ასიმეტრიული კრიპტოგრაფიული RSA სისტემისთვის ღია და საიდუმლო გასაღებების წყვილის მაფორმირებელი ალგორითმი

გიორგი გოგოლაძე, ვასილ კუციავა, ანა კუციავა
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია ასიმეტრიული კრიპტოგრაფიული სისტემისთვის დაშიფვრისა (ღია) და გაშიფვრის (საიდუმლო) გასაღებების წყვილების მიმდევრობის მაფორმირებელი ალგორითმი. თითოეული წყვილი ფორმირდება კორპორაციული ქსელის კანონიერი მომხმარებლების მიერ პროგრამულად ალგორითმში მოყვანილი გარკვეული პროცედურების შესრულების შედეგად და ამასთან, გასაღებების კონკრეტული მნიშვნელობები უცნობია მომსახურე პერსონალისთვის. ბოროტგამზრახველი, კორპორაციული 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: ასიმეტრიული კრიპტოგრაფიული სისტემა. ღია გასაღები. საიდუმლო გასაღები. კრიპტომედეგობა. სწრაფქმედება.

1. შესავალი

კორპორაციულ ქსელებში ჩართულ კანონიერ მომხმარებლებს შორის გადაცემული ინფორმაციის კონფიდენციალობის უზრუნველსაყოფად გამოიყენება როგორც სიმეტრიული (მაგალითად: $\boldsymbol{DES}, \boldsymbol{IDEA}, \boldsymbol{AES}, \boldsymbol{RC2}, \boldsymbol{RC5}$ და სხვ.), ისე ასიმეტრიული ($\boldsymbol{RSA}$ კრიპტოსისტემა, ელ-გამალის დაშიფვრის სქემა და სხვ.) სისტემები. ასიმეტრიული კრიპტოგრაფიული სისტემა $\boldsymbol{RSA}$, რომელიც დამუშავებული იქნა 1977 წელს რონალდ რივესტის, ადი შამირის და ლეონარდ ადლემანის მიერ (კრიპტოსისტემის დასახელება მიღებული იქნა ავტორების გვარების პირველი ასოების გაერთიანების შედეგად), წარმოადგენს სისტემას ღია გასაღებით და იგი უზრუნველყოფს მონაცემთა დაცვის ისეთი მექანიზმების განხორციელებას, როგორიცაა დაშიფვრა, გაშიფვრა და ციფრული ხელმოწერა (აუტენტიფიკაცია).

$\boldsymbol{RSA}$ ალგორითმი მუშაობს შემდეგნაირად: აიღება საკმაოდ დიდი ორი მარტივი $\boldsymbol{P}$ და $\boldsymbol{Q}$ რიცხვი; გამოითვლება მათი ნამრავლი $\boldsymbol{N = P \cdot Q}$ ($\boldsymbol{N}$ -ს ეწოდება მოდული); შეირჩევა ისეთი $\boldsymbol{E}$ რიცხვი, რომელიც აკმაყოფილებს შემდეგ პირობებს: $\boldsymbol{1 < E < \varphi}$ და უსგ $\boldsymbol{(E, \varphi) = 1}$, სადაც $\boldsymbol{\varphi}$ ეილერის ფუნქციაა და $\boldsymbol{\varphi = (P - 1) \cdot (Q - 1);}$ გამოითვლება $\boldsymbol{D}$ რიცხვი შემდეგი პირობით

$\boldsymbol{(E \cdot D) mod \varphi(N) = 1}$.

ინფორმაციის გამგზავნს დაუცველი კავშირის ხაზით გადაეცემა ღია გასაღები $\boldsymbol{(N, E)}$ გასაგზავნი ინფორმაციის დასაშიფრად; ინფორმაციის მიმღები ახდენს დაშიფრული ინფორმაციის გაშიფვრას საიდუმლო $\boldsymbol{(N, D)}$ გასაღებით.

ალგორითმიდან ჩანს, რომ ბოროტგამზრახველის მიერ ღია გასაღების ხელში ჩაგდებისას მას შეუძლია N რიცხვის ფაქტორიზაციის შედეგად დაეუფლოს საიდუმლო (N, D) გასაღებს და გაშიფროს მოპოვებული დაშიფრული ინფორმაცია. ამიტომ RSA კრიპტოსისტემის კრიპტომედეგობის უზრუნველსაყოფად აუცილებელია ერთმანეთისგან საგრძნობლად განსხვავებული და ერთი და იმავე სიგრძის (არანაკლებ 512 ბიტი) ორი დიდი მარტივი რიცხვის გამოყენება, მაგრამ დიდი რიცხვების შემთხვევაში საგრძნობლად რთულდება დაშიფვრისა და გაშიფვრის პროცედურები.

ზემოაღნიშნულიდან გამომდინარე მიზანშეწონილად ჩავთვალეთ კორპორაციულ ქსელებში გადაცემული ინფორმაციის კონფიდენციალობის შესანარჩუნებლად ისეთი ასიმეტრიული კრიპტოსისტემის დამუშავება, რომელიც არ საჭიროებს კავშირის ხაზში დაშიფვრის პროცედურაში უშუალოდ მონაწილე არც ერთი პარამეტრის მნიშვნელობის გადაცემას. ამასთან, უნდა იქნეს გამორიცხული მომსახურე პერსონალის წვდომა დაშიფვრისა და გაშიფვრის გასაღებების მნიშვნელობებთან. არსებულ ასიმეტრიულ სისტემებისგან განსხვავებით დაშიფვრისა და გაშიფვრის პროცედურები უნდა განხორციელდეს შედარებით მცირე დროში. ალგორითმი უნდა გამოირჩეოდეს როგორც მაღალი კრიპტომედეგობით, ისე სწრაფქმედებით.

2. ძირითადი ნაწილი

RSA კრიპტოსისტემის გასაღებების მაფორმირებელი ალგორითმი

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

P_0, Q_0 და R_0 რიცხვების მნიშვნელობებით A მომხმარებელი ახდენს დაშიფვრისა და გაშიფვრის გასაღებების წყვილების მიღებას შემდეგი ალგორითმით:

1. გამოითვლება $\varphi_{i-1}(N_{i-1}) = (P_{i-1} - 1) \cdot (Q_{i-1} - 1) \cdot (R_{i-1} - 1)$.
2. განისაზღვრება P_{i-1}, Q_{i-1} და R_{i-1} რიცხვების ერთეულოვან თანრიგში მოთავსებული a_{i-1}, b_{i-1} და c_{i-1} ციფრებისაგან შედგენილი $(a_{i-1}, b_{i-1}, c_{i-1})$ წყვილი. ცხადია, რომ $a_{i-1} \in \{1, 3, 7, 9\}$, $b_{i-1} \in \{1, 3, 7, 9\}$ და $c_{i-1} \in \{1, 3, 7, 9\}$
3. გამოითვლება $K_{i-1} = \varphi_{i-1}(N_{i-1}) mod 10$, $T_{i-1} = \varphi_{i-1}(N_{i-1}) mod 15$ და $S_{i-1} = \varphi_{i-1}(N_{i-1}) mod 3$ მნიშვნელობები, სადაც K_{i-1}, T_{i-1} და S_{i-1} არაუარყოფითი მთელი რიცხვებია. რადგან ეილერის $\varphi_{i-1}(N_{i-1})$ ფუნქციის 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;14]** შუალედიდან, ხოლო S_{i-1} კი **0, 1** და **2** მნიშვნელობებიდან ერთ-ერთს.
4. ერთმანეთისგან განსხვავებული **15×5** განზომილების მქონე სამი მატრიცისა და მე-3 პუნქტში გამოთვლილი K_{i-1}, T_{i-1} და S_{i-1} მნიშვნელობების გამოყენებით განისაზღვრება მარტივი რიცხვების დაბოლოებების ახალი $(d_{i-1}, e_{i-1}, f_{i-1})$ წყვილი (სტატიაში ნაჩვენებია ორი მატრიცა, პირველი სრულად, ხოლო მეორე ნაწილობრივ).

თითოეული მატრიცა შეიცავს მარტივ რიცხვთა დაბოლოებების **75** ვარიანტს (64 განსხვავებული და 11 გამეორება ამ 64 –დან) განაწილებულს თანაბრად 5 სვეტსა და 15 სტრიქონში. 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 K_{i-1} მნიშვნელობებით.

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	9,9,1	7,7,1
T = 6	3,1,3	3,9,9	7,3,9	1,1,3	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	1,3,1	9,7,1	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	7,7,9	9,1,9	1,9,9
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	3,1,1	9,3,3	7,7,3
T = 14	3,3,1	3,9,7	9,1,7	9,7,1	1,3,9

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

მაგალითად, თუ $N_0 = 83964153$, $P_0 = 673$, $Q_0 = 457$, $R_0 = 273$, (a_0, b_0, c_0)-(3,7,3). როცა $i = 1$, მაშინ $\varphi_0(N_0) = 672 \cdot 456 \cdot 272 = 83349504$, $K_0 = 83349504(mod10) = 4$, $T_0 = 83349504(mod15) = 9$, $S_0 = 83349504(mod3) = 0$.

ე.ი. შეირჩევა პირველი მატრიცის მე-3 სვეტსა და მე-10 სტრიქონში მოთავსებული (d_0, e_0, f_0) წყვილი, რომელიც არის (9,7,1).

თუ $N_0 = 134460959$, $P_0 = 617$, $Q_0 = 569$, $R_0 = 383$, (a_0, b_0, c_0)-(7,9,3).

როცა $i = 1$, მაშინ

$$\varphi_0(N_0) = 616 \cdot 568 \cdot 382 = 133657216, \quad K_0 = 133657216(mod10) = 6,$$
$$T_0 = 8133657216(mod15) = 1, \quad S_0 = 133657216(mod3) = 1.$$

ე.ი. შეირჩევა მეორე მატრიცის მე-4 სვეტსა და მე-2 სტრიქონში მოთავსებული (d_0, e_0, f_0) წყვილი, რომელიც არის (3,9,1).

5. განისაზღვრება ახალი მარტივი რიცხვები $\mathbf{P_i}$, $\mathbf{Q_i}$ და $\mathbf{R_i}$ შემდეგი თანაფარდობებით: $\mathbf{P_i = P_{i-1} + d_{i-1} - a_{i-1} + 10\alpha}$, $\mathbf{Q_i = Q_{i-1} + e_{i-1} - b_{i-1} + 10\alpha}$ და $\mathbf{R_i = R_{i-1} + f_{i-1} - c_{i-1} + +10\alpha}$, სადაც $\boldsymbol{\alpha \in N}$ და იცვლება ერთიდან ზემოთ მანამ, სანამ თითოეული რიცხვი არ გახდება მარტივი. განხილული პირველი მაგალითის შემთხვევაში, როცა $\mathbf{i = 1}$, , მიიღება: $\mathbf{P_1 = P_0 + +d_0 - a_0 + 10\alpha = 673 + 9 - 3 + 10\alpha = 679 + 10\alpha}$, როცა $\boldsymbol{\alpha}$=4, მაშინ $\mathbf{P_1 = 719}$ და ეს რიცხვი მარტივია; $\mathbf{Q_1 = Q_0 + e_0 - b_0 + 10\alpha = 457 + 7 - 7 + 10\alpha = 457 + 10\alpha}$, როცა $\boldsymbol{\alpha}$=1, მაშინ $\mathbf{Q_1}$ =467 და ეს რიცხვი მარტივია; $\mathbf{R_1 = R_0 + f_0 - c_0 + 10\alpha = 253 + 1 - 3 + 10\alpha = 251 + +10\alpha}$, როცა $\boldsymbol{\alpha}$ =2, მაშინ $\mathbf{R_1 = 271}$ და ეს რიცხვი მარტივია.

მეორე მაგალითის შემთხვევაში, როცა $\mathbf{i = 1}$, მიიღება: $\mathbf{P_1 = 617 + 3 - 7 + 10\alpha = 613 + +10\alpha}$, როცა $\boldsymbol{\alpha}$=3, მაშინ $\mathbf{P_1 = 643}$ და ეს რიცხვი მარტივია; $\mathbf{Q_1 = 569 + 9 - 9 + 10\alpha = 569 + +10\alpha}$, როცა $\boldsymbol{\alpha}$=3, მაშინ $\mathbf{Q_1 = 599}$ და ეს რიცხვი მარტივია; $\mathbf{R_1 = 383 + 1 - 3 + 10\alpha = 381 + +10\alpha}$, როცა $\boldsymbol{\alpha}$=2, მაშინ $\mathbf{R_1 = 401}$ და ეს რიცხვი მარტივია.

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

$$\boldsymbol{\varphi_i' = (P_i - 1) \cdot (Q_i - 1), \varphi_i'' = (P_i - 1) \cdot (R_i - 1), \varphi_i''' = (Q_i - 1).(R_i - 1).}$$

7. მე-6 პუნქტში მიღებული მნიშვნელობებით განისაზღვრება დაშიფვრის ღია გასაღებში შემავალი $\mathbf{E_i}$ შემდეგი თანაფარდობიდან $\boldsymbol{E_i' = P_i - 10\alpha}$, $\boldsymbol{E_i'' = R_i - 10\alpha}$, $\boldsymbol{E_i''' = Q_i - 10\alpha}$, სადაც $\boldsymbol{\alpha \in N}$ და იცვლება ერთიდან ზემოთ მანამ, სანამ არ შესრულდება შემდეგი პირობები: თითოეული $\boldsymbol{E_i', E_i''}$ და $\boldsymbol{E_i'''}$ მარტივია, უსგ $\boldsymbol{(E_i', \varphi_i') = 1}$, უსგ $\boldsymbol{(E_i'', \varphi_i'') = 1}$, უსგ $\boldsymbol{(E_i''', \varphi_i''') = 1}$.

8. გამოითვლება შესაბამის საიდუმლო გასაღებში შემავალი $\boldsymbol{D_i}$ –ის მნიშვნელობა შემდეგი თანაფარდობიდან $\boldsymbol{E_i' \cdot D_i' \equiv 1 (mod\ \varphi_i')}$, $\boldsymbol{E_i'' \cdot D_i'' \equiv 1 (mod\ \varphi_i'')}$, $\boldsymbol{E_i''' \cdot D_i''' \equiv 1 (mod\ \varphi_i''')}$. ე.ი. მიიღება $\boldsymbol{D_i', D_i''}$ და $\boldsymbol{D_i'''}$.

9. მე-7 და მე-8 პუნქტებში მიღებულ $\boldsymbol{(E_i, D_i)}$ სამ წყვილში $\boldsymbol{(E_i', D_i')}$, $\boldsymbol{(E_i'', D_i'')}$, $\boldsymbol{(E_i''', D_i''')}$ შემავალი სიდიდეების ახარისხებით კვადრატში, კუბში და მე-4 ხარისხში დამატებით მიიღება კიდევ ცხრა წყვილი (ე.ი. წყვილების რაოდენობა გახდება თორმეტი).

10. გამოითვლება $\mathbf{N_i = P_i \cdot Q_i \cdot R_i}$.

11. ეს ათი პუნქტი გამეორდება კიდევ ორჯერ $\mathbf{i = 2}$ და $\mathbf{i = 3}$ მნიშვნელობებისათვის. ამასთან, ყოველი შემდეგი ციკლის საწყის პარამეტრებს წარმოადგენენ წინა ციკლში მიღებული $\boldsymbol{P}$, $\boldsymbol{Q}$ და $\boldsymbol{R}$ მნიშვნელობები.

მე-11 პუნქტის შესრულების შემდეგ მიღებული $\boldsymbol{(E_i, D_i)}$წყვილების რაოდენობა გახდება **36** (ერთ ციკლში **12**, ხოლო სამ ციკლში **3·12=36**). ამ წყვილების გამოყენებით შესაძლებელია ***RSA*** კრიპტოსისტემის **36** გასაღების ფორმირება. პირველ ცხრილში ნაჩვენებია $\boldsymbol{N, \varphi, E, D}$ მნიშვნელობები (თითოეული სტრიქონი მოიცავს გასაღებების ოთხ წყვილს).

RSA კრიპტოსისტემაში ინფორმაციის გამგზავნი (ჩვენ შემთხვევაში $\boldsymbol{A}$ მომხმარებელი) ახდენს გასაგზავნი ინფორმაციის გარკვეული სიგრძის მქონე $\boldsymbol{X_i}$ბლოკის დაშიფვრას $\boldsymbol{(N, E)}$ გასაღებით შემდეგი გამოსახულების მიხედვით $\boldsymbol{Y_i \equiv X_i^{E(mod\varphi(N))} (mod\ N)}$.

ინფორმაციის მიმღები (ჩვენ შემთხვევაში $\boldsymbol{B}$ მომხმარებელი) ახდენს დაშიფრული $\boldsymbol{Y_i}$ ინფორმაციული ბლოკის გაშიფვრას $(\boldsymbol{N, D})$ გასაღების გამოყენებით შემდეგი გამოსახულების მიხედვით

$$\boldsymbol{X_i \equiv Y_i^{D(mod\varphi(N))}(modN)}.$$

ამ ალგორითმის გამოყენებით შესაძლებელია ინფორმაციული ბლოკების მიმდევრობაში შემავალი თითოეული ბლოკის დასაშიფრად და დაშიფრული ბლოკის გასაშიფრად კონკრეტული $(\boldsymbol{N, E})$ და $(\boldsymbol{N, D})$ გასაღებების გამოყენება. გამოსაყენებელი გასაღებების წყვილების შემთხვევითი არჩევა ხდება მეორე ცხრილის მიხედვით.

ცხრ.1

№	$\boldsymbol{N}$	$\boldsymbol{\varphi}$	$\boldsymbol{E, D}$
1-4	$\boldsymbol{N_1' = P_1 \cdot Q_1}$	$\boldsymbol{\varphi_1' = (P_1 - 1) \cdot (Q_1 - 1)}$	$(\boldsymbol{E_1', D_1'}), (\boldsymbol{E_1'', D_1''}), (\boldsymbol{E_1''', D_1'''}), (\boldsymbol{E_1'''', D_1''''})$
5-8	$\boldsymbol{N_2' = P_1 \cdot R_1}$	$\boldsymbol{\varphi_2' = (P_1 - 1) \cdot (R_1 - 1)}$	$(\boldsymbol{E_2', D_2'}), (\boldsymbol{E_2'', D_2''}), (\boldsymbol{E_2''', D_2'''}), (\boldsymbol{E_2'''', D_2''''})$
9-12	$\boldsymbol{N_3' = Q_1 \cdot R_1}$	$\boldsymbol{\varphi_3' = (Q_1 - 1) \cdot (R_1 - 1)}$	$(\boldsymbol{E_3', D_3'}), (\boldsymbol{E_3'', D_3''}), (\boldsymbol{E_3''' D_3'''}), (\boldsymbol{E_3'''', D_3''''})$
13-16	$\boldsymbol{N_4' = P_2 \cdot Q_2}$	$\boldsymbol{\varphi_4' = (P_2 - 1) \cdot (Q_2 - 1)}$	$(\boldsymbol{E_4', D_4'}), (\boldsymbol{E_4'', D_4''}), (\boldsymbol{E_4''', D_4'''}), (\boldsymbol{E_4'''', D_4''''})$
17-20	$\boldsymbol{N_5' = P_2 \cdot R_2}$	$\boldsymbol{\varphi_5' = (P_2 - 1) \cdot (R_2 - 1)}$	$(\boldsymbol{E_5', D_5'}), (\boldsymbol{E_5'', D_5''}), (\boldsymbol{E_5''', D_5'''}), (\boldsymbol{E_5'''', D_5''''})$
21-24	$\boldsymbol{N_6' = Q_2 \cdot R_2}$	$\boldsymbol{\varphi_6' = (Q_2 - 1) \cdot (R_2 - 1)}$	$(\boldsymbol{E_6', D_6'}), (\boldsymbol{E_6'', D_6''}), (\boldsymbol{E_6''' D_6'''}), (\boldsymbol{E_6'''', D_6''''})$
25-28	$\boldsymbol{N_7' = P_3 \cdot Q_3}$	$\boldsymbol{\varphi_7' = (P_3 - 1) \cdot (Q_3 - 1)}$	$(\boldsymbol{E_7', D_7'}), (\boldsymbol{E_7'', D_7''}), (\boldsymbol{E_7''', D_7'''}), (\boldsymbol{E_7'''', D_7''''})$
29-32	$\boldsymbol{N_8' = P_3 \cdot R_3}$	$\boldsymbol{\varphi_8' = (P_3 - 1) \cdot (R_3 - 1)}$	$(\boldsymbol{E_8', D_8'}), (\boldsymbol{E_8'', D_8''}), (\boldsymbol{E_8''', D_8'''}), (\boldsymbol{E_8'''', D_8''''})$
33-36	$\boldsymbol{N_9' = Q_3 \cdot R_3}$	$\boldsymbol{\varphi_9' = (Q_3 - 1) \cdot (R_3 - 1)}$	$(\boldsymbol{E_1', D_1'}), (\boldsymbol{E_1'', D_1''}), (\boldsymbol{E_1''', D_1'''}), (\boldsymbol{E_1'''', D_1''''})$

ცხრ.2

K	RSA კრიპტოსისტემის დაშიფვრისა და გაშიფვრის გასაღებების წყვილების თანმიმდევრობის არჩევის ვარიანტები
K=0	23, 1, 18, 14, 8, 33, 9, 30, 4, 34, 16, 28
K=0	5, 26, 10, 22, 32, 12, 29, 3, 31, 2, 11, 27
K=4	19, 11, 31, 24, 13, 34, 16, 6, 17, 26, 7, 20
K=6	4, 7, 36, 25, 17, 27, 2, 22, 5, 33, 9, 14
K=8	28, 20, 21, 3, 35, 15, 10, 1, 18, 5, 12, 13

ცხრილის თითოეულ სტრიქონში მოთავსებულია გასაღების **12** წყვილი მათი გამომსახველი ნომრების შემთხვევითი განაწილებით. გასაღებების თანმიმდევრობა შეიცავს **36** მონაცემს, ე.ი. სამ სტრიქონს. პირველი სტრიქონი აირჩევა $\boldsymbol{K_1}$ -ის, მეორე $\boldsymbol{K_2}$ --ის,, ხოლო მესამე $\boldsymbol{K_3}$ -ის მნიშვნელობის მიხედვით ($\boldsymbol{K}$ -ს მნიშვნელობიდან გამომდინარე შესაძლებელია მოხდეს სტრიქონების გამეორება). ამ **36** წყვილით შესაძლებელია **36** ინფორმაციული ბლოკის დაშიფვრისა და გაშიფვრის განხორციელება.

მაგალითად, თუ $\boldsymbol{K_1 = 0,}$ $\boldsymbol{K_2 = 2}$ და $\boldsymbol{K_3 = 6,}$ მაშინ დამშიფრავი (გამშიფრავი) გასაღებების მიმდევრობაში შემავალი წყვილებია: **23, 1, 18, 14, 8, 33, 9, 30, 4, 34, 16, 28, 5, 26, 10, 22, 32, 12, 29, 3, 31, 2, 11, 27, 4, 7, 36, 25, 17, 27, 2, 22, 5, 33, 9, 14.**

$(\boldsymbol{N}, \boldsymbol{E})$ ღია გასაღებების ამოწურვის შემდეგ დასაშიფრად გამოიყენება საიდუმლო $(\boldsymbol{N}, \boldsymbol{D})$ გასაღებები, ხოლო გასაშიფრად ღია $(\boldsymbol{N}, \boldsymbol{E})$ გასაღებები. აქედან გამომდინარე გასაღებების წყვილების საერთო რაოდენობა გახდება **72**.

ინფორმაციული ბლოკების დასაშიფრად გასაღებების სხვადასხვა წყვილების ერთობლივი გამოყენებისას დაშიფრული $\boldsymbol{Y_i}$ ბლოკის სიგრძე $\boldsymbol{N'_1 \cdots N'_9}$ მოდულებიდან უდიდესის სიგრძის ტოლია.

$\boldsymbol{A}$ მომხმარებელი გამოთვლის შემთხვევით არჩეული $\boldsymbol{P_0}$, $\boldsymbol{Q_0}$ და $\boldsymbol{R_0}$ მარტივი რიცხვების ნამრავლს $\boldsymbol{N_0 = P_0 \cdot Q_0 \cdot R_0}$ და **B** მომხმარებელთან გააგზავნის როგორც $\boldsymbol{N_0}$–ის მნიშვნელობას, ისე დაშიფრულ ინფორმაციას. $\boldsymbol{B}$ მომხმარებელი $\boldsymbol{N_0}$–დან აღადგენს $\boldsymbol{P_0}$, $\boldsymbol{Q_0}$ და $\boldsymbol{R_0}$ რიცხვებს $(\boldsymbol{P_0 \geq Q_0 \geq R_0})$ ჩვენს მიერ დამუშავებული ალგორითმის მიხედვით, რომლის პროგრამულ რეალიზაციას $\boldsymbol{C\#}$ ენაზე აქვს შემდეგი სახე:

```
   List<long> factors3(long n)
{
    var factors = new List<long>();

    for (var i = 3; n > 1; i+=2)
        for (; n % i == 0; n /= i)
            factors.Add(i);
    return factors;
}
```

აღდგენილი $\boldsymbol{P_0}$, $\boldsymbol{Q_0}$ და $\boldsymbol{R_0}$ რიცხვების მნიშვნელობებით $\boldsymbol{B}$ მომხმარებელი თავდაპირველად დააფორმირებს დაშიფვრისა და გაშიფვრის გასაღებების წყვილებს იმავე ალგორითმით, ხოლო შემდეგ შეასრულებს დაშიფრული ინფორმაციის გაშიფვრას.

3. დასკვნა

ჩვენ მიერ შემუშავებულ ალგორითმს აქვს შემდეგი ღირსებები: ალგორითმის პროცედურებში მონაწილე ნებისმიერი პარამეტრის მნიშვნელობა უცნობია მომსახურე პერსონალისთვის; არ საჭიროებს კავშირის ხაზში დაშიფვრის პროცედურაში უშუალოდ მონაწილე არც ერთი პარამეტრის მნიშვნელობის გადაცემას; კორპორაციული ქსელის არაკანონიერ მომხმარებელს შეუძლია ალგორითმის საწყისი მონაცემის (სამი დიდი მარტივი რიცხვის ნამრავლის) მოპოვება, მაგრამ ამ მონაცემით იგი ვერ შეძლებს გაშიფვრის საიდუმლო გასაღების გამოცნობას; დამშიფრავი გასაღები წარმოადგენს პროგრამულად გამოთვლილ შემთხვევით არჩეულ 36 მონაცემის მიმდევრობით გაერთიანებას; მე-11 პუნქტში ციკლების რაოდენობის გაზრდით შესაძლებელია გასაღებების წყვილების რაოდენობის გაზრდა ($\boldsymbol{i = 4}, \boldsymbol{i = 5}$ და ა.შ. ყოველი ახალი ციკლის შემდეგ ემატება გასაღებების **12** წყვილი); კანონიერ მომხმარებლებს შორის კავშირის ყოველი ახალი სეანსის განხორციელებისას ფორმირდება გასაღებების განსხვავებული წყვილები; ალგორითმი გამოირჩევა მაღალი კრიპტომედეგობით და სწრაფქმედებით.

ლიტერატურა - References – Литература:

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

2. კუციავა ვ., კუციავა ა., გოგუა ქ., გოგოლაძე გ. (2016). ინფორმაციის დაშიფვრის სიმეტრიული კრიპტოგრაფიული სისტემებისათვის საიდუმლო გასაღების მაფორმირებელი ალგორითმი. სტუ-ს შრ.კრ., „მართვის ავტომატიზებული სისტემები", N1 (21), გვ. 70-77.

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

ALGORITHM FOR FORMATION OF PAIRS OF PUBLIC AND PRIVATE KEYS FOR ASYMMERICAL CRYPTOGRAPHIC RSA SYSTEM

Giorge Gogoladze, Vasil Kusiava, Ana Kutsiava

Georgian Technical University

Summary

The paper describes algorithm for formation sequence of pairs of encoding (public) and decoding (private) keys for asymmetrical cryptographic RSA system. Each pair is formed as a result of performing specific procedures entailed automatically in the algorithm by the legal users of corporate network and at the same time key values are unknown by service personnel. 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 ПАР ОТКРЫТЫХ И ЗАКРЫТЫХ КЛЮЧЕЙ ДЛЯ АССИМЕТРИЧНОЙ КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ RSA

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

Грузинский Технический Университет

Резюме

Рассмотрен алгоритм формирования пар ключей шифрования (открытый) и расшифрования (секретный) для ассиметричной криптографической системы RSA. Каждая пара ключей формируется программно законным потребителем корпоративной сети после выполнения определенных процедур приведенных в алгоритме, причем, конкретные значения остаются неизвестными обслуживающему персоналу. Злоумышленник не сможет завладеть секретным ключом в случае захвата передаваемых данных на линиях связи корпоративной сети или путем шантажа и подкупа обслуживающего персонала. Предлогаемый алгоритм отличается высокой криптостойкостью и быстротой действия.