոկ-սխեման: Մշակված է Վիժենների գաղտնագրման ալգորիթմով նախագծված սարքի կառուցվածքային սխեման, և գնահատված են սարքի արագագործությունը և ապարատային ծախսերը FPGA ռեսուրսների տեսակետից:

Առանցքային բառեր. Վիժենների գաղտնագրման ալգորիթմ, գաղտնագրման բանալի, կառուցվածքային սխեմա, ապարատային իրագործում:

Վիժենների ալգորիթմը համարվում է բազմայբուբեն փոխարինման պարզ ձև: Չնայած կոդը հեշտ է հասկանալ ու իրագործել, սակայն հարյուրամյակների ընթացքում դիմակայել է կոտրվելու բոլոր տարբերակներին, որի շնորհիվ էլ վաստակել է **le chiffre indéchiffrable** (ֆրանսերենից՝ «չգուշակված գաղտնագիր») հայտանիշը: Այն ներառում է Կեսարի ծածկագրի միայբուբեն փոխարինման կանոնների ամբողջությունը՝ [0:25] միջակայքում տեղաշարժով: Վիժենների գաղտնագրումն իրականացվում է՝ գաղտնագրվող տեքստի սիմվոլի ինդեքսին գումա-րելով գաղտնագրի սիմվոլի (բանալի) ինդեքսը, որը հիմնված է Վիժենների քառակուսի անունով (Vigenere table): Վիժենների ծածկագրի գաղտնագրումը և վերծանումը մաթեմատիկորեն ունի այս տեսքը,

$$C_i = E(P_i + K_i) mod 26, \quad (1)$$

$$P_i = D(C_i + K_i) mod 26, \quad (2)$$

որտեղ C-ն գաղտնագրված տեքստն է, P-ն՝ գաղտնագրվող տեքստը, K-ն՝ բանալին, E-ն՝ գաղտնագրման ֆունկցիան, D-ն՝ գաղտնազերծման ֆունկցիան: Վիժենների ալգորիթմը (շիֆրը) բազմայբուբեն փոխարինման ծածկագիր է, որը կազմված է Կեսարի ծածկագրի տեղափոխության՝ 26x26 չափի զանգվածից (նկ.1) [1 - 3]:

Բացի դասական քառակուսուց, կան նաև այլ տարբերակներ, որոնցից յուրաքանչյուրը ներկայացնում է Վիժենների քառակուսու վարիացիա:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Նկ.1. Վիժեների գաղտնագրման քառակուսին

Դիցուք ունենք գաղտնագրման համար անհրաժեշտ ***SECURITY IS ESSENTIAL*** տեքստը: Գաղտնագրման բանալին ***TRUE*** –ն է:

Վիժեների գաղտնագրման աղյուսակի միջոցով տեքստը գաղտնագրելուց հետո կստանանք հետևյալ արդյունքը.

Հիմնական տեքստ. **SECURITYISESSENTIAL**

Բանալի բառ. **TRUETRUETRUETRUETRU**

Գաղտնագրված տեքստ. **LVWYKZNCBJYWLCHXBRF**

Գաղտնագրման ալգորիթմների հուսալիությունը գնահատվում է նաև սիմվոլների համընկնումների հավանականությամբ և էնտրոպիայով:

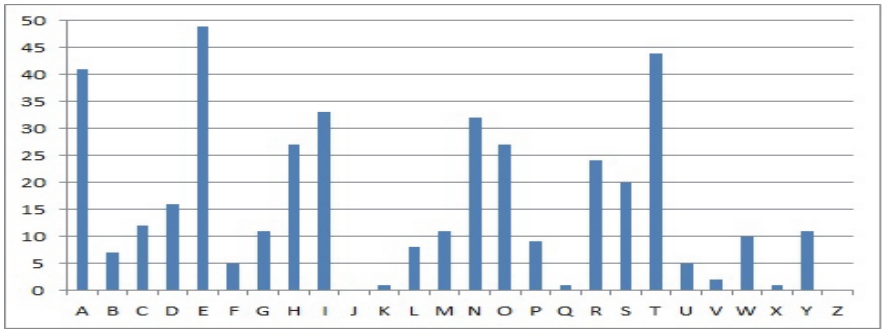
Էնտրոպիան բազմաթիվ տարրերից բաղկացած համակարգի անկարգավորվածության չափն է: Տվյալ դեպքում այն որոշվում է որպես համընկնումների հակառակ ֆունկցիա [3]:

Համընկնումների հավանականությունը հաշվարկելու համար օգտագործում են հետևյալ բանաձևը.

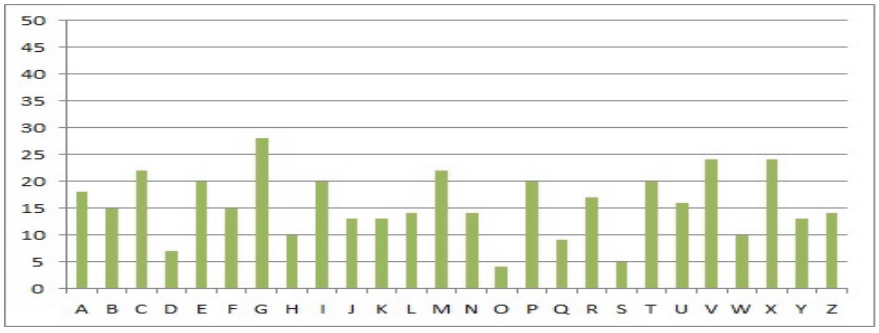
$$Ci = \frac{\sum_{i=Z}^{i=A} f_i(f_i-1)}{N(N-1)}, \quad (3)$$

որտեղ N-ը սիմվոլների ընդհանուր քանակն է, f_i-ն՝ i-րդ սիմվոլի օգտագործման հաճախականությունը:

Գաղտնագրված տեքստի համընկնումների հավանականությունը և էնտրոպիան հիմնված են ավանդական Վիժեների ծածկագրման մեթոդի վրա, որոնք հաշվարկվում են այլ տարբերակներով: Համընկնումների հավանականությունը 0,02925 է, իսկ էնտրոպիան՝ 3,7216 բիթ: Հաշվի առնենք, որ լատինատառ այբուբենի էնտրոպիան մոտավորապես 4,7 բիթ է, իսկ համընկնումների հավանականությունը՝ 0,0667: 4-8 տառերի երկարությամբ բանալիով Վիժեների ծածկագրի համընկնումների հավանականությունը 0,045±0,05 է: Որքան համընկնումների հավանականությունը մոտ է 0,07-ի, այնքան մեծ է տեքստը գաղտնազերծելու հավանականությունը, իսկ էնտրոպիայի դեպքում հակառակն է. որքան մեծ է թիվը, այնքան վերծանման հավանականությունը փոքր է: Վիժեների ալգորիթմի յուրահատկությունը բանալի բառի երկարությունն է: Որքան երկար է բանալին, այնքան արդյունավետ է գաղտնագրումը: Օրինակ, եթե բանալու երկարությունը 12 է, ապա բանալին ունի 26^{12} հնարավոր տարբերակ, որը բավականին մեծ թիվ է [4]: Ստորև ներկայացված նկարներում դիտարկված են տառերի կրկնվելու հաճախականությունները հիմնական և Վիժեների ալգորիթմով գաղտնագրելու դեպքում (նկ.2 և 3):

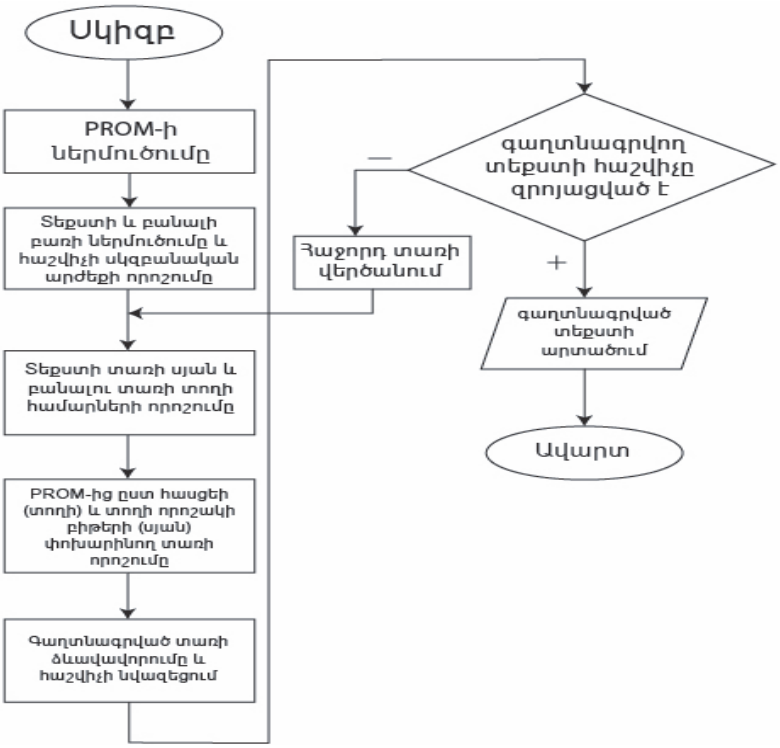


Նկ.2. Գաղտնագրվող տեքստի տառերի կրկնման հաճախականությունը



Նկ.3. Տառերի կրկնման հաճախականությունը Վիժեների ալգորիթմով տեքստի գաղտնագրմամբ

Ներկայացված դիագրամներն ապացուցում են, որ Վիժեների ալգորիթմում տառերի կրկնման հաճախականությունը գրեթե հավասար է, ինչի շնորհիվ էլ նույնիսկ մեր օրերում այն օգտագործվում է [4]: Գաղտնագրող սարքի իրագործման համար մշակվել է հիմնական ալգորիթմի բլոկ-սխեման, որը ներկայացված է նկ.4-ում:



Նկ. 4. Գաղտնագրման ալգորիթմի մշակված բլոկ-սխեման

Վիժեների գաղտնագրման քառակուսու մտապահման համար մշակվել է PROM (Programmable Read-Only Memory) մշտական հիշող սարք:

PROM-ի կառուցվածքը պայմանավորված է նրանով, որ նրա տողերի քանակը համապատասխանում է գաղտնագրման նոր աղյուսակի տողերի քանակին (26 տող, սակայն երկուական համակարգի կիրառումը հնարավորություն է տալիս քառակուսին ընդլայնել մինչև 32 սիմվոլ), իսկ յուրաքանչյուր տողի երկարությունը՝ նոր աղյուսակի կոդավորված սիմվոլների բիթերի քանակին (160 բիթ): Այդ պատճառով PROM-ի հասցեական մուտքերի քանակը $\log_2 32=5$, իսկ ելքային տվյալի երկարությունը՝ 32x5=160 բիթ: Հետևաբար՝ PROM-ի նվազագույն ծավալը հավասար է 32x160 բիթ կամ 2^5 x 160 բիթ: Գաղտնագրման դասական քառակուսին կարելի է համալրել բազմաթիվ լրացուցիչ սիմվոլներով:

Սիմվոլների կոդավորման համար կարելի էր կիրառել նաև ASCII միջազգային ստանդարտը, որի համար քառակուսու մտապահման PROM սարքի ծավալը 2^8x 2046 բիթ է [5,6]: Ընդհանուր դեպքում, եթե քառակուսին պարունակում է N տարբեր սիմվոլներ, ապա դրա մտապահման համար նախատեսված PROM սարքի ծավալը կարելի է հաշվարկել հետևյալ բանաձևով (4)՝

$$V_{PROM} = 2^{log_2 N}\, x\, N\, log_2 N \qquad (4)$$

Գաղտնագրվող բանալու տառին համապատասխան PROM-ի տողին դիմելու համար կարող ենք օգտագործել հասցեավորման հետևյալ տարբերակը. քանի որ արդեն նկարագրել ենք սկզբնական տարբերակով, թե յուրաքանչյուր տառի երկուական կոդը որն է, արդեն PROM-ում հասցեավորման համար առանց որևէ խնդրի կարող ենք գրել ոչ թե կոդավորված տարբերակը, այլ հենց համապատասխան սիմվոլը: PROM-ում տառերի հասցեավորման սկզբունքը ներկայացված է նկ. 5-ում:

Տառ	PROM-ի հասցե	Տառ	PROM-ի հասցե	Տառ	PROM-ի հասցե	Տառ	PROM-ի հասցե
a	addr=[0]	i	addr=[8]	q	addr=[16]	y	addr=[24]
b	addr=[1]	j	addr=[9]	r	addr=[17]	z	addr=[25]
c	addr=[2]	k	addr=[10]	s	addr=[18]	:	addr=[26]
d	addr=[3]	l	addr=[11]	t	addr=[19]	.	addr=[27]
e	addr=[4]	m	addr=[12]	u	addr=[20]	,	addr=[28]
f	addr=[5]	n	addr=[13]	v	addr=[21]	;	addr=[29]
g	addr=[6]	o	addr=[14]	w	addr=[22]	!	addr=[30]
h	addr=[7]	p	addr=[15]	x	addr=[23]	␣	addr=[31]

Նկ. 5. PROM-ում հասցեավորման եղանակը

Ինչպես արդեն նշեցինք, գաղտնագրման ամենաապահով տարբերակը բանալի բառի և գաղտնագրվող տեքստի սիմվոլների հավասարությունն է:

key 1	key 2	key 3	key 4	key 5
letter 1	letter 2	letter 3	letter 4	letter 5

key 2	key 3	key 4	key 5	key 1
letter 2	letter 3	letter 4	letter 5	letter 1

key 3	key 4	key 5	key 1	key 2
letter 3	letter 4	letter 5	letter 1	letter 2

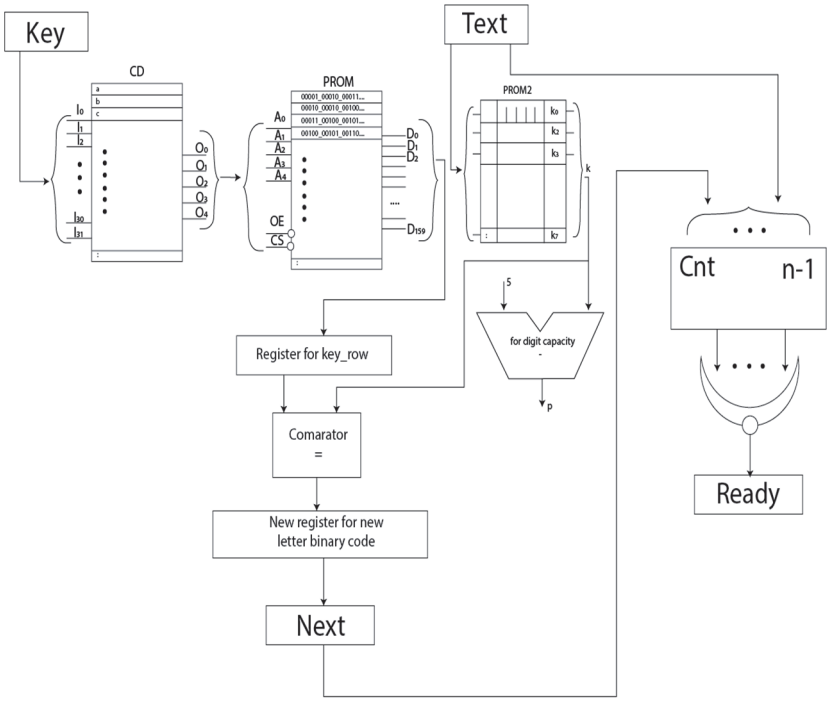
key 1	key 2	key 3	key 4	key 5
letter 1	letter 2	letter 3	letter 4	letter 5

key 2	key 3	key 4	key 5
letter 2	letter 3	letter 4	letter 5

key 3	key 4	key 5
letter 3	letter 4	letter 5

Գաղտնագրումը կարելի է կատարել տեքստի և բանալի բառի 5-ական բիթի միաժամանակ տեղաշարժով: Իսկ անհավասար լինելու դեպքում բանալի բառը 5 կարգով ցիկլիկ տեղաշարժում ենք դեպի ձախ, քանզի այն պետք է գալու ամբողջ տեքստը գաղտնագրելու համար:

Սարքի աշխատանքը կատարվում է հետևյալ սկզբունքով. նախ PROM-ից ընտրվում է բանալի բառի հերթական տառին համապատասխանող տողը, հետո այն գրանցվում է դրա համար նախատեսված ռեգիստրում: Այնուհետև գաղտնագրվող տեքստից բանալի բառի տողին համապատասխան տառի k և p բիթերի համարները համեմատվում են տողում գտնվող տառերի բիթերի համարների հետ: Համընկման դեպքում նոր ռեգիստրում գրանցվում է համապատասխան k ու p համարներ ունեցող տառի երկուական կոդը: Վերոհիշյալ քայլերից հետո այն հաշվիչում, որը պարունակում է տեքստի տառերի քանակը, կատարվում է ստուգում՝ արդյո՞ք տառերի քանակը հավասար է 0-ի: Եթե այո, ապա կոդավորման գործընթացը ավարտվում է, եթե ոչ, ապա անցում է կատարվում տեքստի հաջորդ տառի գաղտնագրմանը: Գաղտնագրող սարքի մշակված կառուցվածքային սխեման ներկայացված է նկ.6-ում:



Նկ. 6. Վիժեների գաղտնագրման ալգորիթմով մշակված սարքի ճշգրտված կառուցվածքային սխեման

Սխեմայի սկզբնական հատվածում կոդավորիչի միջոցով ըստ նկ.5-ի աղյուսակի տվյալների՝ կոդավորվում է սիմվոլը PROM-ում ունեցած հասցեի հիման վրա [6,7]:

Ըստ մուտքագրվող տեքստի սիմվոլներին համապատասխան բիթերի կազմվել է աղյուսակ, որտեղ որոշվում է k բիթը, այնուհետև կարգայնությունը որոշող սարքի միջոցով՝ k-ից 5 միավոր քիչ՝ p-ն: Ճշգրտված տարբերակում համեմատող սարքի մեջ մուտք է գործում k-ն:

Եզրակացություն: Գաղտնագրման սարքի նախագծման համար նկարագրվել են 3 առանձին մշտական հիշող սարքեր.

1. Վիժեների աղյուսակի մտապահման համար PROM, որի ծավալն է 2^5x160 բիթ՝ *reg [159:0] rom [0:31];*

2. Գաղտնագրող բանալու յուրաքանչյուր սիմվոլի կոդին համապատասխանող հասցեները մտապահող մշտական հիշող սարք PROM1, որի ծավալն է 2^5x5 բիթ՝ *reg [4:0]rom1[0:31]:* PROM1-ի կառուցվածքը ներկայացված է կառուցվածքային ճշգրտված սխեմայում:

3. Գաղտնագրվող տեքստի յուրաքանչյուր սիմվոլի կոդին համապատասխանող Վիժեների աղյուսակի մտապահման PROM-ի որոշակի տողի բիթերի (k) մշտական հիշող սարք *reg [7:0] k*. որի կառուցվածքը ներկայացված է [8]-ում:

Վերլուծելով նախագծված սարքի մեկ սիմվոլի փոխարինման գործընթացի տևողությունը գործողության սկզբից (start=1) մինչև ավարտման մասին ազդարարող (ready=1) ազդանշանը՝ սիմուլյատորի ժամանակային դիագրամի միջոցով, պարզվում է, որ այն կազմում է 120 նվ: Իսկ ապարատային ծախսերը, համաձայն հաշվետվության, կազմում են ծրագրավորվող սարքի (Spartan-3E, xc6s500e) ռեսուրսների մոտավորապես 11%-ը:

ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. https://crypto.stackexchange.com/questions/378/what-is-entropy
2. https://www.academia.edu/31794739/Vigenere_Cipher_Trends_Review_and_Possible_Modifications
3. https://crypto.interactive-maths.com/vigenegravere-cipher.html
4. **Крэндалл Р., Померанс К**. Простые числа: Криптографические и вычислительные аспекты/ Пер с англ.; Под ред. и с предисл. В.Н.Чубарикова.-М.: Книжныйдом 'ЛИБРОКОМ&#39, 2015.- 664 с.
5. **Столлингс У.** Структурная организация и архитектура компьютерных систем.-5-е изд. –М.: Изд.дом “ Ильамс”, 2002.-893 с.
6. **Цилькер Б.Я., Орлов С.А.** Организация ЭВМ и систем.-СПб.: Питер, 2016.- 667 с.

7. **Saghatelyan A.**The Hardware Implementation of the Cryptographic Key Generation based on Diffie-Hellman algorithm //Հայաստանի ճարտարագիտական ակադեմիայի Լրաբեր.Գիտական հոդվածների ժողովածու.- 2015.- Հատոր 10, N 4.-էջ 760-763:
8. Ծրագրավորվող տրամաբանական սարքեր /**Ա.Կ. Թումանյան, Ա.Հ. Համազասպյան, Ա.Կ. Սաղաթելյան, Է.Վ. Վիրաբյան, Ա.Գ. Քամալյան.** «Թվային սարքերի նախագծման միջոցներ» առարկայի դասընթացի մեթոդական ցուցումներ/ ՀՊՃՀ.- Եր.: Ճարտարագետ, 2014.- 90էջ:

А.К. САГАТЕЛЯН, А.А. АМАЗАСПЯН, А.Г. КАМАЛЯН

АППАРАТНАЯ РЕАЛИЗАЦИЯ И ОЦЕНКА КРИПТОУСТРОЙСТВА ПО АЛГОРИТМУ ВИЖЕНЕРА

Исследованы вопросы аппаратной реализации криптоустройства по алгоритму Виженера. Представлено математическое обоснование алгоритма, разработаны постоянное запоминающее устройство для хранения квадрата Виженера и блок-схема алгоритма загрузки символов текста и криптоключа. Спроектирована структурная схема криптоустройства по алгоритму Виженера и оценены его быстродействие и аппаратные затраты с точки зрения ресурсов FPGA.

Ключевые слова: криптоалгоритм Виженера, ключ кодирования, структурная схема, аппаратная реализация.

A.K. SAGHATELYAN, A.A. HAMAZASPYAN, A.A. QAMALYAN

THE HARDWARE IMPLEMENTATION AND EVALUATION OF A CRYPTOGRAPHIC DEVICE USING THE VIGENERE ALGHORITHM

The issues of hardware implementation of a cryptodevice based on the Vigenère algorithm have been studied. The mathematical substantiation of the algorithm is presented, a permanent memory device for storing the Vigenère square and a block diagram of the algorithm for loading text symbols and a cryptokey are developed. A block diagram of a cryptodevice based on the Vigenère algorithm is designed and its performance and hardware costs are estimated from the point of view of FPGA resources.

Keywords: Vigenère cryptoalgorithm, encryption key, block diagram, hardware implementation.