ინფორმაციის დაშიფვრის სიმეტრიული კრიპტოგრაფიული სისტემებისათვის საიდუმლო გასაღების მაფორმირებელი ალგორითმი

ვასილ კუციავა, ანა კუციავა, ქეთევან გოგუა,
გიორგი გოგოლაძე
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია ინფორმაციის დაშიფვრის სიმეტრიული კრიპტოგრაფიული სისტემებისათვის საიდუმლო გასაღების მაფორმირებელი ორიგინალური ალგორითმი. ამ ალგორითმით ხდება შემთხვევითი მნიშვნელობის და შემთხვევითი სიგრძის მქონე საიდუმლო გასაღების მიღება. გასაღები შედგება მიმდევრობით დაწერილი დიდი რაოდენობის ათობითი ციფრებისგან და იგი ფორმირდება პროგრამულად ალგორითმში მოყვანილი გარკვეული პროცედურების შესრულების შედეგად. კორპორაციული ქსელის კავშირის ხაზში არ გადაიცემა დაშიფვრის პროცედურებში მონაწილე არც ერთი პარამეტრის ნამდვილი მნიშვნელობა. გასაღების მნიშვნელობა უცნობია კორპორაციულ ქსელში ჩართული კანონიერი მომხმარებლების მომსახურე პერსონალისათვის. წარმოდგენილი ალგორითმი გამოირჩევა კრიპტომედეგობით და მაღალი სწრაფქმედებით.

საკვანძო სიტყვები: სიმეტრიული კრიპტოგრაფიული სისტემა. ეილერის ფუნქცია. საიდუმლო გასაღები. მატრიცა.კვადრატული გამონაქვითი. მარტივი რიცხვი.

1. შესავალი

კორპორაციულ ქსელებში ჩართულ კანონიერ მომხმარებლებს შორის გადაცემული ინფორმაციის კონფიდენციალურობის უზრუნველსაყოფად ფართოდ გამოიყენება სიმეტრიული (მაგალითად: DES,$IDEA$,$RC2$,$RC5$,AESდა სხვ.) კრიპტოგრაფიული სისტემები. ამ სისტემების ძირითადი ნაკლი არის ის, რომ გადასაცემი ინფორმაციის დაშიფვრისას მთელი ინფორმაცია იყოფა გარკვეული სიგრძის ბლოკებად (56-დან 128 ორობით ბიტამდე) და ყველა ბლოკის დაშიფვრა-გაშიფვრა სრულდება ერთი და იმავე სადუმლო გასაღებით. ამ გარემოების გამო კავშირის არხთან მიერთებულ არაკანონიერ მიმღებს შეუძლია განახორციელოს კრიპტოანალიზური შეტევა გასაღებების ყველა შესაძლო ვარიანტების გადარჩევის მეთოდით ან ბანდიტური კრიპტოანალიზის შედეგად (გასაღების მნიშვნელობის მოპოვება დაშინების, წამების, შანტაჟის ან ქრთამის მიცემის გზით).

ამ ნაკლის უგულებელსაყოფად მიზანშეწონილია საიდუმლო გასაღების მნიშვნელობის მისაღებადისეთი ალგორითმის შემუშავება, რომელიც ქსელში ჩართული კანონიერი მომხმარებლების მომსახურე პერსონალის ყოველგვარი მონაწილეობის გარეშე (გამოირიცხება ბანდიტური კრიპტოანალიზი) პროგრამულად დააფორმირებს 128 ბიტზე გაცილებით მეტი სიგრძის გასაღებს (რაც უფრო დიდია გასაღების სიგრძე, მით უფრო ძნელია ყველა შესაძლებელი ვარიანტის გადარჩევა). გასაღების დასაფორმირებელ ალგორითმში გათვალისწინებული უნდა იყოს: მრავალი პროცედურის შესრულების საჭიროება; თითოეული პროცედურა უნდა სრულდებოდეს სხვადასხვა ვარიანტით; სასურველი ვარიანტის არჩევა უნდა ხდებოდეს პროგრამულად.

2. ძირითადი ნაწილი

კორპორაციული ქსელის ორი მომხმარებლიდან ინფორმაციის გადამცემი მხარე ახდენს: სამი მარტივი P_0,Q_0 დაR_0რიცხვის შემთხვევით არჩევას მარტივი რიცხვების შემცველი სამი

ბაზიდან(ერთი რიცხვი ერთი ბაზიდან); ამ რიცხვების დალაგებას $\boldsymbol{P_0 \geq Q_0 \geq R_0}$პირობის შესრულებით; საიდუმლო გასაღების ფორმირებას ქვემოთ განხილული ალგორითმის მიხედვით; ღია ტექსტის დაშიფვრას სიმეტრიული კრიპტოგრაფიული ალგორითმით; დაშიფრული ინფორმაციისა და არჩეული $\boldsymbol{P_0, Q_0}$ და$\boldsymbol{R_0}$რიცხვების ნამრავლის- $\boldsymbol{N_0 = P_0 \cdot Q_0 \cdot R_0}$გადაცემას ინფორმაციის მიმღებ მხარესთან. ეს უკანასკნელი $\boldsymbol{N_0}$რიცხვიდან აღადგენს $\boldsymbol{P_0, Q_0}$ და$\boldsymbol{R_0}$ რიცხვებს ($\boldsymbol{P_0 \geq Q_0 \geq R_0}$), საიდუმლო გასაღების მაფორმირებელი იმავე ალგორითმით დააფორმირებს გასაღებს და გაშიფრავს დაშიფრულ ტექსტს. საიდუმლო გასაღების ფორმირების ალგორითმი შემდეგში მდგომარეობს:

1. გამოითვლება ეილერის ფუნქციის მნიშვნელობა

$$\boldsymbol{\varphi_{i-1}(N_{i-1}) = (P_{i-1} - 1) \cdot (Q_{i-1} - 1) \cdot (R_{i-1} - 1)};$$

2. განისაზღვრება $\boldsymbol{P_{i-1}, Q_{i-1}}$და $\boldsymbol{R_{i-1}}$ რიცხვების ერთეულოვან თანრიგში მოთავსებული$\boldsymbol{a_{i-1}}$, $\boldsymbol{b_{i-1}}$ და$\boldsymbol{c_{i-1}}$ციფრებისაგან შედგენილი ($\boldsymbol{a_{i-1}, b_{i-1}, c_{i-1}}$) წყვილი. ცხადია, რომ თითოეული ეკუთვნის$\{\boldsymbol{1, 3, 7, 9}\}$სიმრავლეს;

3. გამოითვლება:$\boldsymbol{K_{i-1} = \varphi_{i-1}(N_{i-1}) mod 10}$, $\boldsymbol{T_{i-1} = \varphi_{i-1}(N_{i-1}) mod 15}$, $\boldsymbol{S_{i-1} = \varphi_{i-1}(N_{i-1}) mod 3}$მნიშვნელობები, სადაც $\boldsymbol{K_{i-1}}$, $\boldsymbol{T_{i-1}}$ და $\boldsymbol{S_{i-1}}$არაუარყოფითი მთელი რიცხვებია. რადგან ეილერის ფუნქციის $\boldsymbol{(\varphi_{i-1}(N_{i-1}))}$ მნიშვნელობა ლუწი რიცხვია, ამიტომ $\boldsymbol{K_{i-1}}$-ის გამოთვლისას მიიღება $\boldsymbol{0, 2, 4, 6}$ან$\boldsymbol{8}$; $\boldsymbol{T_{i-1}}$მიიღებს ერთ-ერთ მნიშვნელობას $\boldsymbol{[0, 14]}$შუალედიდან, ხოლო $\boldsymbol{S_{i-1}}$კი$\boldsymbol{0}$, $\boldsymbol{1}$ და $\boldsymbol{2}$ მნიშვნელობებიდან ერთ-ერთს;

4. ერთმანეთისგან განსხვავებული $\boldsymbol{15 \times 5}$ განზომილების მქონე სამი მატრიცისა ($\boldsymbol{0}$, $\boldsymbol{1}$ და $\boldsymbol{2}$) დამე-3 პუნქტში გამოთვლილი $\boldsymbol{K_{i-1}}$, $\boldsymbol{T_{i-1}}$ და $\boldsymbol{S_{i-1}}$მნიშვნელობების გამოყენებით განისაზღვრება მარტივი რიცხვების დაბოლოებების ახალი ($\boldsymbol{d_{i-1}, e_{i-1}, f_{i-1}}$) წყვილი.

მატრიცა-0

	K = 0	**K = 2**	**K = 4**	**K = 6**	**K = 8**
T = 0	1,3,1	9,3,1	7,9,9	1,7,7	7,1,7
T = 1	7,7,9	3,3,7	7,1,1	1,1,3	9,9,9
T = 2	3,1,7	7,1,9	3,7,3	9,3,7	3,7,7
T = 3	1,9,3	1,3,9	9,3,9	3,1,9	1,3,3
T = 4	3,7,1	1,7,3	7,7,7	9,9,7	1,3,1
T = 5	1,3,7	3,9,3	7,3,1	1,7,9	3,7,3
T = 6	9,1,9	3,1,1	3,7,9	1,9,1	1,9,3
T = 7	3,9,7	1,1,7	7,1,7	3,3,9	7,1,1
T = 8	7,1,3	1,9,9	7,9,3	9,7,3	9,7,9
T = 9	9,9,1	3,7,7	9,7,1	9,9,3	3,1,9
T = 10	9,3,3	7,3,3	7,3,7	1,1,1	9,3,9
T = 11	3,3,3	3,3,1	1,1,9	9,1,7	7,9,17
T = 12	9,1,1	1,9,7	7,9,7	3,9,9	9,1,3
T = 13	7,7,3	7,9,1	3,1,3	9,7,7	3,3,7
T = 14	7,3,9	7,7,1	3,9,1	1,7,1	3,7,1

მატრიცა-1

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

მატრიცა-2

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

თითოეული მატრიცა შეიცავს მარტივ რიცხვთა დაბოლოებების **75** ვარიანტს (**64** განსხვავებული და **11** გამეორება ამ **64**-დან) განაწილებულს თანაბრად ხუთ სვეტსა და **15** სტრიქონში. მატრიცის ნომერი შეირჩევა S_{i-1} –ის მნიშვნელობით, ხოლო მატრიცაში სვეტისა და სტრიქონის ნომრები შესაბამისად განისაზღვრება K_{i-1} და T_{i-1}მნიშვნელობებით. მაგალითად, ვთქვათ:

$$N_0 = 4935589,\ P_0 = 239, Q_0 = 193,\ R_0 = 107, (a_0, b_0, c_0) - (9,3,7).$$

როცა$i = 1$, მაშინ

$$\varphi_0(N_0) = 238 \cdot 192 \cdot 106 = 4843776, K_0 = 4843776(mod10) = 6,$$

$$T_0 = 4843776(mod15) = 6, \qquad S_0 = 4843776(mod3) = 0.$$

ე.ი. შეირჩევა ნულოვანი მატრიცის $K = 6$ სვეტსა და $T = 6$ სტრიქონში მოთავსებული (d_0,e_0,f_0) წყვილი, რომელიც არის (**1,9,1**);

5. განისაზღვრება ახალი მარტივი P_i, Q_iდა R_iრიცხვები შემდეგი თანაფარდობებით:

$P_i = P_{i-1} + d_{i-1} - a_{i-1} + 10\alpha$, $Q_i = Q_{i-1} + e_{i-1} - b_{i-1} + 10\alpha$და $R_i = R_{i-1} + f_{i-1} - c_{i-1} + +10\alpha$, სადაც $\alpha \in N$ და იცვლება ერთიდან ზემოთ მანამ, სანამ თითოეული რიცხვი არ გახდება მარტივი (აქ გამოიყენება მარტივი რიცხვის დამდგენი ალგორითმი). განხილული მაგალითის შემთხვევაში, როცა $i = 1$, მიიღება:

$$P_1 = P_0 + d_0 - a_0 + 10\alpha = 239 + 1 - 9 + 10\alpha = 231 + 10\alpha,$$

როცა $\alpha = 1$, მაშინ $P_1 = 241$ და ეს რიცხვი მარტივია;

$$Q_1 = Q_0 + e_0 - b_0 + 10\alpha = 193 + 9 - 3 + 10\alpha = 199 + 10\alpha,$$

როცა$\alpha = 3$, მაშინ $Q_1 = 229$ და ეს რიცხვი მარტივია;

$$R_1 = R_0 + f_0 - c_0 + 10\alpha = 107 + 1 - 7 + +10\alpha = 101 + 10\alpha,$$

როცა$\alpha = 3$, მაშინ $R_1 = 131$და ეს რიცხვი მარტივია;

6. გამოითვლება$N_i = P_i \cdot Q_i \cdot R_i$**;**

7. გამოითვლება: $m_i = a_{i-1} + b_{i-1} + c_{i-1} + d_{i-1} + e_{i-1} + f_{i-1}$;

8. გამოითვლება:$P^*_i = ((P_i - 1)/2 - m_i)^2 \ mod\ P_i$, $Q^*_i = ((Q_i - 1)/2 - m_i)^2 \ mod\ Q_i$და$R^*_i = ((R_i - 1)/2 - m_i)^2 \ mod\ R_i$, სადაც$P^*_i, Q^*_i$და$R^*_i$კვადრატული გამონაქვითებია, შესაბამისად P_i, Q_i და R_iმოდულებით.

ეს რვა პუნქტი გამეორდება სამ ციკლში $i = 1$, $i = 2$ და $i = 3$მნიშვნელობებისთვის. ამასთან, ყოველი შემდეგი ციკლის საწყის პარამეტრებს წარმოადგენს წინა ციკლში მიღებული **P**, **Q**და**R**მნიშვნელობები.

სამივე ციკლის შესრულების შემდეგ $i = 4$ მნიშვნელობისათვის გამოითვლება $T_{i-1}, \varphi_{i-1}(N_{i-1})$და$S_{i-1}$მნიშვნელობები. ზემოთ აღწერილი პროცედურების შესრულების შედეგად მიიღება:

$$N_1, N_2, N_3, \varphi_1(N_1), \quad \varphi_2(N_2), \quad \varphi_3(N_3),$$

$$P_1, P_2, P_3, Q_1, Q_2, Q_3, R_1, R_2, R_3, P^*_1, P^*_2, P^*_3, Q^*_1, Q^*_2, Q^*_3,$$

$R^*_1, R^*_2, R^*_3, K_0, K_1, K_2, K_3, T_0, T_1, T_2, T_3, S_0, S_1, S_2$ და S_3მნიშვნელობები.

$\mathbf{N}, \boldsymbol{\varphi}(\mathbf{N}), \mathbf{P}, \mathbf{Q}, \mathbf{R}, \boldsymbol{P}^*, \boldsymbol{Q}^*$და $\boldsymbol{R}^*$მნიშვნელობების მიხედვით გამოითვლება ერთსახელა პარამეტრებისათვის როგორც ორ-ორი, ისე სამ-სამი წევრის ნამრავლები და ჯამები. მიღებული შედეგების მიხედვით შეივსება ცხრილი 1 და თითოეულს მიენიჭება რიგითი ათობითი ნომერი.

ცხრ.1

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

№	$\boldsymbol{R}$	№	$\boldsymbol{P^*}$	№	$\boldsymbol{Q^*}$	№	$\boldsymbol{R^*}$
45	$\boldsymbol{R_1}$	56	$\boldsymbol{P^*_1}$	67	$\boldsymbol{Q^*_1}$	78	$\boldsymbol{R^*_1}$
46	$\boldsymbol{R_2}$	57	$\boldsymbol{P^*_2}$	68	$\boldsymbol{Q^*_2}$	79	$\boldsymbol{R^*_2}$
47	$\boldsymbol{R_3}$	58	$\boldsymbol{P^*_3}$	69	$\boldsymbol{Q^*_3}$	80	$\boldsymbol{R^*_3}$
48	$\boldsymbol{R_1 \cdot R_2}$	59	$\boldsymbol{P^*_1 \cdot P^*_2}$	70	$\boldsymbol{Q^*_1 \cdot Q^*_2}$	81	$\boldsymbol{R^*_1 \cdot R^*_2}$
49	$\boldsymbol{R_1 \cdot R_3}$	60	$\boldsymbol{P^*_1 \cdot P^*_3}$	71	$\boldsymbol{Q^*_1 \cdot Q^*_3}$	82	$\boldsymbol{R^*_1 \cdot R^*_3}$
50	$\boldsymbol{R_2 \cdot R_3}$	61	$\boldsymbol{P^*_2 \cdot P^*_3}$	72	$\boldsymbol{Q^*_2 \cdot Q^*_3}$	83	$\boldsymbol{R^*_2 \cdot R^*_3}$
51	$\boldsymbol{R_1 + R_2}$	62	$\boldsymbol{P^*_1 + P^*_2}$	73	$\boldsymbol{Q^*_1 + Q^*_2}$	84	$\boldsymbol{R^*_1 + R^*_2}$
52	$\boldsymbol{R_1 + R_3}$	63	$\boldsymbol{P^*_1 + P^*_3}$	74	$\boldsymbol{Q^*_1 + Q^*_3}$	85	$\boldsymbol{R^*_1 + R^*_3}$
53	$\boldsymbol{R_2 + R_3}$	64	$\boldsymbol{P^*_2 + P^*_3}$	75	$\boldsymbol{Q^*_2 + Q^*_3}$	86	$\boldsymbol{R^*_2 + R^*_3}$
54	$\boldsymbol{R_1 \cdot R_2 \cdot R_3}$	65	$\boldsymbol{P^*_1 \cdot P^*_2 \cdot P^*_3}$	76	$\boldsymbol{Q^*_1 \cdot Q^*_2 \cdot Q^*_3}$	87	$\boldsymbol{R^*_1 \cdot R^*_2 \cdot R^*_3}$
55	$\boldsymbol{R_1 + R_2 + R_3}$	66	$\boldsymbol{P^*_1 + P^*_2 + P^*_3}$	77	$\boldsymbol{Q^*_1 + Q^*_2 + Q^*_3}$	88	$\boldsymbol{R^*_1 + R^*_2 + R^*_3}$

ამ ცხრილში მოთავსებული **88** შედეგიდან ხდება საიდუმლო გასაღების შემადგენლობაში მონაწილე მონაცემების არჩევა მე-2 ცხრილისა და $\boldsymbol{K}$–ს მნიშვნელობის მიხედვით.

ცხრ.2

K	გასაღების მიმდევრობის შემადგენლობაში მონაწილე მონაცემები
$\mathbf{K = 0}$	$\mathbf{23, 39, 54, 1, 64, 73, 81, 18, 57, 76, 43, 29, 14, 8, 46, 85, 33, 9, 40, 11}$
$\mathbf{K = 2}$	$\mathbf{5, 62, 37, 26, 15, 48, 87, 70, 10, 41, 22, 66, 32, 51, 74, 82, 12, 45, 29, 56}$
$\mathbf{K = 4}$	$\mathbf{78, 50, 19, 11, 31, 61, 88, 67, 2, 24, 42, 65, 80, 13, 34, 71, 55, 16, 6, 44}$
$\mathbf{K = 6}$	$\mathbf{30, 52, 69, 4, 36, 53, 60, 77, 6, 44, 79, 25, 40, 86, 58, 72, 17, 5, 84, 27}$
$\mathbf{K = 8}$	$\mathbf{28, 84, 20, 7, 38, 49, 56, 68, 21, 59, 27, 3, 75, 83, 63, 47, 35, 4, 52, 13}$

ცხრილის თითოეულ სტრიქონში მოთავსებულია ოცი მონაცემი მათი გამომსახველი ნომრების შემთხვევითი განაწილებით. საიდუმლო გასაღები შეიცავს სამოც მონაცემს, ე.ი. სამ სტრიქონს. პირველი სტრიქონი აირჩევა K_1-ის, მეორე K_2-ის, ხოლო მესამე კი K_3-ის მნიშვნელობების მიხედვით (K-ს მნიშვნელობიდან გამომდინარე შესაძლებელია მოხდეს სტრიქონების გამეორება). ამ სამოც მონაცემში შემავალი ათობითი ციფრები განლაგდება ერთმანეთის გვერდით მარცხნიდან მარჯვნივ.

მაგალითად, თუ $K_1 = 0, K_2 = 2$ და $K_3 = 6$, მაშინ საიდუმლო გასაღების მიმდევრობაში შემავალი მონაცემებია:

23, 39, 54, 1, 64, 73, 81, 18, 57, 76, 43, 29, 14, 8, 46, 85, 33, 9, 40, 11, 5, 62, 37, 26, 15, 48, 87, 70, 10, 41, 22, 66, 32, 51, 74, 82, 12, 45, 29, 56, 30, 52, 69, 4, 36, 53, 60, 77, 6, 44, 79, 25, 40, 86, 58, 72, 17, 5, 84, 27.

ცხადია, რომ გასაღებში შემავალი ციფრების რაოდენობა დამოკიდებულია საწყისი მარტივი რიცხვების თანრიგებისა და გამოთვლების შედეგად მიღებული შედეგების თანრიგების რაოდენობაზე.

მე-3 ცხრილში მოცემულია ფორმირებული გასაღებების სიგრძეები როგორც ათობითი თანრიგების, ისე ორობითი ბიტების რაოდენობის მიხედვით სამი მარტივი რიცხვის სხვადასხვა სამეულების შემთხვევაში. იქვე ნაჩვენებია ამ გასაღებების ფორმირებაზე დახარჯული დროის მიახლოებითი მნიშვნელობები.

ცხრ.3

N_0	P_0	Q_0	R_0	ათობითი თანრიგების რაოდენობა	ორობითი ბიტების რაოდენობა	დახარჯული დრო მილიწამებში
1001	**13**	**11**	**7**	**232**	**998**	**0,90150**
932539661	**983**	**977**	**971**	**431**	**1721**	**1,2106**
967458601121	**9901**	**9887**	**9883**	**513**	**2052**	**1,833**
7997080271798713	**199999**	**199967**	**199961**	**626**	**2504**	**25,1251**

ცხრილის მიხედვით, როცა $N_0 = 932539661$, მაშინ საიდუმლო გასაღების ორობითი ბიტების რაოდენობაა 1724 და 128ბიტის შემცველი ინფორმაციული ბლოკის დაშიფრისას შესაძლებელია 13 $(1724/128 \approx 13)$ მიმდევრობითი ბლოკის დაშიფვრა სხვადასხვა გასაღებით.

როცა $N_0 = 7997080271798713$ მაშინ საიდუმლო გასაღებების ბლოკების რაოდენობა 19-ის ტოლია. 64 ბიტის შემცველი ინფორმაციული ბლოკების დაშიფვრისას საიდუმლო გასაღების ბლოკების რაოდენობა განხილული შემთხვევისათვის გაიზრდება ორჯერ (26 და 38). საიდუმლო გასაღების ორობითი ბიტების შემცველი კომბინაციის სახით გამოყენებისას მიზანშეწონილია ამ კომბინაციის დაძვრა მარცხნივ ერთი სიმბოლოთი (ათობითი ციფრის შესაბამისი ათი ორობითი კომბინაციის ნაცვლად მიიღება 16 კომბინაცია).

ალგორითმში გამოყენებული მატრიცებისა და როგორც პირველი ცხრილის (გამოანგარიშებული პარამეტრებისათვის გარკვეული ათობითი ნომრის მინიჭება), ისე მეორე ცხრილის

(თითოეულ სტრიქონში შემავალი პოზიციათა ათობითი ნომრები) შემადგენლობები წარმოადგენს ე.წ საიდუმლო გასაღებებს და ისინი იცვლება გარკვეული დროის გასვლის შემდეგ.

3. დასკვნა

ჩვენს მიერ შემუშავებულ ალგორითმს აქვს შემდეგი ღირსებები:

1. კავშირის ხაზში არ გადაიცემა საიდუმლო გასაღების ფორმირებაში უშუალოდ მონაწილე არცერთი პარამეტრის მნიშვნელობა;კორპორაციულ ქსელში ჩართული კანონიერი მომხმარებლების მომსახურე პერსონალმა არ იცის საიდუმლო გასაღებების მნიშვნელობები (ბანდიტური კრიპტოანალიზის მეთოდის გამოყენება შეუძლებელია);

2. მიუხედავად იმისა, რომ არაკანონიერ მომხმარებელს შეუძლია N_0რიცხვის ხელში ჩაგდება და მისი დაშლა მარტივ მამრავლებად, ის მაინც ვერ გამოიცნობს საიდუმლო გასაღების მნიშვნელობას (ალგორითმში მოცემულია გაგრძელებების მრავალი ვარიანტი: მარტივი რიცხვების დაბოლოებების არჩევის **64** ვარიანტი სამჯერ, გამოანგარიშებული პარამეტრებისათვის რიგითი ნომრების მინიჭება- ვარიანტების რაოდენობა **88**!–ის ტოლია, საიდუმლო გასაღებში შემავალი გამოთვლილი პარამეტრების მიმდევრობა და სხვ.);

3. რადგან საიდუმლო გასაღებში შემავალი ათობითი ციფრების რაოდენობა შემთხვევითი რიცხვია (დამოკიდებულია სასტარტო N_0რიცხვზე და მეორე ცხრილზე), ამიტომ საიდუმლო გასაღებების ბლოკების რაოდენობაც წარმოადგენს საიდუმლოებას (უცნობია მომსახურე პერსონალისათვის);

4. ეს ალგორითმი საიდუმლო გასაღებში შემავალი ათობითი ციფრების რაოდენობის საგრძნობლად გაზრდის შესაძლებლობას იძლევა, თუ ინფორმაციის გადამცემი გამოიყენებს სამი დიდი მარტივი რიცხვების არა ერთ, არამედ ორ, სამ და ა.შ. სამეულებს. ამ შემთხვევაში თითოეულ სამეულზე დაფორმირდება შესაბამისი საიდუმლო გასაღები და შემდეგ ამ გასაღებების ერთმანეთის მიყოლებით მიმდევრობითი გაერთიანებით მიიღება ერთი მთლიანი გასაღები;

5. ფორმირებული საიდუმლო გასაღები გამოიყენება მხოლოდ ერთი ღია ტექსტის დასაშიფრად (ყოველი შემდეგი ღია ტექსტის დასაშიფრად ფორმირდება ახალი საიდუმლო გასაღები);

6. რაც უფრო დიდია გასაღების სიგრძე, მით უფრო ძნელია ყველა შესაძლებელი ვარიანტის გადარჩევა (თუ საიდუმლო გასაღები შედგება n თანრიგისგან, მაშინ გადასარჩევ ვარიანტთა რაოდენობა 10^n-ის ტოლია).

ავტორების მიერ დამუშავებულია ამ ალგორითმის განმახორციელებელი პროგრამული უზრუნველყოფა.

ლიტერატურა - References - Литература:

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

2. კუციავა ვ., კუციავა ა., გოგოლაძე გ. (2015). მონაცემთა ბლოკის დაშიფვრის არასტანდარტული სიმეტრიუ-ლი კრიპტოალორითმი. სტუ-ს შრ.კრ., „მართვის ავტომატიზებული სისტემები", №1(19), გვ. 30-37.

FORMING ALGORITHM OF SECRET KEY FOR SYMMETRICAL CRYPTOGRAPHIC SYSTEMS OF INFORMATION ENCODING

KutsiavaVasil, Kutsiava Ana, Gogua Ketevan,
Gogoladze Giorge

Georgian Technical University

Summary

The paper describes original algorithm for the formation of secret key of information encoding for symmetrical cryptographic systems. This algorithm helps to generate secret key with random value and random length. The key is composed from large amount of sequential decimal digits and it is formed programmatically as a result of performing certain procedures entailed in the algorithm. None of the true values of the parameters participating in encoding procedures are transmitted through the connection line of corporate network. The value of the key is unknown for the personnel serving legal users of the corporate network. Presented algorithm is characterized by high speed and crypto durability.

АЛГОРИТМ ФОРМИРОВАНИЯ СЕКРЕТНОГО КЛЮЧА ДЛЯ СИММЕТРИЧНЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМ ШИФРОВАНИЯ ИНФОРМАЦИИ

Куциава В.А., Куциава А.В., Гогуа К.Н., Гоголадзе Г.Н.
Грузинский Технический Университет

Резюме

Рассмотрен оригинальный алгоритм формирования секретного ключа для симметричных криптографических систем шифрования информации. При помощи этого алгоритма осуществляется получение секретного ключа с случайным значением и случайной длиной. Ключ представляет собой множество десятичных цифр, прописанных последовательно и формируется программно в следствии выполнения определенных процедур, приведенных в алгоритме.Любое действительное значение параметра, применяемого в процедурах шифрования, не передается в линиях связи корпоративной сети.Значение ключа неизвестно обслуживающему персоналу законных абонентов корпоративной сети.Предложенный алгоритм характеризуется высокой криптостойкостью и быстродействием.

.