ცვლადპარამეტრებიანი დაშიფვრის RSA კრიპტოსისტემა

ვასილ კუციავა, გიორგი გოგოლაძე
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია კორპორაციულ ქსელში გადაცემული ინფორმაციის დაცვის ორგანიზება RSA კრიპტოსისტემის ისეთი ალგორითმით, რომელშიც დაშიფვრის და გაშიფვრის პროცედურების შესრულებისას გამოიყენება ცვლადი პარამეტრები, ამასთან კორპორაციული ქსელის კავშირის ხაზში არ გადაიცემა პროცედურებში მონაწილე არცერთი პარამეტრის ნამდვილი მნიშვნელობა და იდენტური ინფორმაციული სიმბოლოების დაშიფვრისას მიიღება შიფრტექსტი განსხვავებული გამოსახულებებით.

საკვანძო სიტყვები: RSA კრიპტოსისტემა. ღია გასაღები. საიდუმლო გასაღები. ეილერის ფუნქციის მნიშვნელობა. შიფრტექსტი. კრიპტომედეგობა.

1. შესავალი

ინფორმაციის დაცვის RSA კრიპტოსისტემის გამოყენებისას ინფორმაციის გამგზავნი ახდენს გასაგზავნი ინფორმაციის დაშიფვრას ინფორმაციის მიმღებისაგან მიღებული N და E რიცხვითი მნიშვნელობებით, სადაც N წარმოადგენს ორი დიდი მარტივი P და Q რიცხვების ნამრავლს, ხოლო E კი ინფორმაციული X_i ბლოკის დასაშიფრ ე.წ. ღია გასაღებს (1, 2). დაშიფვრის შედეგად მიიღება შიფრტექსტის Y_i ბლოკი:

$$Y_i \equiv X_i^E (mod\ N).$$

ინფორმაციის გაშიფვრისას ხდება X_i ბლოკის აღდგენა $X_i \equiv Y_i^E (\mathrm{mod} N)$ გამოსახულებით, სადაც D საიდუმლო გასაღებია და იგი წარმოადგენს E რიცხვის შებრუნებულს $\varphi(N)$ მოდულით ($\varphi(N)$ ეილერის ფუნქციის მნიშვნელობაა და $\varphi(N) = (p-1)(q-1)$).

RSA კრიპტოსისტემის კრიპტომედეგობის უზრუნველსაყოფად აუცილებელია ერთმანეთისაგან საგრძნობლად განსხვავებული და ერთი და იმავე სიგრძის (არანაკლებ 512 ბიტი) P და Q მარტივი რიცხვების გამოყენება. რადგან ასეთი დიდი რიცხვების შემთხვევაში საგრძნობლად რთულდება დაშიფვრისა და გაშიფვრის პროცედურები, ამიტომ მიზანშეწონილად ჩავთვალეთ კორპორაციული ქსელებისთვის ისეთი ალგორითმის შემუშავება, რომელიც მუშაობს გაცილებით პატარა რიცხვებზე და ამასთან გამოირჩევა მაღალი კრიპტომედეგობით.

2. ძირითადი ნაწილი

კორპორაციულ ქსელებში გადაცემული ინფორმაციის კონფიდენციალობის შესანარჩუნებლად შევიმუშავეთ RSA კრიპტოსისტემის ალგორითმი ცვლადი პარამეტრებით.

ინფორმაციის მიმღები აგზავნის ინფორმაციის გამგზავნთან ორი მარტივი P_0 და Q_0 რიცხვების (თითოეულის სიგრძე 8-16 ბიტი) ნამრავლს – $N_0 = P_0 \cdot Q_0$. ინფორმაციის გამგზავნი N_0-ის მარტივ მამრავლებად დაშლით აღადგენს P_0 და Q_0 რიცხვებს. ამ რიცხვების მნიშვნელობების ცოდნა უზრუნველყოფს ინფორმაციის მიმღები და გადამცემი მხარეების პარალელურ მუშაობას ერთი და იმავე ალგორითმით, კერძოდ:

1. გამოითვლება ეილერის ფუნქციის მნიშვნელობა $\varphi_{i-1}(N_{i-1}) = (P_{i-1}-1)\cdot(Q_{i-1}-1), i \in N$.
2. გამოითვლება: ა) $\varphi_{i-1}(N_{i-1}) mod 10$ და ბ) $\varphi_{i-1}(N_{i-1}) mod 15$ მნიშვნელობები.
3. განისაზღვრება P_{i-1} და Q_{i-1} რიცხვების ერთეულოვან თანრიგში განთავსებული a და b ციფრებისაგან შედგენილი (a, b) წყვილი. ცხადია, რომ $a \in \{1,3,7,9\}$ და $b \in \{1,3,7,9\}$.

4. ერთმანეთისაგან განსხვავებული თხუთმეტი მატრიცისა და მე-2 პუნქტში გამოთვლილი ა და ბ მნიშვნელობების გამოყენებით განისაზღვრება მარტივი რიცხვების დაბოლოებების ახალი (c,d) წყვილი.

თითოეული მატრიცა შეიცავს მარტივ რიცხვთა დაბოლოებების თექვსმეტი ვარიანტის {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} შედგენილ ხუთ განსხვავებულ ქვეჯგუფს (ქვეჯგუფების რაოდენობა 16!-ის ტოლია. ალგორითმში გამოყენებულია 75 ქვეჯგუფი). ეს მატრიცები ალგორითმის საიდუმლო გასაღებია და მათი შემადგენლობა ცნობილი უნდა იყოს მხოლოდ კორპორაციულ ქსელში ჩართული მომხმარებლებისთვის. ალგორითმის კრიპტომედეგობის გასაზრდელად მიზანშეწონილია ამ მატრიცების შემადგენლობის ცვლილება დროის გარკვეული პერიოდის გასვლის შემდეგ. რადგან ეილერის ფუნქციის მნიშვნელობა ლუწი რიცხვია, ამიტომ $\varphi_{i-1}(N_{i-1})\mathrm{mod}10$-ის გამოთვლით მიიღება 0,2,4,6 და 8 რიცხვებიდან ერთ-ერთი. ამ რიცხვებით ხდება თითოეულ მატრიცაში ქვეჯგუფის ნომრის განსაზღვრა $(0 \to 1,2 \to 2,4 \to 3,6 \to 4,8 \to 5)$. $\varphi_{i-1}(N_{i-1})\mathrm{mod}15$ გამოთვლისას შესაძლებელია მთელი რიცხვების მიღება 0-დან 14-ის ჩათვლით, ამიტომ ამ რიცხვით შეირჩევა შესაბამისი მატრიცა და ქვეჯგუფში სტრიქონის ნომერი (ნაშთის მნიშვნელობა განსაზღვრავს მატრიცის ნომერს და შერჩეულ ქვეჯგუფში სტრიქონის ნომერს). სტრიქონის შერჩევისას (a,b) წყვილის შესაბამისი კომბინაცია დროებით გადადის ქვეჯგუფის მე-15 სტრიქონში (შესრულდება ქვეჯგუფში (a,b) წყვილის ქვემოთ განთავსებული წყვილების ციკლური დაძვრა ქვემოდან ზემოთ) გამეორების გამოსარიცხად.

მაგალითად, ვთქვათ

$N_0 = 2881, N_0 = P_0 \cdot Q_0 = 67 \cdot 43,\ P_0 = 67, Q_0 = 43,$

$(a,b) \to (7,3),\ \varphi_0(N_0) = (P_0 - 1)(Q_0 - 1) = 66 \cdot 42 = 2772;$

$\varphi_0(N_0)\mathrm{mod}10 = 2772(\mathrm{mod}\ 10) \equiv 2; \varphi_0(N_0)\mathrm{mod}15 = 2772(\mathrm{mod}\ 15) \equiv 12.$

ე.ი. შეირჩევა მე-12 მატრიცის (ცხრ.1), მე-2 ქვეჯგუფის და მე-12 სტრიქონში (მე-13 სტრიქონი ხდება მე-12 სტრიქონი, რადგან მე-4 სტრიქონი გადადის ბოლოში) განთავსებული (c,d) წყვილი, რომელიც არის (9,7).

ცხრ.1

	1	2	3	4	5
0	3,1	1,3	9,9	9,1	1,7
1	7,9	7,9	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	9,1	9,7	9,9	1,3
13	7,3	9,7	1,3	7,7	3,7
14	3,9	3,7	9,1	3,3	7,1
15	7,7	7,1	3,3	3,1	9,7

5. განისაზღვრება ახალი მარტივი P_i და Q_i რიცხვები შემდეგი თანაფარდობებით: $P_i = P_{i-1} + c - a + 10\alpha$ და $Q_i = Q_{i-1} + d - b + 10\alpha$, 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; $Q_1 = Q_0 + d - b + 10\alpha = 43 + 7 - 3 + 10\alpha = 47 + 10\alpha$, როცა $\alpha = 2$, მაშინ $Q_1 = 67$ და ეს რიცხვი მარტივია.

6. გამოითვლება $N_i = P_i \cdot Q_i$ და $\varphi_i(N_i) = (P_i - 1)(Q_i - 1)$. განხილული მაგალითის შემთხვევაში $N_1 = P_1 \cdot Q_1 = 79 \cdot 67 = 5293$ და $\varphi_1(N_1) = (P_1 - 1)(Q_1 - 1) = 78 \cdot 66 = 5148$.

7. განისაზღვრება დაშიფვრის ღია E_i გასაღები შემდეგი თანაფარდობიდან $E_i = Q_i + 10\alpha$, სადაც $\alpha \in N$ და იზრდება 1-დან ზემოთ მანამ, სანამ არ შესრულდება შემდეგი პირობები: E_iმარტივია, $E_i < \varphi_i(N_i)$ და $უსგ(E_i, \varphi_i(N_i)) = 1$. განხილული მაგალითის შემთხვევაში: $E_1 = Q_1 + 10\alpha = 67 + 10\alpha$, როცა $\alpha = 3$, მაშინ $E_1 = 97$ და ეს რიცხვი მარტივია, ამასთან $97 < 5148$ და $უსგ(97, 5148) = 1$.

8. გამოითვლება საიდუმლო D_i გასაღების მნიშვნელობა შემდეგი თანაფარდობიდან:

$$E_i \cdot D_i \equiv 1 (mod \varphi_i(N_i)).$$

განხილული მაგალითის შემთხვევაში:

$$E_1 \cdot D_1 \equiv 1 (mod \varphi_1(N_1)), 97 \cdot D_1 \equiv 1 (mod 5148), D_1 = 4405.$$

9. ამ პუნქტების შესრულების შემდეგ ალგორითმით შესაძლებელია შემდეგი სამი გაგრძელებიდან ერთ-ერთის არჩევა:

I. მე-8 პუნქტში მიღებული E_i და D_i მნიშვნელობებისაგან ახალი E,D წყვილების მიღება და დასაშიფრი ინფორმაციის თითოეული X_i სიმბოლოს დაშიფვრა რიგრიგობით E_{i+t} გასაღებების გამოყენებით, ხოლო დაშიფრული Y_i-ს გაშიფვრა შესაბამისი D_{i+t} გასაღებებით. ამასთან, E გასაღებების ამოწურვის შემდეგ შესაძლებელია დასაშიფრად D გასაღებების გამოყენება, ხოლო გასაშიფრად E გასაღებების. ეს პუნქტი მეორდება ციკლურად მანამ, სანამ არ ამოიწურება გადასაცემი ინფორმაცია. ყოველი ახალი E,D წყვილის მიღება ხდება წინა წყვილის კვადრატში ახარისხებით (თუ E_i და D_i-ის აღვნიშნავთ, შესაბამისად, E_{i+t-1}დაD_{i+t-1}-ით, მაშინ $t \in N$-თვის $E_{i+t} \equiv E^2_{i+t-1} (mod \varphi_i(N_i))$ და $D_{i+t} \equiv D^2_{i+t-1} (mod \varphi_i(N_i))$ თანაფარდობების გამოყენებით მიიღება გასაღებების გარკვეული რაოდენობის წყვილები. ჩხადია, რომ $E_{i+t} < \varphi_i(N_i)$ და $D_{i+t} < \varphi_i(N_i)$). განხილული მაგალითის შემთხვევაში:

$E_2 \equiv E^2_1 (mod \varphi_1(N_1)), E_2 \equiv 97^2 (mod 5148), E_2 = 4261;$

$E_3 \equiv E^2_2 (mod \varphi_1(N_1)), E_3 \equiv 4261^2 (mod 5148), E_3 = 4273;$

$E_4 \equiv E^2_3 (mod \varphi_1(N_1)), E_4 \equiv 4273 (mod 5148), E_4 = 3721;$

$E_5 \equiv E^2_4 (mod \varphi_1(N_1)), E_5 \equiv 3721^2 (mod 5148), E_5 = 2869;$

$E_6 \equiv E^2_5 (mod \varphi_1(N_1)), E_6 \equiv 2869^2 (mod 5148), E_6 = 4657;$

და ა.შ. $E_{1+t} < \varphi_1(N_1)$ პირობის შესრულებამდე.

$D_2 \equiv D^2_1 (mod \varphi_1(N_1)), D_2 \equiv 4405^2 (mod 5148), D_2 = 1213;$

$D_3 \equiv E^2_2 (mod \varphi_1(N_1)), D_3 \equiv 1213^2 (mod 5148), D_3 = 4189;$

$D_4 \equiv E^2_3 (mod \varphi_1(N_1)), D_4 \equiv 4189^2 (mod 5148), D_4 = 3337;$

$D_5 \equiv E^2_4 (mod \varphi_1(N_1)), D_5 \equiv 3337^2 (mod 5148), D_5 = 445;$

$D_6 \equiv E^2_5 (mod \varphi_1(N_1)), D_6 \equiv 445^2 (mod 5148), D_6 = 2401;$

და ა.შ. $D_{1+t} < \varphi_1(N_1)$ პირობის შესრულებამდე.

II. $1 \div 8$ პუნქტების ციკლური გამეორებით შესაძლებელია N, E და D რიცხვების სამეულების რამდენიმე ვარიანტის მიღება (დაახლოებით ოცამდე) და X_i სიმბოლოების დასაშიფრად და Y_i-ის გასაშიფრად სხვადასხვა სამეულები გამოიყენება რიგრიგობით. ე.ი. თუ დასაშიფრი სიმბოლოების რაოდენობაა 20 და სამეულების რაოდენობაც 20-ის ტოლია, მაშინ თითოეული სიმბოლოს დაშიფვრა-გაშიფვრა სრულდება სხვადასხვა სამეულებით. თუ დასაშიფრი სიმბოლოების რაოდენობა აღემატება სამეულების რაოდენობას, მაშინ ხდება ციკლების გამეორება დასაშიფრი ინფორმაციის ამოწურვამდე. განხილული მაგალითის შემთხვევაში:

N_1=5293, E_1=97, D_1 = 4405 ;N_2=6887, E_2=101, D_2 = 2861 ;

N_3=10403, E_3=131, D_3 = 3971 ;N_4=16637, E_4=137, D_4 = 1913 ;

N_5=20567, E_5=151, D_5 = 17191 ;

N_6=28417, E_6=167, D_6 = 26903 და ა.შ. სასურველი რაოდენობის სამეულების მიღებამდე.

III.I და II გაგრძელებების გაერთიანება. ე.ი. დაშიფვრა მიმდინარეობს თითოეული გაგრძელების თითო ციკლის გამოყენებით (I გაგრძელების შემთხვევაში დაშიფვრა მიმდინარეობს მხოლოდ E გასაღებებით) და შემდეგ ხდება ორივე ციკლის ციკლური გამეორება გადასაცემი ინფორმაციის ამოწურვამდე.

ამ სამი გაგრძელებიდან ერთ-ერთის არჩევა ხდება მეორე პუნქტში გამოთვლილი $\varphi_0(N_0) \bmod 15$–ის მნიშვნელობების გაყოფით სამზე. რადგან ამ შემთხვევაში შესაძლებელია 0, 1 ან 2-ის ტოლი ნაშთის მნიშვნელობის მიღება, ამიტომ ექვსი ვარიანტიდან აირჩევა ერთ-ერთი. მაგალითად, 0-ის შემთხვევაში აირჩევა III, 1-ის შემთხვევაში II, ხოლო 2-ის შემთხვევაში I გაგრძელება. მაგალითად, როცა:

1) P_0 = 67,Q_0 = 43, N_0 = 2881, $\varphi_0(N_0) mod 15 = (2772) mod 15 = 12$, ნაშთი ტოლია 0-ის:

2) P_0 = 71, Q_0 = 59, N_0 = 4189, $\varphi_0(N_0) mod 15 = (4060) mod 15 = 10$, ნაშთი ტოლია 1-ის:

3) P_0 = 107, Q_0 = 3N_0 = 321, $\varphi_0(N_0) mod 15 = (212) mod 15 = 2$, ნაშთი ტოლია 2-ის:

თუ დასაშიფრი ღია ტექსტი შეიცავს ოცდაორ ერთნაირ სიმბოლოს, მაგალითად, kkkkkkkkkkkkkkkkkkkkkk, მაშინ დაშიფრულ ტექსტს მესამე გაგრძელების შემთხვევაში ექნება შემდეგი სახე (I გაგრძელებისთვის გამოთვლილია E და D გასაღებების მხოლოდ ექვსი წყვილი,ხოლო II გაგრძელებისთვის ხუთი N, E და D სამეული):

N_1=79 67=5293, E_1=97, E_2=4261, E_3=4273, E_4 = 3721 , E_5=2869, E_6 = 4657 , D_1 = 4405 , D_2 = 1213 , D_3 = 4189, D_4 = 3337, D_5 = 445, D_6 = 2401;

N_2=6887, E_{27}=101, D_{27} = 2861 ;N_3=10403, E_{38}=131, D_{38} = 3971 ;

N_4=16637, E_{49}=137, D_{49} = 1913 ;N_5=20567, $E_{5\,10}$=151, $D_{5\,10}$ = 17191 ;

N_6=28417, $E_{6\,11}$=167, $D_{6\,11}$ = 26903 .

4849 2878 2828 82 695 2610 1933 4248 14116 12296 19760;

4849 2878 2828 82 695 2610 1933 4248 14116 12296 19760.

შიფრტექსტიდან ნათლად ჩანს, რომ ერთმანეთის გვერდით მდებარე ერთნაირი სიმბოლოების დაშიფვრისას მიიღება განსხვავებული გამოსახულებები (რადგან ღია გასაღებების საერთო რაოდენობა ტოლია თერთმეტის, ამიტომ შიფრტექსტში მიიღება გამოსახულებების ორი იდენტური ჯგუფი).

3. დასკვნა

ტრადიციული ალგორითმისაგან განსხვავებით ჩვენ მიერ შემუშავებული ალგორითმი გამოირჩევა: 1) სწრაფქმედებით (მცირე რიცხვების გამოყენებით დაშიფვრისა და გაშიფვრის

პროცედურების შესრულება მოითხოვს გაცილებით მცირე დროს, ვიდრე 512 ბიტის სიგრძის მქონე რიცხვების გამოყენებისას); 2) კრიპტოგრაფიული მედეგობის უკეთესი მაჩვენებლით (კავშირის ხაზში არ გადაიცემა დაშიფვრისა და გაშიფვრის პროცედურებში მონაწილე არცერთი პარამეტრი; მატრიცების შემადგენლობა იცვლება დროის გარკვეული პერიოდის გასვლის შემდეგ; მეცხრე პუნქტის მიხედვით შესაძლებელია ალგორითმის შესრულების სამი გაგრძელებიდან ერთ-ერთის არჩევა; გაგრძელება I-ის შემთხვევაში შესაძლებელია დასაშიფრად E და D გასაღებების, ხოლო გასაშიფრად შესაბამისად D და E გასაღებების მორიგეობით გამოყენება; გაგრძელება II-ის შემთხვევაში შესაძლებელია ერთ ციკლში სხვადასხვა რაოდენობის N, E და D სამეულების გამოყენება; ერთმანეთის გვერდით განთავსებული იდენტური ინფორმაციული სიმბოლოების დაშიფვრისას მიიღება შიფრტექსტი განსხვავებული გამოსახულებებით).

ლიტერატურა:

1. Соколов А. Б., МаньгинВ.Ф. Защита информации в распределенных корпоративных системах. М., ДМК Процесс. 2002
2. კუციავა ვ., კაცაძე გ., დიაკონიძე ქ. ინფორმაციის დაცვა. სტუ. თბ., 2005.

VARIABLE PARAMETERS ENCODING RSA CRYPTOSYSTEM

Kutsiava Vasili, Gogoladze Georgi
Georgian Technical University

Summary

The paper presents protection of information which is transmitted to the corporate network, using by algorithm of RSA cryptosystem which uses during the performance of encoding and decoding procedures. At the same time none of the valid values are transferred in the corporate network chain and different depictions of cipher text are obtained during the encoding of identical information symbols..

КРИПТОСИСТЕМА ШИФРОВАНИЯ RSA С ПЕРЕМЕННЫМИ ПАРАМЕТРАМИ

Куциава В.А., Гоголадзе Г.Н.

Грузинский Технический Университет

Резюме

Рассмотрена организация защиты переданной информации в корпоративных сетях таким алгоритмом криптосистемы RSA, в котором для выполнения процедур шифрования и расшифрования используются переменные параметры. При этом в линии связи корпоративной сети не передаются действительные значения ни одного применяемого параметра и после шифрования открытого текста с идентичнимы символами получается шифртекст, состояший из различных символов.