# კრიპტოგრაფიული სისტემებისათვის საიდუმლო გასაღების მაფორმირებელი ალგორითმი

ვასილ კუციავა, ანა კუციავა, ნატალია კობერიძე

საქართველოს ტექნიკური უნივერსიტეტი

**რეზიუმე**

განხილულია კორპორაციულ ქსელებში გამოყენებადი სიმეტრიული და ასიმეტრიული კრიპტოგრაფიული სისტემებისათვის დამშიფრავი საიდუმლო გასაღებების მაფორმირებელი ალგორითმი. სიმეტრიული სისტემებისათვის ხდება შემთხვევითი სიგრძისა და შემთხვევითი მნიშვნელობის მქონე საიდუმლო გასაღების ფორმირება, ხოლო ასიმეტრიული სისტემებისათვის კი დაშიფვრისა და გაშიფვრის საიდუმლო გასაღებების შემთხვევითი წყვილების ფორმირება. ამასთან, გასაღების ფორმირების პროცედურის ყოველი ახალი ციკლის შესრულებისას მიიღება საიდუმლო გასაღებების განსხვავებული მნიშვნელობები. კორპორაციული ქსელის კავშირის ხაზში არ გადაიცემა საიდუმლო გასაღების არც ერთი პარამეტრის ნამდვილი მნიშვნელობა. საიდუმლო გასაღების მნიშვნელობა უცნობია კორპორაციულ ქსელში ჩართული ყველა კანონიერი აბონენტის მომსახურე პერსონალისათვის. აქედან გამომდინარე ბოროტგამზრახველი კორპორაციულ ქსელის კავშირის ხაზში გადაცემული მონაცემების ხელში ჩაგდებით ან მომსახურე პერსონალის როგორც დაშანტაჟების, ისე მოსყიდვის მცდელობით ვერ შეძლებს საიდუმლო გასაღების დაუფლებას. წარმოდგენილი ალგორითმი გამოირჩევა კრიპტომედეგობით და მაღალი სწრაფქმედებით.

**საკვანძო სიტყვები:** სიმეტრიული კრიპტოგრაფიული სისტემა. ასიმეტრიული კრიპტოგრაფიული სისტემა. კორპორაციული ქსელი. საიდუმლო გასაღები. კრიპტომედეგობა. სწრაფქმედება.

## 1. შესავალი

კორპორაციულ ქსელებში ჩართულ კანონიერ მომხმარებლებს შორის ინფორმაციის მიმოცვლისას ფართოდ გამოიყენება როგორც სიმეტრიული, ისე ასიმეტრიული კრიპტოსისტემები. ამ სისტემებით გადაცემული ინფორმაციის კონფიდენციალობის უზრუნველყოფა შესაძლებელია განხორციელდეს მხოლოდ იმ შემთხვევაში, თუ მათში გამოყენებული საიდუმლო გასაღების მნიშვნელობა მიუწვდომელი იქნება როგორც ბოროტგამზრახველისათვის, ისე თითოეული კანონიერი აბონენტის მომსახურე პერსონალისათვის და ინფორმაციული ბლოკები დაიშიფრება სხვადასხვა საიდუმლო გასაღებების გამოყენებით.

## 2. ძირითადი ნაწილი

კორპორაციული ქსელის ორი მომხმარებლიდან (პირობითად $A$ და $B$), თუ $A$ წარმოადგენს ინფორმაციის გადამცემს, ხოლო $B$ კი მიმღებს, მაშინ $A$ –მომხმარებელი პროგრამულად ირჩევს შემთხვევით ოთხ დიდ $P_0, Q_0, R_0$ და $U_0$ ($P_0 \geq Q_0 \geq R_0 \geq U_0$) მარტივ რიცხვს. ამ მარტივი რიცხვების შემთხვევითი არჩევა ხდება მარტივი რიცხვების ბაზიდან და ამასთან, მომსახურე პერსონალმა არ იცის არჩეული რიცხვების მნიშვნელობები.

$P_0, Q_0, R_0$ და $U_0$ რიცხვების მნიშვნელობებით $A$ მომხმარებელი ახდენს საიდუმლო გასაღების მიღებას შემდეგი ალგორითმით:

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

2) განისაზღვრება $P_{i-1}, Q_{i-1}, R_{i-1}$ და $U_{i-1}$ რიცხვების ერთეულოვან თანრიგში მოთავსებული $a_{i-1}$, $b_{i-1}, c_{i-1}$ და $d_{i-1}$ ციფრებისაგან შედგენილი $(a_{i-1}, b_{i-1}, c_{i-1}, d_{i-1})$ ოთხეული. ცხადია, რომ $a_{i-1} \in \{1, 3, 7, 9\}$, $b_{i-1} \in \{1, 3, 7, 9\}$, $c_{i-1} \in \{1, 3, 7, 9\}$, $d_{i-1} \in \{1, 3, 7, 9\}$ და ასეთი ოთხეულების რაოდენობა ტოლია $2$ -ის;

3) გამოითვლება: $K_{i-1} \equiv \varphi_{i-1}(N_{i-1}) m \quad 1$ , $T_{i-1} \equiv \varphi_{i-1}(N_{i-1}) m \quad 1$ და $S_{i-1} \equiv (P_{i-1} + Q_{i-1} + + R_{i-1} + U_{i-1}) m \quad 3$ მნიშვნელობები, სადაც $K_{i-1}, T_{i-1}$ და $S_{i-1}$ არაუარყოფითი მთელი რიცხვებია. რადგან ეილერის ფუნქციის $\varphi_{i-1}(N_{i-1})$ მნიშვნელობა ლუწი რიცხვია, ამიტომ $K_{i-1}$ – ის გამოთვლისას მიიღება $0, 2, 4, 6, 8$ რიცხვებიდან ერთ-ერთი. $T_{i-1}$ მიიღებს ერთ-ერთ მთელ მნიშვნელობას $[0; 1]$ შუალედიდან, ხოლო $S_{i-1}$ კი $0, 1$ და $2$ მნიშვნელობებიდან ერთ-ერთს.

მაგალითად, ვთქვათ $N_0 = 6$ , $P_0 = 2$ , $Q_0 = 1$ , $R_0 = 1$ , $U_0 = 1$ $(a_0, b_0, c_0, d_0) - (9, 3, 9, 7)$. როცა $i = 1$, მაშინ $\varphi_0(N_0) = 2 \quad 1 \quad 1 \quad 1 \quad = 6$ ,
$K_0 \equiv 6 \quad (m \quad 1) = 8$, $T_0 \equiv 6 \quad (m \quad 1) = 17$,
$S_0 \equiv (2 \quad + 1 \quad + 1 \quad + 1 \quad) m \quad = 0$.

4) ერთმანეთისგან განსხვავებული $1$ x $5$ განზომილების მქონე სამი მატრიცისა და მე-3 პუნქტში გამოთვლილი $K_{i-1}, T_{i-1}$ და $S_{i-1}$ მნიშვნელობების გამოყენებით განისაზღვრება მატრიცის ნომერი და ამ მატრიცაში სვეტისა და სტრიქონის ნომერი. მატრიცის ნომერი შეირჩევა $S_{i-1}$ -ის მნიშვნელობით ($0$ – პირველი, $1$ – მეორე, $2$ – მესამე), ხოლო მატრიცაში სვეტისა და სტრიქონის ნომერი, შესაბამისად განისაზღვრება $K_{i-1}$ და $T_{i-1}$ მნიშვნელობებით. სამივე მატრიცა შეიცავს ოთხციფრა დაბოლოებების $2$ ვარიანტს, რომელთაგან $2$ ერთმანეთისგან განსხვავებულია, ხოლო $2$ კი წარმოადგენს ზოგიერთის გამეორებას. ამასთან, გამეორებებს შეიცავს მხოლოდ მესამე მატრიცა (რომელიღაც 15 ვარიანტი პირველი მატრიციდან და 14 მეორედან).

მესამე პუნქტში გამოთვლილი $K_0, T_0$ და $S_0$ მნიშვნელობებით შეირჩევა 1-ელი მატრიცის მე- $5$ სვეტსა და მე- $1$ სტრიქონში მოთავსებული $(e_0, f_0, g_0, h_0)$ წყვილი, რომელიც არის $(3, 9, 3, 9)$.

მატ.1

| T /K | K=0 | K=2 | K=4 | K=6 | K=8 |
|---|---|---|---|---|---|
| T=0 | 7, 9, 3, 7 | 3, 1, 3, 9 | 9, 3, 7, 7 | 7, 3, 3, 1 | 3, 7, 7, 9 |
| T=1 | 1, 1, 3, 3 | 3, 7, 7, 3 | 7, 3, 9, 9 | 3, 3, 9, 9 | 9, 7, 1, 9 |
| T=2 | 7, 1, 3, 3 | 1, 3, 7, 3 | 3, 3, 1, 7 | 9, 7, 7, 9 | 1, 7, 7, 3 |
| T=3 | 1, 1, 7, 9 | 3, 7, 1, 3 | 9, 7, 9, 1 | 9, 3, 1, 3 | 9, 7, 9, 7 |
| T=4 | 3, 7, 9, 3 | 9, 3, 7, 1 | 1, 7, 9, 7 | 1, 1, 9, 7 | 9, 3, 3, 1 |
| T=5 | 9, 1, 9, 3 | 9, 1, 1, 7 | 3, 9, 3, 3 | 3, 7, 3, 7 | 1, 9, 3, 3 |
| T=6 | 1, 9, 7, 1 | 3, 1, 1, 1 | 9, 7, 9, 9 | 9, 1, 7, 1 | 3, 3, 7, 1 |
| T=7 | 7, 1, 1, 3 | 9, 1, 3, 7 | 1, 3, 3, 7 | 1, 7, 9, 9 | 1, 3, 7, 9 |
| T=8 | 9, 9, 7, 3 | 1, 1, 1, 9 | 7, 3, 7, 9 | 9, 9, 3, 1 | 3, 9, 9, 9 |
| T=9 | 1, 3, 1, 9 | 7, 7, 9, 3 | 7, 9, 7, 7 | 3, 3, 1, 9 | 7, 1, 7, 3 |
| T=10 | 1, 7, 7, 7 | 9, 9, 3, 7 | 9, 9, 9, 9 | 1, 9, 1, 1 | 9, 1, 3, 3 |

| | | | | | |
|---|---|---|---|---|---|
| T=11 | 7, 1, 7, 1 | 3, 9, 9, 3 | 7, 7, 1, 9 | 7, 7, 1, 3 | 1, 7, 9, 3 |
| T=12 | 9, 9, 3, 9 | 9, 7, 7, 1 | 1, 3, 3, 3 | 7, 7, 9, 1 | 7, 9, 9, 1 |
| T=13 | 3, 9, 7, 3 | 7, 9, 9, 3 | 7, 1, 9, 7 | 9, 7, 1, 3 | 1, 1, 3, 9 |
| T=14 | 1, 7, 3, 7 | 3, 1, 1, 9 | 3, 3, 7, 3 | 1, 3, 9, 7 | 9, 3, 3, 3 |
| T=15 | 7, 9, 7, 3 | 3, 3, 7, 9 | 1, 9, 1, 3 | 3, 1, 9, 1 | 7, 3, 7, 1 |
| T=16 | 3, 9, 1, 7 | 1, 7, 3, 1 | 7, 3, 3, 9 | 9, 3, 9, 7 | 1, 3, 1, 1 |
| T=17 | 3, 1, 3, 3 | 7, 7, 3, 9 | 1, 1, 7, 7 | 1, 9, 3, 7 | 3, 9, 3, 9 |
| T=18 | 1, 9, 7, 9 | 3, 3, 9, 1 | 3, 1, 9, 7 | 7, 7, 1, 1 | 7, 7, 7, 7 |

5) განისაზღვრება ახალი მარტივი რიცხვები $P_i, Q_i, R_i$ და $U_i$ შემდეგი თანაფარდობებით: $P_i = P_{i-1} + e_{i-1} - a_{i-1} + 1$ , $Q_i = Q_{i-1} + f_{i-1} - b_{i-1} + 1$ , $R_i = R_{i-1} + g_{i-1} - c_{i-1} + 1$ , და $U_i = U_{i-1} + h_{i-1} - d_{i-1} + 1$ , სადაც $\alpha \in N$ და იცვლება ერთიდან ზემოთ მანამ, სანამ თითოეული რიცხვი არ გახდება მარტივი.

განხილული მაგალითის შემთხვევაში, როცა $i = 1$, მიიღება: $P_1 = 2 + 3 - 9 + 1 = 2 + 1$ , როცა $\alpha = 3$, მაშინ $P_1 = 2$ და ეს რიცხვი მარტივია; $Q_1 = 1 + 9 - 3 + 1 = 1 + 1$ , როცა $\alpha = 3$, მაშინ $Q_1 = 2$ და ეს რიცხვი მარტივია; $R_1 = 1 + 3 - 9 + 1 = 1 + 1$ , როცა $\alpha = 3$, მაშინ $R_1 = 1$ და ეს რიცხვი მარტივია; $U_1 = 1 + 9 - 7 + +1 = 1 + 1$ , როცა $\alpha = 3$, მაშინ $U_1 = 1$ და ეს რიცხვი მარტივია.

6) გამოითვლება $N_1 = P_1 \cdot Q_1 \cdot R_1 \cdot U_1$ და $\varphi_1(N_1) = (P_1 - 1) \cdot (Q_1 - 1) \cdot (R_1 - 1) \cdot (U_1 - 1)$.

ამ ექვსი პუნქტის შესრულების შედეგად მიიღება $N_1, \varphi_1(N_1), P_1, Q_1, R_1, U_1, K_1, T_1$ და $S_1$ მნიშვნელობები.

7) ზემოთ აღწერილი პროცედურების კიდევ სამჯერ გამეორებით (წინა ციკლში გამოთვლილი $P, Q, R$ და $U$ წარმოადგენს შემდეგი ციკლის საწყის მონაცემებს) მიიღება $N_2, N_3, N_4, \varphi_2(N_2), \varphi_3(N_3), \varphi_4(N_4), P_2, P_3, P_4, Q_2, Q_3, Q_4, R_2, R_3, R_4, U_2, U_3$ და $U_4$ მნიშვნელობები.

თუ საიდუმლო გასაღების ფორმირება ხდება სიმეტრიული კრიპტოსისტემისათვის, მაშინ $N, \varphi(N), P, Q, R$ და $U$ შედეგების მიხედვით გამოითვლება ერთსახელა პარამეტრებისათვის როგორც ორ-ორი და სამ-სამი, ისე ოთხივე წევრის ნამრავლები და ჯამები (თითოეულისათვის მიიღება 2 შედეგი, ხოლო ყველასთვის $2 \cdot 6 = 12$ . სტატიაში სრულად ნაჩვენებია $N_1, N_2, N_3$ და $N_4$ -ით მიღებული ყველა შედეგი, ხოლო დანარჩენები შემოკლებით). ასევე გამოითვლება ყოველ ციკლში შერჩეული ოთხივე მარტივი რიცხვის ჯამი და საბოლოოდ მიღებული 1 მონაცემი განლაგდება ერთმანეთის გვერდით და თითოეულს მიენიჭება რიგითობის მიხედვით ათობითი ნომერი.

$$1 - N_1, 2 - N_2, 3 - N_3, 4 - N_4, 5 - N_1 \cdot N_2, 6 - N_1 \cdot N_3, 7 - N_1 \cdot N_4, 8 - N_2 \cdot N_3, 9 - N_2 \cdot N_4, 10 - N_3 \cdot N_4,$$
$$11 - N_1 + N_2, 12 - N_1 + N_3, 13 - N_1 + N_4, 14 - N_2 + N_3, 15 - N_2 + N_4, 16 - N_3 + N_4, 17 - N_1 \cdot N_2 \cdot N_3,$$
$$18 - N_1 \cdot N_2 \cdot N_4, 19 - N_1 \cdot N_3 \cdot N_4, 20 - N_2 \cdot N_3 \cdot N_4, 21 - N_1 \cdot N_2 \cdot N_3 \cdot N_4, 22 - N_1 + N_2 + N_3,$$
$$23 - N_1 + N_2 + N_4, 24 - N_1 + N_3 + N_4, 25 - N_2 + N_3 + N_4, 26 - N_1 + N_2 + N_3 + N_4, 27 - \varphi_1, \dots$$
$$28 - \varphi_1 + \varphi_2 + \varphi_3 + \varphi_4, 29 - P_1, \dots 30 - P_1 + P_2 + P_3 + P_4, 31 - Q_1, \dots 32 - Q_1 + Q_2 + Q_3 + Q_4,$$
$$33 - R_1, \dots 34 - R_1 + R_2 + R_3 + R_4, 35 - U_1, \dots 36 - U_1 + U_2 + U_3 + U_4.$$
$$37 - P_1 + Q_1 + R_1 + U_1, 38 - P_2 + Q_2 + R_2 + U_2, 39 - P_3 + Q_3 + R_3 + U_3, 40 - P_4 + Q_4 + R_4 + U_4.$$

ეს 1 მონაცემი აიღება ორჯერ და 3 მონაცემი გაერთიანდება ერთ სტრიქონში მათი რიგითი ნომრების შემთხვევითი გადანაწილების მიხედვით. ამასთან, ერთთანრიგა რიგით ნომერს წინ ემატება ორი ნული, ხოლო ორთანრიგას კი ერთი ნული. რიგითი ნომრების ასეთ გადანაწილებას უზრუნველყოფს შემდეგი პროცედურები:

ა) შესრულდება $N_1, N_2, N_3$ და $N_4$ რიცხვების ბოლო ოთხ-ოთხი ციფრით გამოსახული ათობითი რიცხვების წარმოდგენა ორობითი სისტემით;

ბ) მიღებული ოთხი ორობითი კომბინაციიდან აიღება ექვს-ექვსი ორობითი ბიტი მარცხნიდან მარჯვნივ და მიიღება ოთხი ორობითი კომბინაცია: $G_1, G_2, G_3$ და $G_4$;

გ) $G_1, G_2, G_3$ და $G_4$ ორობითი კომბინაციების ათობითი სისტემით წარმოდგენის შედეგად მიიღება $G'_1, G'_2, G'_3$ და $G'_4$ ათობითი რიცხვები;

დ) 3 მონაცემის რიგითი ნომრები გადანაწილდება ხუთ 8x8 მატრიცაში (მატრიცა №0, №1, №2, №3 და №4). თითოეული მატრიცა წარმოადგენს ე.წ. *ჭადრაკის დაფას* (ნახ.1), რომელიც დანომრილია მასზე მხედრის მოძრაობის ჩაკეტილი მარშრუტის მიხედვით (მხედარი შემოივლის დაფის ყველა უჯრას და, ამასთან, იგი თითოეულ უჯრაზე მხოლოდ ერთხელ მოხვდება). მატრიცები განლაგდება ერთმანეთის გვერდით მარცხნიდან მარჯვნივ რიგითი ნომრების წრიული გადაადგილებით. განაპირა მარცხენა მატრიცის ნომერს განსაზღვრავს $G'_1(m$ ) – ის მნიშვნელობა (მაგალითად, თუ $G'_1(m$ ) = 3, მაშინ მატრიცების განლაგებას მარცხნიდან მარჯვნივ ექნება შემდეგი სახე №3, №4, №0, №1, და №2). $G'_2((m$ ) – ის მნიშვნელობით განისაზღვრება №0, №1, №2, №3 და №4 მატრიცების იმ საწყისი უჯრის ნომერი, რომელშიც უნდა განთავსდეს შესაბამისად რიცხვები 0 1, 0 , 1 , 1 და 2 . რიცხვები 0 2, 06 , 1 , 1 და 2 განთავსდება იმავე მატრიცებში საწყის ნომერზე ერთით მეტი ან ერთით ნაკლები ნომრის მქონე უჯრაში ( $G'_3$ რიცხვის ლუწობისას განთავსება ხდება ნომრის მატებით, ხოლო კენტობის შემთხვევაში კი ნომრის კლებით).

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 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

მაგალითად, თუ $G'_2((m$ ) = 3 და $G'_3$ რიცხვი კენტია, მაშინ №0 მატრიცის 3 -ე უჯრაში ჩაიწერება რიცხვი 0 , 3 -ში 0 , 3 -ში 0 და და ა.შ. 1 -ში 0 , 6 -ში 0 , 6 -ში 0 და ა.შ. 3 -ში 06 .

№1 მატრიცისათვის მითითებულ უჯრებში შესაბამისად ჩაიწერება: 0 , 0 , 0 ... 0 , 0 ... 1 .

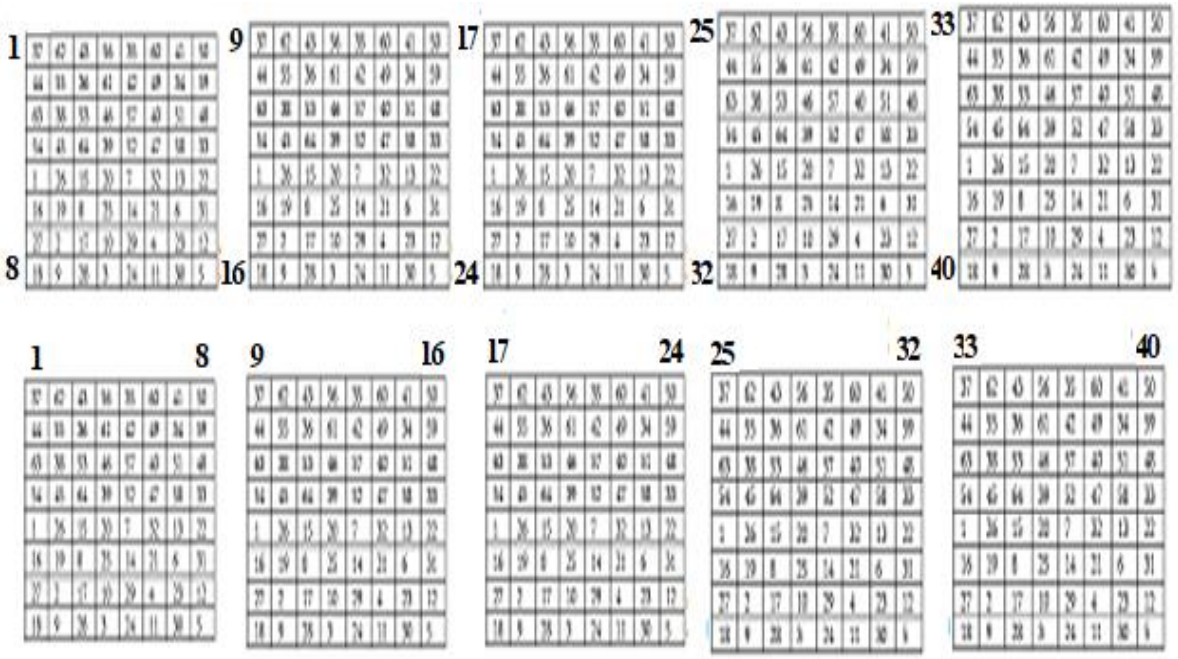
№2 მატრიცისათვის - 1 , 1 , 1 ... 1 , 1 , 1 ... 1 .

№3 მატრიცისათვის - 1 , 1 , 1 ... 2 , 2 , 2 ... 2 .

№4 მატრიცისათვის - 2 , 2 , 2 ... 2 , 2 , 2 ... 3 .

$G'_3$ რიცხვის ლუწობისას 3 უჯრის შემდეგ იქნება: 3 , 3 ..... 6 , 1, 2, .... 3 .

ყველა მატრიცის შევსების შემდეგ შესრულდება მათში ჩაწერილი რიცხვების მიმდევრობის წაკითხვა მარცხნიდან მარჯვნივ სტრიქონების ან სვეტების მიხედვით ($G'_4$ რიცხვის ლუწობისას წაკითხვა ხდება სტრიქონებით, ხოლო კენტობის შემთხვევაში კი სვეტებით) (ნახ.2);




ნახ.2

ე) წაკითხვის შედეგად მიღებულ რიცხვების მიმდევრობაში თითოეული რიცხვი შეიცვლება იმ მონაცემის შესაბამისი ათობითი რიცხვით, რომლის რიგით ნომერსაც წარმოადგენს ეს რიცხვი;

ვ) საბოლოოდ მიღებული ათობითი ციფრების მიმდევრობა წარმოადგენს შემთხვევითი სიგრძისა და შემთხვევითი მნიშვნელობის მქონე საიდუმლო გასაღებს.

თუ გამოყენებული კრიპტოსისტემა ინფორმაციული მონაცემთა ბლოკის დასაშიფრად საჭიროებს გარკვეული რაოდენობის ორობით ბიტებში გამოსახულ საიდუმლო გასაღებს, მაშინ ათობითი ციფრების მიმდევრობაში თითოეული ათობითი ციფრი იცვლება ოთხთანრიგა ორობითი კომბინაციით, მიღებული ორობითი ბიტების მიმდევრობა დაიძვრება მარჯვნიდან მარცხნივ ერთი სიმბოლოთი და შემდეგ დაძრული კომბინაცია მარცხნიდან მარჯვნივ დაიყოფა საჭირო რაოდენობის ბიტების შემცველ ჯგუფებად. მიღებული თითოეული ჯგუფი წარმოადგენს დამოუკიდებელ საიდუმლო გასაღებს და ამიტომ სხვადასხვა ინფორმაციული ბლოკების დაშიფვრის განხორციელება შესაძლებელია სხვადასხვა გასაღებით.

თუ საიდუმლო გასაღების ფორმირება ხდება ასიმეტრიული კრიპტოსისტემისათვის, მაშინ:

1) $\mathbf{P_i}$, $\mathbf{Q_i}$, $\mathbf{R_i}$ და $\mathbf{U_i}$ მარტივი რიცხვები ჯგუფდება ორ-ორად $(\mathbf{P_i}, \mathbf{Q_i})$ და $(\mathbf{R_i}, \mathbf{U_i})$. თითოეული წყვილისთვის გამოითვლება ეილერის ფუნქციის მნიშვნელობა:

$$\varphi_i'(P_i, Q_i) = (P_i - 1)\,(Q_i - 1) \text{ და } \varphi_i''(R_i, U_i) = (R_i - 1)\,(U_i - 1).$$

2) $\mathbf{P_i}$, $\mathbf{Q_i}$, $\mathbf{R_i}$ და $\mathbf{U_i}$ მარტივი რიცხვების გამოყენებით ხდება დაშიფვრის ღია გასაღების მნიშვნელობების განსაზღვრა შემდეგი თანაფარდობების გამოყენებით:

$E'_i = P_i + 1$ , $E''_i = Q_i + 1$ , $E'''_i = R_i + 1$ , $E^{I}_i = U_i + 1$ , სადაც $\alpha \in N$ და იზრდება 1-დან ზემოთ მანამ, სანამ არ შესრულდება შემდეგი პირობები: თითოეული $E'_i, E''_i, E'''_i$ და $E^{I}_i$ მარტივია, უსგ $(E'_i, \varphi'_i) = 1$, უსგ $(E''_i, \varphi''_i) = 1$, უსგ $(E'''_i, \varphi'''_i) = 1$, უსგ $(E^{I}_i, \varphi^{I}_i) = 1$;

3) გამოითვლება შესაბამისი საიდუმლო $D_i$ გასაღების მნიშვნელობა შემდეგი თანაფარდობებიდან $E'_i \cdot D'_i \equiv 1(m \quad \varphi'_i)$, $E''_i \cdot D''_i \equiv 1(m \quad \varphi''_i)$, $E'''_i \cdot D'''_i \equiv 1(m \quad \varphi'''_i)$ და $E^{I}_i \cdot D^{I}_i \equiv 1(m \quad \varphi^{I}_i)$. ე.ი. მიიღება $D'_i, D''_i, D'''_i$ და $D^{I}_i$. ამასთან $N'_i = P_i \cdot Q_i$ და $N''_i = R_i \cdot U_i$.

4) მე-2 და მე-3 პუნქტებში მიღებული $(E_i, D_i)$ გასაღებების ოთხ წყვილში $(E'_i, D'_i)$, $(E''_i, D''_i)$, $(E'''_i, D'''_i)$, $(E^{I}_i, D^{I}_i)$ შემავალი როგორც ღია, ისე საიდუმლო გასაღების ახარისხებით კვადრატში დამატებით მიიღება ოთხი წყვილი (ე.ი. გასაღებების წყვილების რაოდენობა ერთ ციკლში გახდება 8, ხოლო ოთხ ციკლში კი 32). 1-ელ ცხრილში ნაჩვენებია $N, E, D$ მნიშვნელობები (თითოეული სტრიქონი შეესაბამება გასაღების ოთხ მნიშვნელობას.

ცხრ.1

| # | $N$ | $E, D$ |
|---|---|---|
| 1-4 | $N'_1 = P_1 \cdot Q_1$ | $(E'_1, D'_1), (E''_1, D''_1), (E'^2_1, D'^2_1), (E''^2_1, D''^2_1)$ |
| 5-8 | $N''_1 = R_1 \cdot U_1$ | $(E'_1, D''_1), (E^{I}_1, D^{I}_1), (E''^2_1, D''^2_1), (E^{I\,2}_1, D^{I\,2}_1)$ |
| 9-12 | $N'_2 = P_2 \cdot Q_2$ | $(E'_2, D'_2), (E''_2, D''_2), (E'^2_2, D'^2_2), (E''^2_2, D''^2_2)$ |
| 13-16 | $N''_2 = R_2 \cdot U_2$ | $(E''_2, D''_2), (E^{I}_2, D^{I}_2), (E''^2_2, D''^2_2), (E^{I\,2}_2, D^{I\,2}_2)$ |
| 17-20 | $N'_3 = P_3 \cdot Q_3$ | $(E'_3, D'_3), (E''_3, D''_3), (E'^2_3, D'^2_3), (E''^2_3, D''^2_3)$ |
| 21-24 | $N''_3 = R_3 \cdot U_3$ | $(E''_3, D''_3), (E^{I}_3, D^{I}_3), (E''^2_3, D''^2_3), (E^{I\,2}_3, D^{I\,2}_3)$ |
| 25-28 | $N'_4 = P_4 \cdot Q_4$ | $(E'_4, D'_4), (E''_4, D''_4), (E'^2_4, D'^2_4), (E''^2_4, D''^2_4)$ |
| 29-32 | $N''_4 = R_4 \cdot U_4$ | $(E''_4, D''_4), (E^{I}_4, D^{I}_4), (E''^2_4, D''^2_4), (E^{I\,2}_4, D^{I\,2}_4)$ |

ამ გასაღებების გამოყენება შესაძლებელია ასიმეტრიულ $R$ კრიპტოსისტემაში. ინფორმაციის გამგზავნი ახდენს გასაგზავნი ინფორმაციის გარკვეული სიგრძის მქონე $X$ ბლოკის დაშიფვრას ღია $E$ გასაღებით შემდეგი გამოსახულების მიხედვით $Y_i \equiv X_i^{E(m \quad (N))}(m \quad N)$. ინფორმაციის მიმღები ახდენს დაშიფრული $Y_i$ ინფორმაციული ბლოკის გაშიფვრას $X_i \equiv Y_i^{D(m \quad (N))}(m \quad )$ გამოსახულებით, სადაც $D$ საიდუმლო გასაღებია.

არსებულ ასიმეტრიულ კრიპტოსისტემებში ინფორმაციის გადამცემი შიფრავს ყველა ინფორმაციულ ბლოკს კავშირის ხაზით მიღებული ღია $E$ გასაღების და $N$ მოდულის მნიშვნელობების გამოყენებით, ამიტომ ამ მნიშვნელობების და დაშიფრული ინფორმაციის ხელში ჩაგდებით ბოროტგამზრახველს შეუძლია გამოითვალოს საიდუმლო $D$ გასაღების მნიშვნელობა და გაშიფროს დაშიფრული ინფორმაცია. შემუშავებული ალგორითმის მიხედვით კავშირის ხაზში როგორც ღია $E$ გასაღების, ისე $N$ მოდულის მნიშვნელობები

არ გადაიცემა და ამიტომ არაკანონიერი მომხმარებლის მიერ დაშიფრული ინფორმაციის გაშიფვრა შეუძლებელია.

შესაძლებელია დასაშიფრად საიდუმლო $D$ გასაღებების, ხოლო გასაშიფრად ღია $E$ გასაღებების გამოყენება. ასეთი პროცედურის ჩატარების შედეგად გასაღებების წყვილების რაოდენობა გახდება $6$ .

$A$ მომხმარებელი გამოთვლის შემთხვევით არჩეული $P_0, Q_0, R_0$ და $U_0$ მარტივი რიცხვების ნამრავლს $N_0 = P_0 \cdot Q_0 \cdot R_0 \cdot U_0$ და $B$ მომხმარებელთან გააგზავნის როგორც $N_0 + F$ –ის მნიშვნელობას, სადაც $F$ კორპორაციული ქსელის საინდეფიკაციო ნომერია, ისე დაშიფრულ ინფორმაციას. $B$ მომხმარებელი $N_0 + F$ ჯამს გამოაკლებს $F$-ს, $N_0$–დან აღადგენს $P_0, Q_0$,

$R_0$ , $U_0$ რიცხვებს ($P_0 \geq Q_0 \geq R_0 \geq U_0$) და შემუშავებული ალგორითმის მიხედვით თავდაპირველად დააფორმირებს საიდუმლო გასაღების მნიშვნელობას, ხოლო შემდეგ შეასრულებს დაშიფრული ინფორმაციის გაშიფვრას.

## 3. დასკვნა

შემუშავებულ ალგორითმს აქვს შემდეგი ღირსებები: ალგორითმის პროცედურებში მონაწილე ნებისმიერი პარამეტრის მნიშვნელობა უცნობია მომსახურე პერსონალისათვის; არ საჭიროებს კავშირის ხაზში დაშიფვრის პროცედურაში უშუალოდ მონაწილე არც ერთი პარამეტრის მნიშვნელობის გადაცემას; არაკანონიერ მომხმარებელს კორპორაციული ქსელის საინდეფიკაციო ნომრის ხელში ჩაგდებით შეუძლია ალგორითმის საწყისი მონაცემის (ოთხი დიდი მარტივი რიცხვის ნამრავლის) მოპოვება, მაგრამ ამ მონაცემით იგი ვერ შეძლებს გაშიფვრის საიდუმლო გასაღების გამოცნობას; კანონიერ მომხმარებლებს შორის კავშირის ყოველი ახალი სეანსის განხორციელებისას ფორმირდება საიდუმლო გასაღების ახალი მნიშვნელობა; ალგორითმი გამოირჩევა მაღალი კრიპტომედეგობით და სწრაფქმედებით.

## ლიტერატურა - References – Литература:

1. კუციავა ვ., კუციავა ა., გოგუა ქ., გოგოლაძე გ. (2016). ინფორმაციის დაშიფვრის სიმეტრიული კრიპტოგრაფიული სისტემებისათვის საიდუმლო გასაღების მაფორმირებელი ალგორითმი. სტუ-ს შრომ.კრებ., „მართვის ავტომატიზებული სისტემები”, №1 (21), თბ., გვ. 70-77

2. გოგოლაძე გ., კუციავა ვ., კუციავა ა. (2017). ასიმეტრიული კრიპტოგრაფიული RSA სისტემისათვის ღია და საიდუმლო გასაღებების წყვილის მაფორმირებელი ალგორითმი. სტუ-ს შრომ.კრებ., „მართვის ავტომატიზებული სისტემები”, №1 (23), თბ., გვ. 49-55

3. კუციავა ვ., კუციავა ა., კაცაძე გ., დიაკონიძე ქ. (2016). ინფორმაციის დაცვა კორპორაციულ ქსელებში. სტუ. გამომც. „ტექნიკური უნივერსიტეტი”. თბილისი.

# ALGORITHM FOR FORMATION OF PRIVATE KEYS FOR CRYPTOGRAPHIC SYSTEMS

Kutsiava Vasil, Kutsiana Ana, Koberidze Natalia

Georgian Technical University

**Summary**

The paper describes algorithm - formation of encoding (private) keys for asymmetric and asymmetric cryptographic systems used in corporate networks. Private key for symmetric system is formed by random length and random value, for asymmetric systems encoding and decoding private key is formed by random pairs. Besides, performing new cycle of procedures each time, gives different values of private keys. None of the authentic values relating to the parameters of private key are transmitted through the wire of corporate network. The value of private key is unknown for personnel assisting legal subscribers of corporate network. As a result, malefactor won't be able to get private key as a result of obtaining data transmitted through corporate network wire and blackmailing or bribing service personnel. Presented algorithm is characterized by high crypto durability and speed.

# АЛГОРИТМ ФОРМИРОВАНИЯ СЕКРЕТНЫХ КЛЮЧЕЙ ДЛЯ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

Куциава В.А., Куциава А.В., Коберидзе Н.А.

Грузинский Технический Университет

**Резюме**

Рассмотрен алгоритм формирования секретных ключей, применяемых в корпоративных сетях симметричных и ассиметричных криптографических системах. Для симметричных систем происходит формирование секретного ключа с случайным значением и случайной длиной, а для ассиметричных систем - формирование пар случайных ключей шифрования (открытый) и расшифрования (секретный). При этом, в каждом новом цикле формирования ключа получаются разные значения. В линиях связи корпоративной сети не передается действительное значение ни одного параметра, применяемого в процедурах формирования ключа. Значения формированных ключей законных абонентов корпоративной сети неизвестно обслуживающему персоналу. Исходя из этого, злоумышленник не сможет завладеть секретным ключом в случае захвата передаваемых данных на линиях связи корпоративной сети или путем шантажа и подкупа обслуживающего персонала. Предложенный алгоритм отличается высокой криптостойкостью и быстротой действия.