1024 ბიტის შემცველი ბლოკის დაშიფვრის სიმეტრიული კრიპტოალგორითმი

ვასილ კუციავა, პაატა ჯღოხაძე, გიორგი გოგოლაძე
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია მონაცემთა ბლოკის დაშიფვრის კრიპტოგრაფიული ალგორითმი, რომელშიც გამოიყენება ბიტების გაბნევისა და შერევის ორიგინალური მეთოდი. ალგორითმი სიმეტრიულია და იძლევა 1024 ბიტის შემცველ მონაცემთა ბლოკის დაშიფვრის საშუალებას შემთხვევითი ხასიათის მქონე 64 რაოდენობის თექვსმეტბიტიანი გასაღებების გამოყენებით. პირველი საიდუმლო გასაღები Z_1, რომლის მნიშვნელობა უცნობია მომსახურე პერსონალისათვის, ფორმირდება ალგორითმში მოყვანილი გარკვეული პროცედურების შესრულების შედეგად, ხოლო შემდეგი გასაღებების შემადგენლობები განისაზღვრება $Z_{i+1}=D_i \oplus Z_i$ ($i \in N, i = 1 \dots 64$) გამოსახულებით, სადაც D_i ღია ტექსტის 16 ბიტიანი სიტყვაა. შემდეგ ხდება ორი ბაიტის შემცველი D_i ინფორმაციის შეცვლა Z_{i+1} გამოსახულებით და ამ უკანასკნელის შემადგენლობაში შემავალი ბიტების გაბნევა ალგორითმის მიხედვით. ყოველი შემდეგი 1024 ბიტის შემცველი მონაცემთა ბლოკის დაშიფვრისას პირველ საიდუმლო გასაღებს წარმოადგენს წინა ციკლის Z_{65} გასაღები. კორპორაციული ქსელის კავშირის ხაზში არ გადაიცემა დაშიფვრის პროცედურებში მონაწილე არცერთი პარამეტრის ნამდვილი მნიშვნელობა. ეს ალგორითმი გამოირჩევა კრიპტომედეგობით და მაღალი სწრაფქმედებით.

საკვანძო სიტყვები: შედგენილი შიფრი. სიმეტრიული ალგორითმი. ეილერის ფუნქცია. ჭადრაკის დაფა. საიდუმლო გასაღები. კრიპტომედეგობა. სწრაფქმედება.

1. შესავალი

შედგენილი შიფრები, რომლებიც მიიღება დასაშიფრ ღია ტექსტში შემავალი სიმბოლოების შესაბამისი ბიტების გაბნევისა და შერევის პრინციპების ერთობლივი გამოყენებით, ღია და დაშიფრული ტექსტების სტატისტიკური თვისებების ურთიერთკავშირების აღდენას ართულებს იმ დონემდე, რომ პრაქტიკულად შეუძლებელი ხდება დამშიფრავი საიდუმლო გასაღების მნიშვნელობის დადგენა მისი ცალკეული ნაწილების ცოდნის შემთხვევაშიც კი.

შედგენილი შიფრები გამოიყენება ისეთ კრიპტოალგორითმებში, როგორიცაა: DES, IDEA, RC2, RC5, SAST, AES და სხვა ბლოკური ალგორითმები. ამ 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 შეუძლია გასაღების მნიშვნელობების გადარჩევა, შესაბამისად 30 და 200 მილიონი ვარიანტი/წამშისიჩქარით. 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 კომპიუტერების საშუალებით კი 6 წუთში [1]. ამის გამო DES სტანდარტის ნაცვლად გამოიყენება AES სტანდარტი, რომლის საიდუმლო გასაღების სიგრძეა 128, 192 ან 256 ბიტი, ხოლო დასაშიფრი ბლოკის კი 128 ბიტი.

ზემოაღნიშნულიდან გამომდინარე მიზანშეწონილად ჩავთვალეთ კორპორაციულ ქსელებში გადაცემული ინფორმაციის კონფიდენციალობის შესანარჩუნებლად ისეთი სიმეტრიული ალგორითმის შემუშავება, რომელიც მუშაობს გაცილებით დიდი გასაღებით და ამასთან გამოირჩევა მაღალი კრიპტომედეგობით.

2. ძირითადი ნაწილი

შემუშავებული სიმეტრიული კრიპტოალგორითმით ხდება 1024 ბიტის შემცველი მონაცემთა ბლოკის დაშიფვრა. დასაშიფრი ინფორმაცია იყოფა 64 ჯგუფად (64*16=1024), თითოეული 16 ბიტიანი (ორ ბაიტიანი) ჯგუფი იკრიბება ორის მოდულით დამშიფრავ 16 ბიტიან გასაღებთან და მიღებული 16 ბიტი ნაწილდება 8x8 განზომილების მქონე 16 იდენტურ მატრიცაში (თითო ბიტი თითოეულ მატრიცაში). 64 პოზიციის დასანომრად პირობითად ავირჩიეთ ჭადრაკის დაფაზე (ნახ.1) მხედრის შემოვლის ჩაკეტილი მარშრუტი (მხედარი შემოივლის ყველა უჯრას და, ამასთან, იგი თითოეულ უჯრაზე მხოლოდ ერთხელ მოხვდება), რომელიც აღმოაჩინა ცნობილმა მათემატიკოსმა ლეონარდო ეილერმა 1759 წელს [2,3]. ამ სურათიდან გამომდინარე მარშრუტის დასაწყისად შეიძლება ნებისმიერი უჯრის აღება. მაგალითად, თუ შემოვლის მარშრუტი სტარტს აიღებს 38 ნომრის მქონე უჯრიდან, მაშინ მარშრუტი დამთავრდება 37 ნომრის უჯრაზე (ნომრის მატებით გადაადგილებისას) ან 39 ნომრის უჯრაზე (ნომრის კლებით გადაადგილებისას).

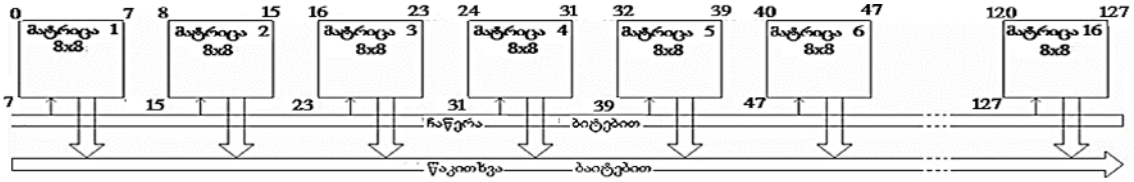
8	37	62	43	56	35	60	41	50
7	44	55	36	61	42	49	34	59
6	63	38	53	46	57	40	51	48
5	54	45	64	39	52	47	58	33
4	1	26	15	20	7	32	13	22
3	16	19	8	25	14	21	6	31
2	27	2	17	10	29	4	23	12
1	18	9	28	3	24	11	30	5
	a	b	c	d	e	f	g	h

ნახ.1.

16 ბიტის განაწილებისას ბიტების ნომრები შეიძლება არ დაემთხვეს მატრიცების ნომრებს, რადგან დაშიფვრის ალგორითმში გამოვიყენეთ მატრიცების განლაგების არჩევის 128 შემთხვევითი ვარიანტი (ვარიანტების საერთო რაოდენობა 16!-ის ტოლია). კერძოდ, შევადგინეთ მატრიცების განლაგების 8 ქვეჯგუფი, თითოეული 16 ვარიანტით. პირველ ცხრილში ნაჩვენებია სამი ქვეჯგუფი (№0, №2 და №6). დამუშავებული ალგორითმი ხასიათდება სიმარტივით და მაღალი კრიპტომედეგობით (თითოეული 1024 ბიტიანი ბლოკი იღებს 2^{1024} რაოდენობის მნიშვნელობიდან ერთ ერთს). დაშიფვრა სრულდება შემდეგი ორი ოპერაციის შესრულებით:

1. ორი ბაიტის შემცველი D_i ინფორმაციის შეცვლა Z_{i+1} გამოსახულებით, სადაც $\mathbf{Z_{i+1}}$დაშიფვრის გასაღებია და $Z_{i+1}=D_i \oplus Z_i$. ამასთან, პირველი ციკლის (პირველი 1024 ბიტის დაშიფვრა) დასაწყისში $\mathbf{Z_1}$გასაღები არის საიდუმლო $\mathbf{Z_0}$გასაღები, ხოლო ყოველი შემდეგი ციკლის დასაწყისში კი წინა ციკლის $\mathbf{Z_{65}}$ გასაღები;

2. M_i ბლოკებში შემავალი ბიტების განაწილება 16 მატრიცაში და შემდეგ დაშიფრული მიმდევრობის წაკითხვა. რადგან ყველა მატრიცა შეიცავს 128 (0-127) სტრიქონს და 128 (0-127) სვეტს, ამიტომ დაშიფვრის ყოველი ციკლის ბოლოს თითოეულ მატრიცაში ჩაწერილი 64 ბიტის წაკითხვა შეიძლება განხორციელდეს სტრიქონების ან სვეტების მიხედვით დაწყებული ნებისმიერი სტრიქონიდან ან სვეტიდან (ნახ.2), ამასთან, წაკითხვის პროცედურა შეიძლება შესრულდეს როგორც ნომრის მატებით, ისე კლებით.



ნახ.2

თითოეული მატრიცისათვის საწყისი პოზიციის (საწყისი ნომერი) და მატრიცაში ბიტების განაწილების მარშრუტის (ნომრის მატება ან კლება), მატრიცების განლაგების ვარიანტების (ქვეჯგუფისა და სტრიქონის ნომრის), სტრიქონების ან სვეტების მიხედვით წაკითხვის რეჟიმის, წასაკითხი სტრიქონის ან სვეტის საწყისი და შემდეგი ნომრის (მატება ან კლება) არჩევა ხდება პროგრამულად ციკლის დასაწყისში $\mathbf{Z_1}$ გასაღების შემადგენლობიდან გამომდინარე.

ცხრ.1

ქვეჯგუფის№	ვარიანტის№	მატრიცებისმიმდევრობა
0	0	8,14,9,3,12,15,5,1,11,16,4,6,13,10,7,2
	1	14,1,16,8,2,9,4,3,11,13,6,12,7,10,5,15
	2	3,5,9,14,11,2,16,10,4,15,7,13,12,6,8,1
	3	11,1,5,12,16,9,14,2,6,15,3,8,13,10,4,7
	4	5,12,8,15,13,6,1,10,3,9,14,7,2,11,16,4
	5	16,13,4,7,3,10,9,12,15,5,11,12,8,6,1,14
	6	6,9,5,11,1,16,14,15,3,13,7,12,4,10,2,8
	7	4,8,13,6,15,2,11,9,16,1,10,7,14,3,12,5
	8	12,2,8,15,11,9,4,14,10,5,7,13,3,6,1,16
	9	15,11,1,7,13,6,9,10,4,16,8,3,12,2,5,14
	10	2,15,12,4,11,7,6,16,8,13,5,1,10,9,14,3
	11	7,10,2,15,4,8,9,1,14,11,6,16,12,5,3,13
	12	10,15,1,9,12,6,5,16,4,13,8,3,14,7,2,11
	13	9,13,4,1,6,14,5,2,10,16,3,8,11,15,7,12
	14	12,3,7,15,14,1,16,13,5,10,2, 9,4,11,8,6
	15	13,15,1,8,7,4,6,10,12,3,11,5,2,16,14,9
2	0	13,1,8,6,10,4,12,14,2,16,11,5,15,9,7,3
	1	2,5,7,11,14,13,9,1,15,6,16,10,3,8,12,4
	2	5,3,9,7, 2,13,15,12,4,14,10,16,1,11,6,8
	3	7,10,1,16,5,3,11,15,13,12,2,14,8,4,9,6
	4	1,8,5,9,11,16,15,3,7,14,4,6,12,10,2,13
	5	4,10,14,13,8,15,1,12,2,6,11,7,3,16,9,5
	6	14,4,13,1,12,10,3,5,11,8,15,16,6,9,7,2
	7	9,14,3,8,15,10,4,11,6,1,13,5,7,2,12,16
	8	6,9,4,16,2,5,14,8,15,13,1,12,11,10,3,7
	9	3,6,7,10,1,9,13,2,12,15,8,11,4,16,14,15
	10	14,2,5,7,15,11,13,16,9,4,6,1,12,3,8,10
	11	8,5,16,3,9,15,2,13,14,11,10,7,6,1,4,12
	12	11,9,8,4,12,1,7,14,3,15,2,16,10,13,6,5
	13	13,6,10,7,4,15,12,16,1,14,9,3,11,2,5,8
	14	12,7,2,5,3,10,15,11,13,16,6,4,8,14,1,9
	15	16,5,9,14,7,12,1,4,15,3,8,2,11,6,10,13
6	0	5,2,11,13,9,8,16,4,7,15,10,14,6,3,12,1
	1	7,14,16,4,10,5,9,3,15,11,6,8,1,13,2,12
	2	1,11,3,15,6,7,4,12,10,5,8,16,14,9,2,13
	3	4,16,7,1,10,15,6,8,5,14,2,13,9,12,3,11
	4	3,12,15,9,4,14,6,5,16,8,2,7,13,11,1,10
	5	11,9,13,5,6,1,3,10,2,4,16,12,7,15,8,14
	6	2,13,8,7,1,4,15,11,9,3,5,14,10,6,12,16
	7	15,8,12,16,7,4,13,3,11,14,2,9,5,6,1,10
	8	6,16,13,8,4,10,9,1,15,7,5,12,3,14,11,2
	9	9,15,5,7,14,16,2,12,1,6,11,13,8,10,4,3
	10	13,10,1,5,12,7,4,3,16,6,2,14,11,9,8,15
	11	8,1,16,3,4,2,9,15,11,5,13,10,12,6,14,7
	12	10,12,7,1,16,5,4,14,13,11,9,2,15,8,3,6
	13	12,7,6,14,2,8,15,9,4,1,10,16,13,3,11,5
	14	14,6,11,15,1,7,4,8,2,13,3,5,10,16,12,9
	15	16,5,13,10,4,9,3,12,15,7,6,11,1,8,2,14

პირველი ციკლის Z_1 გასაღების დასაფორმირებელი Z_0 გასაღების მიღების ალგორითმი.

კორპორაციული ქსელის ორი მომხმარებლიდან (პირობითად **A** და **B**), თუ **A** ინფორმაციის გადამცემია, ხოლო **B** კი მიმღები, მაშინ **B** აგზავნის **A**–სთან ორი დიდი $\mathbf{P_0}$ და $\mathbf{Q_0}$ მარტივი რიცხვების ნამრავლს$\mathbf{N_0}=\mathbf{P_0}\cdot\mathbf{Q_0}$(თითოეულითანამამრავლიოთხთანრიგაათობითირიცხვიადა$\mathbf{P_0}\geq\mathbf{Q_0}$). ამასთან, $\mathbf{P_0}$ და $\mathbf{Q_0}$ მარტივი რიცხვების შემთხვევითი არჩევა ხდება მარტივი რიცხვების ბაზიდან (მომსახურე პერსონალმა არ იცის არჩეული რიცხვების მნიშვნელობები). **A** მომხმარებელი $\mathbf{N_0}$ რიცხვიდან აღადგენს $\mathbf{P_0}$ და $\mathbf{Q_0}$ რიცხვებს. ამ რიცხვების მნიშნელობების ცოდნა უზრუნველყოფს **A** და **B** მომხმარებლების პარალელურ მუშაობას ერთიდაიმავე ალგორითმით საიდუმლო გასაღების მისაღებად. კერძოდ:

1. გამოითვლება: ა) $\boldsymbol{\varphi_0(N_0)mod10}$და ბ)$\boldsymbol{\varphi_0(N_0)mod15}$ მნიშვნელობები.
2. განისაზღვრება$\mathbf{P_1}$და $\mathbf{Q_1}$რიცხვებისერთეულოვანთანრიგშიგანთავსებული$\mathbf{a}$ და b ციფრებისაგანშედგენილი(a,b) წყვილი. ცხადია, რომ $a\in\{\mathbf{1},\mathbf{3},\mathbf{7},\mathbf{9}\}$ და $b\in\{1,3,7,9\}$.
3. მე-2ცხრილშიგანთავსებულიმარტივირიცხვებისდაბოლოებებისთექვსმეტივარიანტისგანშედგენილი{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}ხუთიგანსხვავებულიქვეჯგუფიდან (ქვეჯგუფებისრაოდენობა 16!–ის ტოლია) შეირჩევაერთ-ერთიქვეჯგუფი მე-2 პუნქტშიგამოთვლილი$\boldsymbol{\varphi_0(N_0)mod10}$ შედეგის მიხედვით. რადგანეილერისფუნქციისმნიშვნელობალუწირიცხვია, ამიტომგამოთვლითმიიღება 0,2,4,6 და 8 რიცხვებიდანერთ-ერთი. ამრიცხვებითხდებათითოეულმატრიცაშიქვეჯგუფისნომრისგანსაზღვრა$(0\to1,\ 2\to2,\ 4\to3,\ 6\to4,\ 8\to5)$. $\boldsymbol{\varphi_0(N_0)mod15}$-ის შედეგის მიხედვით (შესაძლებელია 15 მთელი რიცხვის მიღება 0-დან 14-ის ჩათვლით) განისაზღვრებაქვეჯგუფისტრიქონისნომერი.

ცხრ.2

ვარიანტის№	ქვეჯგუფი№1	ქვეჯგუფი№2	ქვეჯგუფი№3	ქვეჯგუფი№4	ქვეჯგუფი№5
0	3,1	1,3	9,9	9,1	1,7
1	7,9	3,7	1,1	1,3	9,9
2	1,7	1,9	7,3	3,7	7,7
3	9,3	3,9	3,9	1,9	3,3
4	7,1	7,3	7,7	9,7	3,1
5	3,7	9,3	3,1	7,9	7,3
6	1,9	1,1	7,9	7,1	9,3
7	9,7	1,7	1,7	3,9	1,1
8	1,3	9,9	9,3	7,3	7,9
9	9,1	7,7	7,1	9,3	1,9
10	3,3	3,3	3,7	1,1	3,9
11	9,9	3,1	1,9	1,7	9,1
12	1,1	9,7	9,7	9,9	1,3
13	7,3	9,1	1,3	7,7	3,7
14	3,9	7,9	9,1	3,3	7,1
15	7,7	7,1	3,3	3,1	9,7

ეს მატრიცა და 8x8 მატრიცების განლაგების ქვეჯგუფები ალგორითმის საიდუმლო გასაღებებია და მათი შემადგენლობა ცნობილი უნდა იყოს მხოლოდ კორპორაციულ ქსელში ჩართული მომხმარებლებისთვის. ალგორითმის კრიპტომედეგობის გასაზრდელად მიზანშეწონილია ამ მატრიცის და მატრიცების განლაგების ქვეჯგუფების შემადგენლობათა ცვლილება დროის გარკვეული პერიოდის გასვლის შემდეგ.

შტრიქონის შერჩევისას (a,b) წყვილის შესაბამისი კომბინაცია დროებით გადადის ქვეჯგუფის ბოლო მე-15 სტრიქონში გამეორების გამოსარიცხად.

განვიხილოთ ორი შემთხვევა:

1. ვთქვათ $P_0 = 4261, Q_0 = 2819, N_0 = P_0 \cdot Q_0 = 4261 \cdot 2819 = 12011759, (a,b) \rightarrow (1,9)$,

$$\varphi_0(N_0) = (P_0 - 1) \cdot (Q_0 - 1) = 4260 \cdot 2818 = 12004680;$$

$$\varphi_0(N_0) \bmod 10 = 12204680 (\bmod 10) \equiv 0; \varphi_0(N_0) \bmod 15 = 12204680 (\bmod 15) \equiv 0.$$

ე.ი. ცხრილი 2-დან შეირჩევა პირველი ქვეჯგუფი და ნულოვან სტრიქონში განთავსებული (c,d) წყვილი, რომელიც არის (3,1).

2. თქვათ $P_0 = 4273, Q_0 = 3217, N_0 = 4273 \cdot 3217 = 13746241, (a,b) \rightarrow (3,7)$,

$$\varphi_0(N_0) = 4272 \cdot 3216 = 13738752;$$

$$\varphi_0(N_0) \bmod 10 = 13738752 (\bmod 10) \equiv 2; \varphi_0(N_0) \bmod 15 = 13738752 (\bmod 15) \equiv 12.$$

მე-2ქვეჯგუფისდა მე-12სტრიქონში (მე-13 სტრიქონი ხდებამე-12სტრიქონი, რადგანპირველისტრიქონიგადადის ბოლოში) განთავსებული (c,d) წყვილი, რომელიცარის (9,1).

5. განისაზღვრებაახალიმარტივი P_1 და Q_1 რიცხვები შემდეგი თანაფარდობებით: $P_1 = P_0 + c - a + 100\alpha$და$Q_1 = Q_0 + d - b + 100\alpha$, სადაც $\alpha \in N$ და იცვლება ერთიდან ზემოთ მანამ, სანამ თითოეულირიცხვიარგახდებამარტივი. განხილულიპირველიმაგალითისშემთხვევაში: $P_1 = P_0 + c - a + 100\alpha = 4261 + 3 - 1 + 100\alpha = 4263 + 100\alpha$, როცა $\alpha = 1$, მაშინ $P_1 = 4363$ და ეს რიცხვი მარტივია; $Q_1 = Q_0 + d - b + 100\alpha = 2819 + 1 - 9 + 100\alpha = 2811 + 100\alpha$, როცა $\alpha = 2$, მაშინ $Q_1 = 3011$ და ეს რიცხვი მარტივია.

მეორემაგალითისშემთხვევაში: $P_1 = P_0 + c - a + 10\alpha = 4273 + 9 - 3 + 100\alpha = 4279 + 100\alpha$, როცა $\alpha = 4$, მაშინ $P_1 = 4679$ და ეს რიცხვი მარტივია; $Q_1 = Q_0 + d - b + 100\alpha = 3217 + 1 - 7 + 100\alpha = 3211 + 100\alpha$, როცა $\alpha = 3$, მაშინ $Q_1 = 3511$ და ეს რიცხვი მარტივია.

6. გამოთვლილი P_1 და Q_1 რიცხვები წარმოიდგინებიან ორობით სისტემაში, ჩამოშორდებათ ბოლო მარჯვენა თითო ბიტი და თითოეულის რვა ბიტის (მარჯვნიდან მარცხნივ) ერთმანეთის გვერდით მიწერით მიიღება საწყისი საიდუმლო გასაღები Z_0. განხილული მაგალითების შემთხვევაში გვექნება:

1. $P_1 = 4363 = 1000100001011B$ -10000101, $Q_1 = 3011 = 101111000011B$ -11100001 და $Z_0 = 1000010111100001$.

2. $P_1 = 4679 = 1001001000111B$ -00100011, $Q_1 = 3511 = 110110110111B$ -11011011 და $Z_0 = 0010001111011011$.

როგორც ზემოთ აღვნიშნეთ $\mathbf{Z_I}$ გასაღების შემადგენლობით ხდება დაშიფვრის პროცესის მართვა. კერძოდ, თუ $\mathbf{Z_1\text{-}K_1K_2\,K_3K_4K_5K_6K_7K_8K_9K_{10}K_{11}K_{12}K_{13}K_{14}K_{15}K_{16}}$, სადაც $\mathbf{K_i}$ $\mathbf{Z_i}$ გასაღების **i**–ური ბიტია, მაშინ: $\mathbf{K_3K_9K_{14}}$–ის შესაბამისი ათობითი რიცხვი განსაზღვრავს მატრიცების განლაგების ქვეჯგუფის ნომერს; $\mathbf{K_2K_7K_{11}K_{15}}$–ის შესაბამისი ათობითი რიცხვი ქვეჯგუფში სტრიქონის ნომერს; $\mathbf{K_4K_5K_6K_{10}K_{12}K_{13}}$–ის შესაბამისი ათობითი რიცხვი გადიდებული ერთით მატრიცებში $\mathbf{Z_2}$ ბაიტის ბიტების ჩაწერის საწყისს ნომერს (რადგან მატრიცის უჯრების დანომვრა იწყება 1-დან), ამასთან თითოეულ მატრიცაში მარშრუტის მიმართულება განისაზღვრება $\mathbf{Z_I}$ გასაღების შესაბამისი ბიტის დონით (1-მატება, 0-კლება). ე.ი. თუ $\mathbf{K_1=1}$ და $\mathbf{K_7=0}$, მაშინ პირველ მატრიცაში მარშრუტი გრძელდებან ნომრის მატებით, ხოლო მეშვიდე მატრიცაში კინომრის კლებით; $\mathbf{K_1 \oplus K_{16} = 1}$- მატრიცებიდან წაკითხვა სტიქონებით, ხოლო $\mathbf{K_1 \oplus K_{16} = 0}$ წაკითხვა სვეტებით; $\mathbf{K_3K_6K_8K_{11}K_{13}K_{15}K_{16}}$–ის შესაბამისი ათობითი რიცხვი განსაზღვრავს პირველად წასაკითხი სტრიქონის ან სვეტის ნომერს, ამასთან, თუ $\mathbf{K_5 \oplus K_{14} = 1}$ – წაკითხვა ნომრის მატებით, ხოლო, თუ $\mathbf{K_5 \oplus K_{14} = 0}$– წაკითხვა ნომრის კლებით.

ზემოთმიღებული$\mathbf{Z_I}$გასაღებისპირველიმნიშვნელობისშემთხვევაში:

K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}	K_{12}	K_{13}	K_{14}	K_{15}	K_{16}
1	0	0	0	0	1	0	1	1	1	1	0	0	0	0	1

$K_3K_9K_{14}$- 010=2- მატრიცების განლაგების ქვეჯგუფის ნომერია 2; **$K_2K_7K_{11}K_{15}$- 0010=2-** ქვეჯგუფში სტრიქონის ნომერი 2 (მატრიცების განლაგებაა 5,3,9,7,2,13,15,12,4,14,10,16,1,11,6,8); **$K_4K_5K_6K_{10}K_{12}K_{13}$-001100-**მატრიცებში **$M_1$** ბაიტის პირველი ბიტის ჩაწერის საწყისი ნომერი 12+1=13 (ამასთან, 1-5, 6-13, 8-12, 9-4, 10-14, 11-10, 16-8 მატრიცებში მარშრუტი გრძელდება ნომრის მატებით, ხოლო 2-3, 3-9, 4-7, 5-2, 7-15, 12-16, 13-1, 14-11, 15-6 მატრიცებში კი კლებით); **$K_1 \oplus K_{16}$ =1⊕1=0-**მატრიცებიდან წაკითხვა სვეტებით; **$K_3K_6K_8K_{11}K_{13}K_{15}K_{16}$-0111001-** პირველად წასაკითხი სვეტის ნომერი 57; **$K_5 \oplus K_{14}$ =0⊕0=0-**წაკითხვა ნომრის კლებით.

Z_1 გასაღების მეორე მნიშვნელობის შემთხვევაში:

K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}	K_{12}	K_{13}	K_{14}	K_{15}	K_{16}
0	0	1	0	0	0	1	1	1	1	0	1	1	0	1	1

$K_3K_9K_{14}$- 110=6-მატრიცების განლაგების ქვეჯგუფის ნომერია 6;

$K_2K_7K_{11}K_{15}$- 0101=5- ქვეჯგუფში სტრიქონის ნომერი 5 (მატრიცების განლაგებაა 11, 9, 13, 5, 6, 1, 3, 10, 2, 4, 16, 12, 7, 15, 8, 14);

$K_4K_5K_6K_{10}K_{12}K_{13}$-000111 მატრიცებში **$M_1$** ბაიტის პირველი ბიტის ჩაწერის საწყისი ნომერი 7+1=8 (ამასთან, 3-13, 7-3, 8-10, 9-2, 10-4, 12-12, 13-7, 15-8, 16-14 მატრიცებში მარშრუტი გრძელდება ნომრის მატებით, ხოლო 1-11, 2-9, 4-5, 5-6, 6-1, 11-16, 14-15 მატრიცებში კი კლებით);

$K_1 \oplus K_{16}$ =0⊕1=1-მატრიცებიდან წაკითხვა სტრიქონებით;

$K_3K_6K_8K_{11}K_{13}K_{15}K_{16}$-1010111-პირველად წასაკითხი სტრიქონის ნომერი 87;

$K_5 \oplus K_{14}$ =0⊕0=0-წაკითხვა ნომრის კლებით.

თითოეულ ციკლში წაკითხული ინფორმაციის ყოველი ოთხი ბიტი წარმოიდგინება თექვსმეტობითი თვლის სისტემით (მიიღება 256 სიმბოლო) და ასეთი სახით მიღებული მთლიანი შიფრტექსტი, რომელიც შედგება 256·n სიმბოლოსგან (n ციკლების რაოდენობაა, რომელიც განისაზღვრება დასაშიფრი ბაიტების საერთო რაოდენობის გამომსახველი რიცხვის გაყოფით 128-ზე, დამრგვალებული უახლოეს მთელ რიცხვამდე მეტობით) გადაიცემა მიმღებისაკენ.

3. დასკვნა

ჩვენს მიერ შემუშავებულ ალგორითმს აქვს შემდეგი ღირსებები: დაშიფვრის ყოველ ციკლში იშიფრება 1024 ბიტის (128 ბაიტის) შემცველი მიმდევრობა, ყოველ ციკლში მონაწილეობს შემთხვევითი შემადგენლობის მქონე 1024 ბიტის სიგრძის გასაღები, გასაღების მნიშვნელობის ფორმირებაში მონაწილეობას იღებენ ღია ტექსტის მონაცემები, მატრიცებში ბიტების განლაგების და მატრიცებიდან მათი წაკითხვის თანმიმდევრობას აქვს შემთხვევითი ხასიათი, დაშიფვრისა და გაშიფვრის პროცედურებისათვის რთული კვანძების არ საჭიროება განაპირობებს ალგორითმის ადვილად გადაწყობის შესაძლებლობას.

ალგორითმი გამოირჩევა სწრაფქმედებით, კრიპტოგრაფიული მედეგობით (კავშირის ხაზში არ გადაიცემა დაშიფვრისა და გაშიფვრის პროცედურებში მონაწილე არც ერთი პარამეტრი, ახალი მარტივი რიცხვების დაბოლოებების განმსაზღვრელი ცხრილის და მატრიცების განლაგების ჯგუფების შემადგენლობა იცვლება დროის გარკვეული პერიოდის გასვლის შემდეგ); ერთმანეთის მიყოლებით განმეორებადი 1024 ბიტის შემცველი მიმდევრობების დაშიფვრისას მიიღება განსხვავებული შიფრტექსტები.

ლიტერატურა:

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

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

3. Куциава В.А., Джохадзе П.Д., Гоголадзе Г.Н. (2013). Алгоритм шифрования данных. Georgian Engineering News, №2, с.9-13.

SYMMETRICAL CRYPTOALGORITHM FOR ENCODING 1024 BIT LONG BLOCK

KutsiavaVasili, Jokhadze Paata, Gogoladze Georgi
Georgian Technical University

Summary

The paper reviews cryptographic algorithm for encoding data block, which uses original method of bits displacement and diffusion. Algorithm is symmetrical and allows encoding the 1024 bit long blocks using 64 random 16 bit long key. The first secret key Z_1, which value is unknown for service personnel, is formed as a result of performing certain procedures given in the algorithm, whereas, the value of each next key is defined by $Z_{i+1}=D_i \oplus Z_i (i \in N, i = 1 \dots 64)$ formula, where D_i is 16 bit long word of an open text. After that D_i information, containing 16 bites, is substituted by $Z_{i+1}$and the bits included in the latter are diffused by the algorithm. The first secret key is the previous cycle's Z_{65}key in encoding every next 1024 bit long data block. Corporate network connection line does not transfer any real value of parameter, which is used in encoding procedures. The proposed algorithm is robust and fast.

СИММЕТРИЧНЫЙ КРИПТОАЛГОРИТМ ШИФРОВАНИЯ БЛОКА ДАННЫХ, СОДЕРЖАЩЕГО 1024 БИТА

Куциава В.А., Джохадзе П.Д., Гоголадзе Г.Н.
Грузинский Технический Университет

Резюме

Рассмотрен криптографический алгоритм для шифрования блока данных, в котором используется оригинальный метод смещения и размещения битов. Алгоритм является симметричным и позволяет шифровать блоки данных содержащих 1024 бита при помощи шестдесятьчетырех 16-битных случайных ключей. Первый секретный ключ Z_1, значение которого неизвестно обслуживающему персоналу, формируется после выполнения определенных процедур, приведенных в алгоритме, а составы последующих ключей определяются при помощи выражения $Z_{i+1}=D_i \oplus Z_i (i \in N, i = 1 \dots 64)$, где D_i 16-битовое слово открытого текста. Далее происходит замена двухбайтовой информации D_i выражениемZ_{i+1}и размещение входящих в него битов по алгоритму. Первым секретным ключом при шифровании каждого последующего блока данных, содержащего 1024 бит, является ключ Z_{65} предыдущего цикла. В линии связи корпоративной сети не передаются действительное значения ни одного параметра, применяемого в процедурах шифрования. Предложенный алгоритм характеризуется стойкостью и высоким быстродействием.