მონაცემთა ბლოკის დაშიფვრის არასტანდარტული სიმეტრიული კრიპტოალგორითმი

ვასილ კუციავა, ანა კუციავა, გიორგი გოგოლაძე

საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია მონაცემთა ბლოკის დაშიფვრის არასტანდარტული სიმეტრიული კრიპტოგრაფიული ალგორითმი, რომელშიც გამოიყენება დამშიფრავი საიდუმლო გასაღების მნიშვნელობის მიღებისა და დაშიფვრის პროცედურის განმახორციელებელი ორიგინალური მეთოდი. შემთხვევითი მნიშვნელობების მქონე საიდუმლო გასაღები, რომელიც შედგება მიმდევრობით დაწერილი დიდი რაოდენობის ათობითი ციფრებისგან, ფორმირდება კანონიერი მომხმარებლების მიერ პროგრამულად ალგორითმში მოყვანილი გარკვეული პროცედურების შესრულების შედეგად და მისი მნიშვნელობა უცნობია მომსახურე პერსონალისათვის. ალგორითმით შესაძლებელია ათობითი სისტემით წარმოდგენილი ASCII ან EBCDIC კოდის ნებისმიერი რაოდენობის სიმბოლოებისაგან შედგენილი ღია ტექსტის დაშიფვრა. კორპორაციული ქსელის კავშირის ხაზში არ გადაიცემა დაშიფვრის პროცედურებში მონაწილე არც ერთი პარამეტრის ნამდვილი მნიშვნელობა. წარმოდგენილი ალგორითმი გამოირჩევა კრიპტომედეგობით და მაღალი სწრაფქმედებით.

საკვანძო სიტყვები: სიმეტრიული ალგორითმი. ეილერის ფუნქციის მნიშვნელობა. საიდუმლო გასაღები. კრიპტომედეგობა. სწრაფქმედება.

1. შესავალი

კორპორაციულ ქსელებში ჩართულ კანონიერ მომხმარებლებს შორის გადაცემული ინფორმაციის კონფიდენციალობის უზრუნველსაყოფად გამოიყენება როგორც სიმეტრიული (მაგალითად: DES, IDEA, RC2, RC5, MD4, MD5 და სხვ.), ისე ასიმეტრიული (RSA კრიპტოსისტემა, ელგამალის დაშიფვრის სქემა და სხვ.) სისტემები. ამასთან, სიმეტრიულ სისტემებში საიდუმლო გასაღების ფორმირება შესაძლებელია განხორციელდეს დიფი-ჰელმანის ალგორითმით.

აქვე უნდა აღინიშნოს, რომ:

DES, IDEA და მათი მსგავსი ალგორითმების „გატეხვა" შესაძლებელია დამშიფრავი გასაღების ყველა მნიშვნელობის სრულად გადარჩევის გზით. ცხადია, რომ რაც უფრო დიდია გასაღების სიგრძე, მით უფრო ძნელია ყველა შესაძლებელი ვარიანტის გადარჩევა. თანამედროვე ეტაპზე ბაზარზე გამოჩნდა FPGA და ASIC მიკროსქემები, რომლებსაც შეუძლიათ გასაღების მნიშვნელობების გადარჩევა წამში, შესაბამისად, 30 და 200 მილიონი ვარიანტის სიჩქარით. ამასთან ამ მიკროსქემების ღირებულება შეადგენს რამდენიმე ათეულ დოლარს. დიდი ბიუჯეტის (10 მილიონ დოლარამდე) მქონე კორპორაციებს შეუძლიათ DES ალგორითმის, რომლის გასაღების ყველა

მნიშვნელობათა რაოდენობა 2^{56}–ის ტოლია, "გატეხვა" FPGA და ASIC მიკროსქემების გამოყენებით 13 საათში, ხოლო სუპერ ეგმ-ის საშუალებით კი 6 წუთში [1]. ამის გამო DES სტანდარტის მაგივრად გამოიყენება AES სტანდარტი, რომლის საიდუმლო გასაღების სიგრძეა 128, 192 ან 256 ბიტი, ხოლო დასაშიფრი ბლოკის კი 128 ბიტი.

RSA კრიპტოსისტემის კრიპტომედეგობის უზრუნველსაყოფად აუცილებელია ერთმანეთისგან საგრძნობლად განსხვავებული და ერთი და იმავე სიგრძის (არანაკლებ 512 ბიტი) ორი მარტივი რიცხვის გამოყენება. ასეთი დიდი რიცხვების შემთხვევაში საგრძნობლად რთულდება დაშიფვრისა და გაშიფვრის პროცედურები.

დიფი-ჰელმანის ალგორითმის სუსტი ადგილია " man-the-meddle" ტიპის შეტევა. თუ მოწინააღმდეგეს შეუძლია განახორციელოს აქტიური შეტევა, ე.ი. აქვს საშუალება არა მარტო დაიჭიროს შეტყობინება, არამედ შეცვალოს კიდეც სხვა შეტყობინებით, მას შეუძლია მიიტაცოს ქსელში ჩართული ორი მომხმარებლის ღია გასაღებები, შექმნას ღია და დახურული გასაღებების საკუთარი წყვილი და გაუგზავნოს თითოეულ მონაწილეს თავისი ღია გასაღები. ამის შემდეგ ყოველი მონაწილე გამოთვლის გასაღებს, რომელიც საერთო იქნება მოწინააღმდეგესთან და არა სხვა მონაწილესთან. გამოთვლითი ტექნოლოგიების განვითარებამ უახლოეს მომავალში შეიძლება მიაღწიოს ისეთ დონეს, რომ შესაძლებელი გახდეს AES სტანდარტის გატეხვაც.

ზემოაღნიშნულიდან გამომდინარე მიზანშეწონილად ჩავთვალეთ კორპორაციულ ქსელებში გადაცემული ინფორმაციის კონფიდენციალობის შესანარჩუნებლად ისეთი სიმეტრიული ალგორითმის შემუშავება, რომელიც მუშაობს გაცილებით დიდი გასაღებით, არ საჭიროებს კავშირის ხაზში დაშიფვრისა და გაშიფვრის პროცედურებში უშუალოდ მონაწილე არც ერთი პარამეტრის მნიშვნელობის გადაცემას და ამასთან გამოირჩევა მაღალი კრიპტომედეგობით.

2. ძირითადი ნაწილი

2.1. დამშიფრავი საიდუმლო გასაღების დასაფორმირებელი ალგორითმი

კორპორაციული ქსელის ორი მომხმარებლიდან (პირობითად A და B), თუ A წარმოადგენს ინფორმაციის გადამცემს, ხოლო B კი მიმღებს, მაშინ B აგზავნის A –სთან ორი დიდი P_0 და Q_0 მარტივი რიცხვების ნამრავლს $N_0=P_0 \cdot Q_0$. ამასთან, P_0 და Q_0 მარტივი რიცხვების შემთხვევითი არჩევა ხდება მარტივი რიცხვების ბაზიდან (მომსახურე პერსონალმა არ იცის არჩეული რიცხვების მნიშვნელობები).

A მომხმარებელი N_0 რიცხვიდან აღადგენს P_0 და Q_0 რიცხვებს ($P_0 \geq Q_0$). ამ რიცხვების მნიშვნელობების ცოდნა უზრუნველყოფს A და B მომხმარებლების პარალელურ მუშაობას ერთი და იმავე ალგორითმით საიდუმლო გასაღების მისაღებად. კერძოდ:

1. გამოითვლება ეილერის ფუნქციის მნიშვნელობა $\varphi_0(N_0) = (P_0 - 1) \cdot (Q_0 - 1)$;

2. განისაზღვრება P_0 და Q_0 რიცხვების ერთეულოვან თანრიგში განთავსებული a და b ციფრებისაგან შედგენილი (a, b) წყვილი. ცხადია, რომ $a \in \{1,3,7,9\}$ და $b \in \{1,3,7,9\}$;
3. გამოითვლება: $K = \varphi_0(N_0) mod 10$ და $T = \varphi_0(N_0) mod 15$ მნიშვნელობები, სადაც K და T არაუარყოფითი მთელი რიცხვებია.

პირველ ცხრილში განთავსებული მარტივი რიცხვების დაბოლოებების თექვსმეტი ვარიანტისგან $\{1,1; 1,3; 1,7; 1,9;\ 3,1; 3,3; 3,7; 3,9;\ 7,1; 7,3; 7,7; 7,9;\ 9,1; 9,3; 9,7; 9,9\}$ შედგენილი ხუთი განსხვავებული ქვეჯგუფიდან (ქვეჯგუფების რაოდენობა 16!–ის ტოლია) შეირჩევა ერთ-ერთი ქვეჯგუფი მე-3 პუნქტში გამოთვლილი $\varphi_0(N_0) mod 10$ შედეგის მიხედვით. რადგან ეილერის ფუნქციის მნიშვნელობა ლუწი რიცხვია, ამიტომ K-ს გამოთვლისას მიიღება $0,2,4,6$ და 8 რიცხვებიდან ერთ-ერთი, ხოლო T მიიღებს ერთ-ერთ მნიშვნელობას $[0;14]$ შუალედიდან. K და T რიცხვებით ხდება მატრიცაში სვეტისა და სტრიქონის ნომრების განსაზღვრა. სტრიქონის შერჩევისას (a, b) წყვილის შესაბამისი კომბინაცია დროებით გადადის ქვეჯგუფის ბოლო მე-15 სტრიქონში გამეორების გამოსარიცხად. სვეტისა და სტრიქონის გადაკვეთაზე განთავსებული წყვილი წარმოადგენს მარტივი რიცხვების დაბოლოებების ახალ (c,d) წყვილს.

ცხრ.1

	K = 0	**K= 2**	**K = 4**	**K = 6**	**K = 8**
T = 0	3,1	1,3	9,9	9,1	1,7
T = 1	7,9	3,7	1,1	1,3	9,9
T = 2	1,7	1,9	7,3	3,7	7,7
T = 3	9,3	3,9	3,9	1,9	3,3
T = 4	7,1	7,3	7,7	9,7	3,1
T = 5	3,7	9,3	3,1	7,9	7,3
T = 6	1,9	1,1	7,9	7,1	9,3
T = 7	9,7	1,7	1,7	3,9	1,1
T = 8	1,3	9,9	9,3	7,3	7,9
T = 9	9,1	7,7	7,1	9,3	1,9
T = 10	3,3	3,3	3,7	1,1	3,9
T = 11	9,9	3,1	1,9	1,7	9,1
T = 12	1,1	9,7	9,7	9,9	1,3
T = 13	7,3	9,1	1,3	7,7	3,7
T = 14	3,9	7,9	9,1	3,3	7,1
15	7,7	7,1	3,3	3,1	9,7

ვთქვათ: $N_0 = 2881;\ P_0 = 67;\ Q_0 = 43;\ (a,b) \to (7,3);$

$$\varphi_0(N_0) = (P_0 - 1)\cdot(Q_0 - 1) = 66 \cdot 42 = 2772;$$

$K = \varphi_0(N_0)\text{mod}10 = 2772(\text{mod}\ 10) \equiv 2;\quad T = \varphi_0(N_0)\text{mod}15 = 2772(\text{mod}\ 15) \equiv 12.$

ე.ი. შეირჩევა მე-2 ქვეჯგუფის და მე-12 სტრიქონში (მე-13 სტრიქონი ხდება მე-12 სტრიქონი, რადგან მეოთხე სტრიქონი გადადის ბოლოში) განთავსებული (c,d) წყვილი, რომელიც არის (9,1).

5. განისაზღვრება ახალი მარტივი P_1 და Q_1 რიცხვები შემდეგი თანაფარდობებით:

$P_1 = P_0 + c - a + 10\alpha$ და $Q_1 = Q_0 + d - b + 10\alpha$, სადაც $\alpha \in N$ და იცვლება ერთიდან ზემოთ მანამ, სანამ თითოეული რიცხვი არ გახდება მარტივი. განხილული მაგალითის შემთხვევაში: $P_1 = P_0 + c - a + 10\alpha = 67 + 9 - 7 + 10\alpha = 69 + 10\alpha$, როცა $\alpha = 1$, მაშინ $P_1 = 79$ და ეს რიცხვი მარტივია; $Q_1 = Q_0 + d - b + 10\alpha = 43 + 1 - 3 + 10\alpha = 41 + 10\alpha$, როცა $\alpha = 2$, მაშინ $Q_1 = 61$ და ეს რიცხვი მარტივია.

6. გამოითვლება $N_1 = P_1 \cdot Q_1$ და $\varphi_1(N_1) = (P_1 - 1)\cdot(Q_1 - 1)$.

ამ ექვსი პუნქტის შესრულების შედეგად მიიღება $N_1, \varphi_1(N_1), P_1, Q_1, K_1$ და T_1 მნიშვნელობები.

ზემოთ აღწერილი პროცედურების კიდევ ორჯერ გამეორებით (წინა ციკლში გამოთვლილი **P** და **Q** წარმოადგენენ შემდეგი ციკლის საწყისს მონაცემებს) მიიღება $N_2, N_3, \varphi_2(N_2), \varphi_3(N_3)$, P_2, P_3, Q_2 და Q_3 მნიშვნელობები. N, $\varphi(N)$, P და Q შედეგების მიხედვით გამოითვლება ერთსახელა პარამეტრებისათვის როგორც ორ-ორი, ისე სამივე წევრის ნამრავლები და ჯამები. მიღებული შედეგების მიხედვით შეივსება მე-2 ცხრილი და თითოეულს მიენიჭება ათობითი ნომერი.

ცხრ.2

№	N	№	$\varphi(N)$	№	P	№	Q
1	N_1	12	φ_1	23	P_1	34	Q_1
2	N_2	13	φ_2	24	P_2	35	Q_2
3	N_3	14	φ_3	25	P_3	36	Q_3
4	$N_1 \cdot N_2$	15	$\varphi_1 \cdot \varphi_2$	26	$P_1 \cdot P_2$	37	$Q_1 \cdot Q_2$
5	$N_1 \cdot N_3$	16	$\varphi_1 \cdot \varphi_3$	27	$P_1 \cdot P_3$	38	$Q_1 \cdot Q_3$
6	$N_2 \cdot N_3$	17	$\varphi_2 \cdot \varphi_3$	28	$P_2 \cdot P_3$	39	$Q_2 \cdot Q_3$
7	$N_1 + N_2$	18	$\varphi_1 + \varphi_2$	29	$P_1 + P_2$	40	$Q_1 + Q_2$
8	$N_1 + N_3$	19	$\varphi_1 + \varphi_3$	30	$P_1 + P_3$	41	$Q_1 + Q_3$
9	$N_2 + N_3$	20	$\varphi_2 + \varphi_3$	31	$P_2 + P_3$	42	$Q_2 + Q_3$
10	$N_1 \cdot N_2 \cdot N_3$	21	$\varphi_1 \cdot \varphi_2 \cdot \varphi_3$	32	$P_1 \cdot P_2 \cdot P_3$	43	$Q_1 \cdot Q_2 \cdot Q_3$
11	$N_1 + N_2 + N_3$	22	$\varphi_1 + \varphi_2 + \varphi_3$	33	$P_1 + P_2 + P_3$	44	$Q_1 + Q_2 + Q_3$

ამ უკანასკნელში განთავსებული 44 შედეგიდან ხდება დამშიფრავი საიდუმლო გასაღების შემადგენლობაში მონაწილე მონაცემების არჩევა მე-3 ცხრილის და K-ს მნიშვნელობის მიხედვით.

ცხრილის თითოეულ სტრიქონში განთავსებულია 9 მონაცემი (ერთი შედეგი მონაწილეობს ორჯერ). მათი გამომსახველი ნომრების შემთხვევითი განაწილებით დამშიფრავი საიდუმლო გასაღები შეიცავს 27 მონაცემს, ე.ი. სამ სტრიქონს. პირველი სტრიქონი აირჩევა K_1 -ის, მეორე K_2 -ის, ხოლო მესამე K_3 -ის მნიშვნელობის მიხედვით (K მნიშვნელობიდან გამომდინარე შესაძლებელია მოხდეს სტრიქონების გამეორება). ამ 45 მონაცემში შემავალი ათობითი ციფრები განთავსდება ერთმანეთის გვერდით მარცხნიდან მარჯვნივ. ცხადია, რომ ამ ციფრების რაოდენობა დამოკიდებულია საწყისი მარტივი რიცხვების თანრიგებისა და გამოთვლების შედეგად მიღებული შედეგების თანრიგების რაოდენობაზე.

ცხრ.3

K	**გასაღების მიმდევრობის შემადგენლობაში მონაწილე მონაცები**								
K=0	16	21	33	1	11	37	41	7	25
K=2	27	42	2	19	23	31	36	8	12
K=4	13	26	32	3	17	22	43	6	38
K=6	34	4	18	24	39	9	44	15	29
K=8	20	10	28	40	5	30	25	14	35

2.2. დაშიფვრის პროცედურა

დასაშიფრი ღია ტექსტის მონაცემები წარმოადგენს ASCII ან EBCDIC კოდში შემავალ სიმბოლოებს, ასახულს ათობითი სისტემის შესაბამისი ნომრებით. ქვემოთ ნაჩვენებია ASCII კოდის ცხრილი.

ცხრ.4

Decimal	Value	Decimal	Value	Decimal	Value	Decimal	Value	Decimal	Value	Decimal	Value	Decimal	Value	Decimal	Value
000	NUL	016	DLE	032	SP	048	0	064	@	080	P	096	`	112	p
001	SOH	017	DC1	033	!	049	1	065	A	081	Q	097	a	113	q
002	STX	018	DC2	034	"	050	2	066	B	082	R	098	b	114	r
003	ETX	019	DC3	035	#	051	3	067	C	083	S	099	c	115	s
004	EOT	020	DC4	036	$	052	4	068	D	084	T	100	d	116	t
005	ENQ	021	NAK	037	%	053	5	069	E	085	U	101	e	117	u
006	ACK	022	SYN	038	&	054	6	070	F	086	V	102	f	118	v
007	BEL	023	ETB	039	'	055	7	071	G	087	W	103	g	119	w
008	BS	024	CAN	040	(	056	8	072	H	088	X	104	h	120	x
009	HT	025	EM	041	)	057	9	073	I	089	Y	105	i	121	y
010	LF	026	SUB	042	*	058	:	074	J	090	Z	106	j	122	z
011	VT	027	ESC	043	+	059	;	075	K	091	[	107	k	123	{
012	FF	028	FS	044	,	060	<	076	L	092	\	108	l	124	|
013	CR	029	GS	045	-	061	=	077	M	093	]	109	m	125	}
014	SO	030	RS	046	.	062	>	078	N	094	^	110	n	126	~
015	SI	031	US	047	/	063	?	079	O	095	_	111	o	127	DEL

თითოეული სიმბოლო გამოსახულია სამთანრიგა ათობითი რიცხვით (მაგალითად, 5-053, W-087, w-119, %-037 და ა.შ.). ღია ტექსტის დაშიფვრისას მასში შემავალი სიმბოლოების შესაბამისი ათობითი ციფრების მიმდევრობის ქვეშ განთავსდება ფორმირებული საიდუმლო გასაღების ციფრების მიმდევრობა და შესრულდება მარცხნიდან მარჯვნივ სამ-სამი ციფრით გამოსახული ჯგუფების შეკრება მოდულით 128 (ASCII კოდისთვის) ან მოდულით 256 (EBCDIC კოდისთვის).

თუ საიდუმლო გასაღების ციფრების რაოდენობა არაა სამის ჯერადი რიცხვი, მაშინ ბოლო ჯგუფი გაუქმდება. განვიხილოთ მაგალითი. ვთქვათ, დასაშიფრი ტექსტია ASCII კოდით წარმოდგენილი CENTRAL, საიდუმლო გასაღების მიმდევრობაა 923241305441003123846 და მოდულის მნიშვნელობა 128.

C	E	N	T	R	A	L	
067	069	078	084	082	065	076	**ღია ტექსტი**
+							
923	241	305	441	003	123	846	**საიდუმლო გასაღები**
990	310	383	525	085	188	922	**ჯამი**
094	054	127	013	085	060	026	**შიფრტექსტი**
^	6	↓	(cr)	U	<	(eof)	**სიმბოლო ASCII კოდით**

როდესაც ღია ტექსტში შემავალი ათობითი ციფრების რაოდენობა აღემატება საიდუმლო გასაღებში შემავალი ციფრების რაოდენობას, მაშინ ხდება გასაღების თანმიმდევრობის გამეორება. დაშიფვრის შედეგად მიღებული შიფრტექსტი ათობითი ციფრების მიმდევრობის სახით გადაიცემა მიმღებისაკენ (განხილული მაგალითის შემთხვევაში გადაიცემა 094054127013085060026).

2.3. გაშიფვრის პროცედურა

გადამცემიდან გადმოცემული შიფრტექსტის მიღების შემდეგ მიმღები ამ მიმდევრობის ქვეშ განათავსებს საიდუმლო გასაღების მიმდევრობას, დაყოფს ამ მიმდევრობებს მარცხნიდან მარჯვნივ სამციფრიან ჯგუფებად და შეასრულებს გამოკლებას იმავე მოდულით (შიფრტექსტს აკლდება გასაღები).

გამოკლების შედეგად უარყოფითი რიცხვის მიღებისას ხდება მოდულის მნიშვნელობის მიმატება. მაგალითად, 094054127013085060026 შიფრტექსტის მიღებისას ხდება:

094	054	127	013	085	060	026	**შიფრტექსტი**
-							
923	241	305	441	003	123	846	**საიდუმლო გასაღები**
-829	-187	-178	-428	082	-063	-820	**სხვაობა**
-061	-059	-050	-044	082	-063	-052	**mod(128)**
067	069	078	084	082	065	076	**ღია ტექსტი**
C	E	N	T	R	A	L	

როდესაც შიფრტექსტში შემავალი ათობითი ციფრების რაოდენობა აღემატება საიდუმლო გასაღებში შემავალი ციფრების რაოდენობას, მაშინ ხდება გასაღების თანმიმდევრობის გამეორება.

1-ელი და მე-3 ცხრილები ალგორითმის საიდუმლო გასაღებებია და მათი შემადგენლობა ცნობილი უნდა იყოს მხოლოდ კორპორაციულ ქსელში ჩართული კანონიერი მომხმარებლებისათვის. ალგორითმის კრიპტომედეგობის გასაზრდელად მიზანშეწონილია ამ ცხრილების შემადგენლობის ცვლილება დროის გარკვეული პერიოდის გასვლის შემდეგ.

3. დასკვნა

ჩვენს მიერ შემუშავებულ ალგორითმს აქვს შემდეგი ღირსებები: ალგორითმის პროცედურებში მონაწილე ნებისმიერი პარამეტრის მნიშვნელობა უცნობია მომსახურე პერსონალისათვის; კორპორაციული ქსელის არაკანონიერ მომხმარებელს შეუძლია ალგორითმის საწყისი მონაცემის (ორი დიდი მარტივი რიცხვის ნამრავლის) მოპოვება, მაგრამ ამ მონაცემით იგი ვერ შეძლებს გაშიფვრის საიდუმლო გასაღების გამოცნობას; დამშიფრავი გასაღები წარმოადგენს პროგრამულად გამოთვლილ შემთხვევით არჩეულ 27 მონაცემის მიმდევრობით გაერთიანებას და იგი შეიცავს წინასწარ გაურკვეველი რაოდენობის ათობითი ციფრების მიმდევრობას (ციფრების რაოდენობა დამოკიდებულია გამოთვლილი 44 მონაცემიდან თითოეულის თანრიგების რაოდენობაზე); ამ ალგორითმით შესაძლებელია მონაცემთა უფრო დიდი სიგრძის ბლოკების დაშიფვრა, ვიდრე არსებული სიმეტრიული კრიპტოალგორითმებით (AES სტანდარტის გამოყენებისას ერთ ციკლში იშიფრება 16 სიმბოლო, ხოლო ამ ალგორითმით 30 სიმბოლოზე მეტი).

ლიტერატურა:

1. Соколов А.Б., Маньгин В.Ф. (2002). Защита информации в распределенных корпоративных системах. -М., ДМК Процесс.

2. კუციავა ვ., კაცაძე გ., დიაკონიძე ქ. (2005). ინფორმაციის დაცვა. სტუ, „ტექნიკური უნივერსიტეტი". თბილისი.

3. კუციავა ვ., გოგოლაძე გ. (2013). ცვლადპარამეტრებიანი დაშიფვრის RSA კრიპტო-სისტემა. სტუ-ს შრ.კრებ., „მართვის ავტომატიზებული სისტემები", №2(15), გვ. 71-75.

NONSTANDARD BLOCK-STRUCTURED SYMMETRICAL CRYPTO ALGORITHM

Vasil Kusiava, Ana Kutsiava, Giorge Gogoladze

Georgian Technical University

Summary

The paper describes nonstandard block-structured symmetrical crypto algorithm for data encoding, where original method of generating and encoding procedure for the value of the secret key is used. The secret key with the random value is the multiplicity of serial decimal digits. This key is formed as a result of performing certain procedures entailed in the algorithm by the legal subscribers of the corporate network and its value is not known by service personnel. This algorithm enables to encode open text composed from any number of symbols presented by decimal system of ASCII or EBCDIC code. None of the real values of the parameters used in encoding procedures are transmitted through connection line of the corporate network. Presented algorithms is characterized by high crypto durability and speed.

НЕСТАНДАРТНЫЙ БЛОЧНЫЙ СИМЕТРИЧНЫЙ КРИПТОАЛГОРИТМ ДЛЯ ШИФРОВАНИЯ ДАННЫХ

Куциава В.А., Куциава А.В., Гоголадзе Г.Н.

Грузинский Технический Университет

Резюме

Рассмотрен нестандартный блочный симетричный криптографический алгоритм, в котором для получения значения секретного ключа и для осуществления процедур шифрования используется оригинальный метод. Секретный ключ со случайным значением представляет собой множество десятичных цифр, прописанных последовательно. Этот ключ формируется законными абонентами корпоративной сети программно, после выполнения определенных процедур, приведенных в алгоритме, и его значение неизвестно обслуживающему персоналу. При помощи алгоритма возможно шифрование открытого текста, состоящего из произвольного множества символов кода ASCII или EBCDIC, представленных в десятичной системе. Действительные значения ни одного параметра, применяемого в процедурах шифрования не передаются по линиям связи корпоративной сети. Предложенный алгоритм характеризуется высокой криптостойкостью и быстрым действием