საქართველოს ტექნიკური უნივერსიტეტი

ხელნაწერის უფლებით

გიორგი გოგოლაძე

მონაცემთა დაშიფვრის არასტანდარტული სიმეტრიული კრიპტოგრაფიული ალგორითმი პროგრამული უზრუნველყოფით

სადოქტორო პროგრამა: მართვის სისტემები, ავტომატიზაცია და ტესტინჟინერინგი

შიფრი: 0403

დოქტორის აკადემიური ხარისხის მოსაპოვებლად

წარდგენილი დისერტაციის

ა ვ ტ ო რ ე ფ ე რ ა ტ ი

თბილისი

2018 წელი

სამუშაო შესრულებულია საქართველოს ტექნიკური უნივერსიტეტში

ინფორმატიკისა და მართვის სისტემების ფაკულტეტი

მართვის სისტემების დეპარტამენტი

ხელმძღვანელი: ასოც. პროფესორი ვ. კუცავა

რეცენზენტები: ----------

დაცვა შედგება ---------- წლის ”------” ----------, --------- საათზე

საქართველოს ტექნიკური უნივერსიტეტის ----------

---------- საუნივერსიტეტო სადისერტაციო საბჭოს

სხდომაზე, კორპუსი ----------, აუდიტორია ----------

მისამართი: 0175, თბილისი, კოსტავას 77.

დისერტაციის გაცნობა შეიძლება სტუ-ის ბიბლიოთეკაში,

ხოლო ავტორეფერატისა - ფაკულტეტის ვებგვერდზე

საუნივერსიტეტო სადისერტაციო საბჭოს მდივანი პროფ. თ. კაიშაური

თემის აქტუალურობა

ნებისმიერ ორ მხარეს შორის ინფორმაციის მიმოცვლისას ხშირ შემთხვევაში დგება საკითხი ამ ინფორმაციის მესამე პირისაგან დაცვის შესახებ. ამ პრობლემის მოგვარების ყველაზე სწრაფი, მარტივი და გავრცელებული მეთოდია გადასაცმი ინფორმაციის დაშიფვრა. ინტერნეტით კომუნიკაციისას დაშიფვრა გამოიყენება ყოველთვის როდესაც საჭიროა გარკვეული ინფორმაციის დაცვა, მაგალითად: ბანკებში ტრანზაქციების შესრულებისას, სამთავრობო ორგანიზაციებში და სხვ.

დღეისათვის არსებობს ინფორმაციის დაშიფვრის მრავალი კრიპტოგრაფიული სისტემა (DES, RSA, AES, …). თითოეული მათგანი ხასიათდება გარკვეული უპირატესობებით და ნაკლულოვანებებით. ამიტომ ისინი გამოიყენებიან სპეციალურ მიმართულებებში, კერძოდ იმ სფეროში რომელსაც უკეთესად მიესადაგებიან. დაშიფვრის არსებული სისტემები ხასიათდებიან იმით, რომ ინფორმაციის დაშიფვრა და გაშიფვრა ხდება საიდუმლო გასაღებებით. ამ გასაღებების მნიშვნელობებთან წვდომა უნდა ჰქონდეთ მხოლოდ კორპორაციულ ქსელში ჩართულ კანონიერ მომხმარებლებს და არ უნდა ჩაუვარდეთ ხელში გარეშე პირებს. თუმცა ეს მაინც შესაძლებელია მოხდეს, მაგალითად შემდეგი მიზეზების გამო:

1.მესამე პირს შეიძლება ერთერთმა არაკეთილსინდისიერმა კანონიერმა მომხმარებელმა გაანდოს მისი მნიშვნელობა;

2.მესამე პირმა შეიძლება მომსახურე პერსონალის დაშინების, შანტაჟის ან მოსყიდვის შედეგად ადვილად მოიპოვოს გასაღების მნიშვნელობა;

3. გასაღების დიდი ხნით გამოყენების შემთხვევაში იზრდება მასზე დატვირთვა და კრიპტოანალიტიკოსს მნიშვნელოვნად უადვილდება ანალიზის ჩატარება იმ შემთხვევაში, როცა ის ფლობს ამ გასაღებით დაშიფრულ დიდი რაოდენობის შიფრტექსტებს. ასევე მას ექნება დიდი დრო და ამასთან შანსები ამ გასაღების კომპრომენტაციისათვის (მას შეუძლია ამ დროის განმავლობაში განახორციელოს სრული ან ნაწილობრივი გადარჩევა);

აქედან გამომდინარე აუცილებელია ამ სავარაუდო პრობლემების წამოჭრისგან კორპორაციულ ქსელში ჩართული კანონიერი მომხმარებლის დაცვა.

მეცნიერული სიახლე

ნაშრომში სიახლეს წარმოადგენს არსებული მეთოდებისგან მკვეთრად განსხვავებული მიდგომა ინფორმაციის დაშიფვრისადმი. კერძოდ:
გასაღების მნიშვნელობა არ არის ფიქსირებული, იგი არ არის ცნობილი ქსელში ჩართული არცერთი პირისთვის, მისი გენერირება ხდება დინამიურად დაშიფვრის ყოველი სეანსისას, ასევე ყოველ ჯერზე სხვადასხვა გასაღებთან გვაქვს საქმე.
დაშიფვრისა და გაშიფვრის ოპერაციები მნიშვნელოვნად განსხვავდება დღეისათვის არსებული როგორც სტანდარტული, ისე არასტანდარტული კრიპტოსისტემებში გამოყენებული ალგორითმებისაგან.
შექმნილია ალგორითმის სარეალიზაციო ფიზიკური მოწყობილობა.

სამუშაოს მიზანი

სამუშაოს მიზანია როგორც სტანდარტული, ისე არასტანდარტული სიმეტრიული კრიპტოგრაფიული ალგორითმებისათვის დამახასიათებელი ნაკლის უგულებელყოფა და კორპორაციულ ქსელებში გადაცემული ინფორმაციის კონფიდენციალურობის შენარჩუნება ისეთი ალგორითმის შემუშავებით, რომლის მეშვეობით შესაძლებელი იქნება: 1) რამდენიმე ასეული ბიტის შემცველი შემთხვევითი მნიშვნელობის მქონე გასაღების მიღება კავშირის ხაზში გასაღების ფორმირებაში უშუალოდ მონაწილე პარამეტრების ნამდვილი მნიშვნელობების გადაუცემლად; 2) ქსელში ჩართული კანონიერი მომხმარებლის მომსახურე პერსონალის დამშიფრავი საიდუმლო გასაღების მნიშვნელობის წვდომისგან იზოლირება; 3) მრავალი პროცედურის შესრულება სხვადასხვა ვარიანტის არჩევით პროგრამულად.

ალგორითმს უნდა ჰქონდეს საკმარისი სწრაფქმედება, გამოყენების სიმარტივე და საიმედობა. იგი უნდა იყოს ფიზიკურად რეალიზებადი.

კვლევის მეთოდები

კვლევა მიმდინარეობდა შემდეგ ეტაპებად:

- შეიქმნა მათემატიკური მოდელი;
- შეიქმნა მოდელის სარეალიზაციო კომპიუტერული პროგრამა მაღალი დონის ფუნქციონალურ ენაზე;
- შეიქმნა კომპიუტერული პროგრამა იმპერატიულ ენაზე სწრაფქმედების გასაზრდელად.

შედეგები და მათი გამოყენების სფერო

შემუშავდა ინფორმაციის დაშიფვრა/გაშიფვრის ალგორითმი, რომელშიც აღმოფხვრილია არსებული მეთოდების ნაკლულოვანებები, აქვს საკმარისი კრიპტომედეგობა და სწრაფქმედება, აკმაყოფილებს თანამედროვე მოთხოვნებს. შეიქმნა ალგორითმის სარეალიზაციო ფიზიკური მოწყობილობა, რომლის საშუალებით შესაძლებელია გადასაცემი ინფორმაციის დაშიფვრა/გაშიფვრა. ამ მოწყობილობის გამოყენება მიზანშეწონილია კორპორაციულ ქსელებში გადასაცემი ინფორმაციის კონფიდენციალურობს შესანარჩუნებლად.

დისერტაციის მოცულობა და სტრუქტურა

დისერტაციის სრული მოცულობა შეადგენს 131 ნაბეჭდ გვერდს. დისერტაცია შედგება რეზიუმესაგან (ორ ენაზე), სარჩევის, ცხრილების ნუსხის, სურათების ნუსხის, შესავლის, ოთხი თავისა და დასკვნისგან. ილუსტრაციის სახით მოყვანილია 29 ცხრილი, 47 სურათი. მოცემულია 35 დასახელების გამოყენებული ლიტერატურის ჩამონათვალი, მათ შორის, ავტორის მიერ გამოქვეყნებული სამეცნიერო ნაშრომების.

ნაშრომის შინაარსი

შესავალში გადმოცემულია დისერტაციის თემის აქტუალურობა, მიზანი და გადასაწყვეტი ამოცანები. აგრეთვე, ნაშრომის მოკლე შინაარსი თავების მიხედვით.

პირველი თავი მოიცავს ლიტერატურის მიმოხილვას. მასში აღწერილია დაშიფვრის განმახორციელებელი არსებული მეთოდები, მათი ნაკლულოვანებები და უპირატესობები.

მეორე თავში აღწერილია საიდუმლო გასაღების გენერირების ალგორითმი გარკვეული შესავალი პარამეტრების მიხედვით. დაშიფვრის ყოველი სეანსისას ფორმირდება განსხვავებული სიგრძისა და მნიშვნელობის მქონე გასაღები. შესავალ სიდიდეს წარმოადგენს რაიმე სამი მარტივი რიცხვის ნამრავლი N. ინფორმაციის მიმოცვლის ქსელში ჩართული ნებისმიერი მომხმარებლისთვის საიდუმლო გასაღების ფორმირების ალგორითმი მდგომარეობს შემდეგში:

- N დაიშლება მარტივ მამრავლებად და გამოითვლება მარტივი P, Q და R რიცხვები.
- გამოითვლება ეილერის ფუნქციის მნიშვნელობა: $\varphi(N) = (P-1)\cdot(Q-1)\cdot(R-1)$.
- განისაზღვრება P, Q და R რიცხვების ერთეულოვან თანრიგში განთავსებული a, b და c ციფრებისაგან შედგენილი (a, b, c) სამეული. ცხადია, რომ $a \in \{1,3,7,9\}$, $b \in \{1,3,7,9\}$ და $c \in \{1,3,7,9\}$.
- გამოითვლება $K = \varphi(N) mod 10$, $T = \varphi(N) mod 15$ და $S = (\mathrm{P} + \mathrm{Q} + \mathrm{R}) mod 3$ მნიშვნელობები. ისინი არაუარყოფითი მთელი რიცხვებია. რადგან ეილერის ფუნქციის მნიშვნელობა ლუწი რიცხვია, ამიტომ K-ს გამოთვლისას მიიღება 0, 2, 4, 6 და 8 რიცხვებიდან ერთ-ერთი. T მიიღებს ერთ-ერთ მნიშვნელობას [0,14] შუალედიდან, ხოლო S კი 0, 1 და 2 მნიშვნელობებიდან ერთ-ერთს;
- ერთმანეთისგან განსხვავებული 15x5 განზომილების მქონე სამი მატრიცისა და მე-3 პუნქტში გამოთვლილი K, T და S მნიშვნელობე-

ბის გამოყენებით განისაზღვრება მარტივი რიცხვების ახალი დაბოლოებები d,e, f.

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 -ის მნიშვნელობით, ხოლო მატრიცაში სვეტისა და სტრიქონის ნომერი შესაბამისად განისაზღვრება K და T მნიშვნელობებით.

ცხრილი 1. 15x5 განზომილების მქონე მატრიცა 1

	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	9,9,3	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	7,9,1
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

ცხრილი 2. 15x5 განზომილების მქონე მატრიცა 2

	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

ცხრილი 3. 15x5 განზომილების მქონე მატრიცა 3

	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

გამოითვლება ახალი მარტივი რიცხვები P_1, Q_1 და R_1:

- $P_1 = P + d - a + 10 \cdot \alpha$
- $Q_1 = Q + e - b + 10 \cdot \alpha$
- $R_1 = R + f - c + 10 \cdot \alpha$

სადაც α∈N და იცვლება ერთიდან ზემოთ მანამ, სანამ თითოეული რიცხვი არ გახდება მარტივი.

- გამოითვლება $N_1 = P_1 \cdot Q_1 \cdot R_1$
- გამოითვლება m=a+b+c+d+e+f
- გამოითვლება $P \mathrel{*}= ((P_1 - 1)/2 - \mathrm{m})^2 \; mod \; P$
- გამოითვლება $Q \mathrel{*}= ((Q_1 - 1)/2 - \mathrm{m})^2 \; mod \; Q$
- გამოითვლება $R \mathrel{*}= ((R_1 - 1)/2 - \mathrm{m})^2 \; mod \; R$

ეს პუნქტები გამეორდება 4-ჯერ, ამასთან, პირველის გარდა ყოველი შემდეგი ეტაპის შესავალ სიდიდეს წარმოადგენს წინა ეტაპზე გამოთვლილი N-ის მნიშვნელობა. შედეგად დაგროვდება მე-4 ცხრილში ნაჩვენები შემდეგი სახის მოაცემები:

ცხრილი 4. ოთხი იტერაციის შედეგად დაგროვილი მონაცემები

#	In	N	φ(N)	P	Q	R	P*	Q*	R*	K	T	S
1	N_0	N_1	$\varphi(\mathrm{N})_1$	P_1	Q_1	R_1	${P^*}_1$	${Q^*}_1$	${R^*}_1$	K_1	T_1	S_1
2	N_1	N_2	$\varphi(\mathrm{N})_2$	P_2	Q_2	R_2	${P^*}_2$	${Q^*}_2$	${R^*}_2$	K_2	T_2	S_2
3	N_2	N_3	$\varphi(\mathrm{N})_3$	P_3	Q_3	R_3	${P^*}_3$	${Q^*}_3$	${R^*}_3$	K_3	T_3	S_3
4	N_3	N_4	$\varphi(\mathrm{N})_4$	P_4	Q_4	R_4	${P^*}_4$	${Q^*}_4$	${R^*}_4$	K_4	T_4	S_4

N, φ(N), P,Q, R, P^*, Q^* და R^* მნიშვნელობების მიხედვით გამოითვლება ერთსახელა პარამეტრებისათვის როგორც ორ-ორი, ისე სამ-სამი წევრის ნამრავლები და ჯამები (ცხრილი 5).

ცხრილი 5. ნამრავლები და ჯამები

1	N_1	23	P_1	45	R_1	67	${Q^*}_1$
2	N_2	24	P_2	46	R_2	68	${Q^*}_2$
3	N_3	25	P_3	47	R_3	69	${Q^*}_3$

4	$N_1 \cdot N_2$	26	$P_1 \cdot P_2$	48	$R_1 \cdot R_2$	70	$Q^*_1 \cdot Q^*_2$
5	$N_1 \cdot N_3$	27	$P_1 \cdot P_3$	49	$R_1 \cdot R_3$	71	$Q^*_1 \cdot Q^*_3$
6	$N_2 \cdot N_3$	28	$P_2 \cdot P_3$	50	$R_2 \cdot R_3$	72	$Q^*_2 \cdot Q^*_3$
7	$N_1 + N_2$	29	$P_1 + P_2$	51	$R_1 + R_2$	73	$Q^*_1 + Q^*_2$
8	$N_1 + N_3$	30	$P_1 + P_3$	52	$R_1 + R_3$	74	$Q^*_1 + Q^*_3$
9	$N_2 + N_3$	31	$P_2 + P_3$	53	$R_2 + R_3$	75	$Q^*_2 + Q^*_3$
10	$N_1 \cdot N_2 \cdot N_3$	32	$P_1 \cdot P_2 \cdot P_3$	54	$R_1 \cdot R_2 \cdot R_3$	76	$Q^*_1 \cdot Q^*_2 \cdot Q^*_3$
11	$N_1 + N_2 + N_3$	33	$P_1 + P_2 + P_3$	55	$R_1 + R_2 + R_3$	77	$Q^*_1 + Q^*_2 + Q^*_3$
12	φ_1	34	Q_1	56	P^*_1	78	R^*_1
13	φ_2	35	Q_2	57	P^*_2	79	R^*_2
14	φ_3	36	Q_3	58	P^*_3	80	R^*_3
15	$\varphi_1 \cdot \varphi_2$	37	$Q_1 \cdot Q_2$	59	$P^*_1 \cdot P^*_2$	81	$R^*_1 \cdot R^*_2$
16	$\varphi_1 \cdot \varphi_3$	38	$Q_1 \cdot Q_3$	60	$P^*_1 \cdot P^*_3$	82	$R^*_1 \cdot R^*_3$
17	$\varphi_2 \cdot \varphi_3$	39	$Q_2 \cdot Q_3$	61	$P^*_2 \cdot P^*_3$	83	$R^*_2 \cdot R^*_3$
18	$\varphi_1 + \varphi_2$	40	$Q_1 + Q_2$	62	$P^*_1 + P^*_2$	84	$R^*_1 + R^*_2$
19	$\varphi_1 + \varphi_3$	41	$Q_1 + Q_3$	63	$P^*_1 + P^*_3$	85	$R^*_1 + R^*_3$

20	$\varphi_2 + \varphi_3$	42	$Q_2 + Q_3$	64	$P^*_2 + P^*_3$	86	$R^*_2 + R^*_3$
21	$\varphi_1 \cdot \varphi_2 \cdot \varphi_3$	43	$Q_1 \cdot Q_2 \cdot Q_3$	65	$P^*_1 \cdot P^*_2 \cdot P^*_3$	87	$R^*_1 \cdot R^*_2 \cdot R^*_3$
22	$\varphi_1 + \varphi_2 + \varphi_3$	44	$Q_1 + Q_2 + Q_3$	66	$P^*_1 + P^*_2 + P^*_3$	88	$R^*_1 + R^*_2 + R^*_3$

მე-5 ცხრილში არსებული მონაცემების შეერთებით მარცხნიდან მარჯვნივ ფორმირდება საიდუმლო გასაღები.

აღწერილ ალგორითმს აქვს ორი მნიშვნელოვანი თვისება:

- N-ის გაზრდისას იზრდება გასაღების სიგრძეც;
- ნებისმიერ N-ს შეესაბამება გასაღების ერთადერთი მნიშვნელობა;

გარდა ამისა, გასაღების ფორმირების ეს ალგორითმი შეგვიძლია გამოვიყენოთ სხვა სიმეტრიული კრიპტოსისტემებისათვის და ნაწილობრივ ასიმეტრიული კრიპტოსისტემებისათვისაც.

ხსენებულ ალგორითმს აქვს შემდეგი დადებითი მხარეები:

- არ საჭიროებს კავშირის ხაზში დაშიფვრის პროცედურაში უშუალოდ მონაწილე არც ერთი პარამეტრის გადაცემას;
- კორპორაციული ქსელის არაკანონიერ მომხმარებელს შეუძლია ალგორითმის საწყისი მონაცემის (სამი 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;

მესამე თავი ეძღვნება არსებული საიდუმლო გასაღებით ნებისმიერი ტიპის ინფორმაციის დაშიფვრის ალგორითმის მიმოხილვას. განხილული დაშიფვრისა და გაშიფვრის ოპერაციები მნიშვნელოვნად განსხვავდება დღეისათვის არსებულ როგორც სტანდარტულ, ისე არასტანდარტულ კრიპტოსისტემებში გამოყენებული მეთოდებისაგან. გასაღების ფორმირების შემდეგ ხდება მისი გამოყენება ირიბად. დასაშიფრი ბლოკების მიხედვით შემთხვევით შეირჩევა გასაღების გარკვეული ფრაგმენტი და შემდეგ ხდება მისი გამოყენება. ამ ყველაფრის შედეგად მივიღებთ იმას, რომ გასაღების მოპოვებაც კი არ არის საკმარისი ინფორმაციის გასატეხად. დამატებით საჭიროა იმ პარამეტრების გადარჩევა, რომელთა საშუალებითაც ხდება დასაშიფრი ბლოკებისთვის გასაღების ფრაგმენტების გამოთვლა.

დაშიფვრის ალგორითმი

ვთქვათ მოცემულია l რაოდენობის დასაშიფრი სიდიდე. ჩვენ შეგვიძლია ისინი გადავნომროთ 0 .. l-1-მდე. ანუ თითოეულ მათგანს შეესაბამება მთელი i რიცხვი => i ∈ {0..l-1} სიმრავლეს. ახლა უკვე შესაძლებელია დაშიფვრის ოპერაციის შესრულება, რომელიც მდგომარეობს შემდეგში:

ყოველი ელემენტისთვის სრულდება შემდეგი სახის გამოთვლები:

$$f(a) = \big(a + K(i)\big) mod\ m,$$

სადაც a არის მიმდინარე დასაშიფრი სიდიდე, ხოლო K(i) არის ფუნქცია, რომელიც ითვლის გასაღების კონკრეტულ მნიშვნელობას მოცემულ ეტაპზე.

გაშიფვრის ალგორითმი

დაშიფრული ინფორმაციის გაშიფვრა, ანუ საწყისი ტექსტის აღდგენა ხდება შემდეგნაირად: შესავალი მასივის ყოველი წევრისათვის სრულდდება გამოთვლები:

$$f(e) = r - K(i),$$

სადაც e არის მიმდინარე დაშიფრული სიდიდე, ხოლო K(i) ფუნქციაა, რომელიც ითვლის გასაღების კონკრეტულ მნიშვნელობას მოცემულ ეტაპზე. ეს ფუნქცია იდენტურია დაშიფვრის ალგორითმში არსებული ფუნქციისა. თუ სრულდება $r \geq 0$ პირობა, მაშინ გაშიფვრა მთავრდება შემდეგი გამოსახულებით: $d = r \bmod m$, ხოლო, თუ არ სრულდება, მაშინ r-ს ემატება მოდული m, მანამ სანამ არ გახდება დადებითი. ბოლოს გამოითვლება ისევ გამოსახულება $d=r \bmod m$. სადაც d გაშიფრული მნიშვნელობაა.

ვნახოთ თუ როგორი სახე ექნება ერთსა და იმავე დასაშიფრ სიდიდეზე მიღებულ შედეგებს სხვადასხვა N-ის გამოყენების დროს. ქვემოთ მე-6 და მე-7 ცხრილებში ნაჩვენებია დასაშიფრი და დაშიფრული რიცხვები, როცა N=1879981 და 1296207281. ისინი ერთმანეთისგან გამოყოფილნი არიან ორწერტილით (დასაშიფრი:დაშიფრული). როგორც ცხრილებიდან ჩანს ერთიდაიგივე დასაშიფრ სიდიდეს შეესაბამება საგრძნობლად განსხვავებული დაშიფრული მნიშვნელობები.

ცხრილი 6. დასაშიფრი და დაშიფრული მნიშვნელობები როცა N=1879981

0:359	0:254	0:57	0:825	0:275	0:736	0:95	0:714
0:15	0:138	0:40	0:302	0:724	0:441	0:681	0:43
0:291	0:112	0:42	0:114	0:78	0:317	0:295	0:144
0:115	0:326	0:132	0:631	0:220	0:471	0:747	0:242
0:409	0:312	0:266	0:129	0:165	0:174	0:174	0:270
0:266	0:99	0:199	0:386	0:175	1:358	2:306	3:274
4:76	5:112	6:158	7:255	8:549	9:444	10:0	11:278
12:195	13:467	14:493	15:31	16:823	17:122	18:168	19:146
20:167	21:388	22:103	23:861	24:326	25:397	26:437	27:131
28:452	29:225	30:164	31:526	32:381	33:73	34:303	35:203
36:633	37:190	38:448	39:85	40:42	41:293	42:309	43:820
44:343	45:87	46:456	47:467	48:119	49:100	50:351	51:499
52:357	53:457	54:71	55:117	56:129	57:142	58:145	59:659
60:85	61:77	62:134	63:123	64:4	65:350	66:323	67:343

68:275	69:5	70:149	71:471	72:115	73:80	74:517	75:100

ცხრილი 7. დასაშიფრი და დაშიფრული მნიშვნელობები როცა N=1296207281

0:592	0:692	0:308	0:769	0:339	0:395	0:595	0:570
0:492	0:412	0:267	0:52	0:373	0:88	0:849	0:531
0:135	0:229	0:347	0:69	0:23	0:567	0:275	0:702
0:35	0:9	0:35	0:356	0:212	0:52	0:395	0:172
0:301	0:157	0:213	0:573	0:39	0:179	0:244	0:367
0:266	0:886	0:31	0:291	0:286	1:134	2:84	3:323
4:74	5:49	6:274	7:228	8:231	9:322	10:156	11:301
12:331	13:21	14:395	15:774	16:306	17:78	18:144	19:311
20:49	21:7	22:253	23:213	24:301	25:406	26:548	27:780
28:314	29:184	30:345	31:171	32:405	33:638	34:339	35:21
36:562	37:96	38:390	39:165	40:401	41:310	42:773	43:107
44:782	45:109	46:321	47:265	48:292	49:454	50:910	51:533
52:405	53:349	54:237	55:185	56:323	57:168	58:194	59:358
60:0	61:42	62:189	63:270	64:359	65:804	66:62	67:12
68:355	69:571	70:441	71:17	72:100	73:393	74:181	75:105

მეოთხე თავში წარმოდგენილია ალგორითმის სარეალიზაციო ფიზიკური მოწყობილობა, რომელსაც შეუძლია დაშიფროს და გაშიფროს როგორც მცირე ტექსტური შეტყობინებები, ისე დიდი ელექტრონული წიგნები, ვიდეო და აუდიო ფაილები, სურათები და ა.შ. ნებისმიერი ფიზიკური ფაილი კომპიუტერის მეხსიერებაში.

მოწყობილობა უერთდება პერსონალურ კომპიუტერს ინტერნეტის კაბელის მეშვეობით. მასთან ურთიერთქმედება ხორციელდება სპეციალური კომპიუტერული პროგრამის მიერ, რომელიც ასევე ჩვენს მიერ არის შექმნილი.

აღწერილი ალგორითმიდან გამომდინარე, დამშიფრავ და გამშიფრავ მოწყობილობასთან დაკავშირებით შეგვიძლია ვიმსჯელოთ შემდეგნაირად:

- იგი წარმოადგენს ერთგვარ ავტონომიურ სერვერულ კომპიუტერს, რომელთან ურთიერთქმედება შესაძლებელია სპეციალურად მისთვის შექმნილი პროგრამისა და პროტოკოლის საშუალებით;
- შესაძლებელია დამზადდეს ნებისმიერი რაოდენობის მოწყობილობა, რომელთაც ერთნაირი საიდუმლო პარამეტრები ექნებათ;
- შესაძლებელია დამზადდეს ნებისმიერი რაოდენობის მოწყობილობა, რომელთაც სრულიად განსხვავებული საიდუმლო პარამეტრები ექნებათ;
- ნებისმიერ მოწყობილობას, რომელსაც შეუძლია ინფორმაციის დაშიფვრა, ასევე შეუძლია იგივე ინფორმაციის გაშიფვრა;
- ნებისმიერ მოწყობილობას შეუძლია მისი იდენტური საიდუმლო პარამეტრების მქონე სხვა მოწყობილობის მიერ დაშიფრული ინფორმაციის გაშიფვრა;
- ნებისმიერ ორ მოწყობილობას, რომელთაც განსხვავებული საიდუმლო პარამეტრები აქვთ, არ შეუძლიათ ერთმანეთის მიერ დაშიფრული ინფორმაციის გაშიფვრა;

ამ საბაზო პრინციპებიდან გამომდინარე, შესაძლებელია არსებობდეს ორი ქსელი, რომელთაგანაც საერთო ქსელში ჩართულ მომხმარებლებს შეეძლებათ ერთმანეთის მიერ დაშიფრული ინფორმაციის გაშიფვრა, მაგრამ არ შეეძლებათ სხვა ქსელში დაშიფრული მონაცემების გაშიფვრა.

ნაშრომის აპრობაცია.

დისერტაციის ძირითადი შინაარსი მოხსენებული იყო ინფორმატიკისა და მართვის სისტემების ფაკულტეტის მართვის სისტემების დეპარტამენტის სემინარებზე. ასევე, ჩატარდა დისერტაციის წინასწარი დაცვა აღნიშნუ-

ლი დეპარტამენტის სხდომაზე. პუბლიკაციები: დისერტაციაში განხილული საკითხები გამოქვეყნებულია 6 სამეცნიერო ნაშრომში, 2013-2018 წლებში:

1. ვ.კუცნავა, გ. გოგოლაძე. ცვლადპარამეტრებიანი დაშიფვრის RSA კრიპტოსისტემა. მართვის ავტომატიზებული სისტემები. №2(15). თბილისი. 2013, გვ. 71-75.
2. ვასილ კუცნავა, პაატა ჯოხაძე, გიორგი გოგოლაძე. 1024 ბიტის შემცველი ბლოკის დაშიფვრის სიმეტრიული კრიპტოალგორითმი. მართვის ავტომატიზებული სისტემები. №2(18). თბილისი. 2014, გვ. 21-27.
3. ვ.კუცნავა, ა. კუცნავა, გ. გოგოლაძე. მონაცემთა ბლოკის დაშიფვრის არასტანდარტული სიმეტრიული კრიპტოალგორითმი. მართვის ავტომატიზებული სისტემები. შრომები. №1(19). თბილისი. 2015, გვ. 30-37.
4. ვ.კუცნავა, ა. კუცნავა, გ. გოგუა, გ. გოგოლაძე. ინფორმაციის დაშიფვრის სიმეტრიული კრიპტოგრაფიული სისტემებისათვის საიდუმლო გასაღების მაფორმირებელი ალგორითმი. მართვის ავტომატიზებული სისტემები. შრომები. №1(21). თბილისი. 2016, გვ. 70-77.
5. ვ.კუცნავა, ა. კუცნავა, გ. გოგოლაძე. ინფორმაციის დაშიფვრის არასტანდარტული სიმეტრიული კრიპტოგრაფიული ალგორითმი. მართვის ავტომატიზებული სისტემები. შრომები. №1(21). თბილისი. 2016, გვ. 78-82.
6. გ. გოგოლაძე, ვ.კუცნავა, ა. კუცნავა. ასიმეტრიული კრიპტოგრაფიული RSA კრიპტოსისტემისათვის ღია და საიდუმლო გასაღებების წყვილის მაფორმირებელი ალგორითმი. მართვის ავტომატიზებული სისტემები. შრომები. №1(23). თბილისი. 2017, გვ. 49-55.

Data encryption nonstandard symmetric cryptographic algorithm with software

Abstract

In case of communication between any two parties, encryption is used to protect the information. Various companies, corporate networks, banks, etc. use different methods of encryption to protect their information from unwanted persons.

Symmetric and asymmetric systems are found in modern cryptography. In order to achieve high levels of security in asymmetric systems, it is necessary to use large numbers, which significantly slows down the process, so in practice this method is less common. Encryption and decryption of information in symmetric systems is carried out with the same secret key, and in asymmetric systems encryption is carried out with public keys and decryption with private keys. These keys should not go into the hands of undesirable persons.

In the attempt to break the information, a person may gain private key from any of the users involved in the network or to fully or partially generate it with a statistical analysis of the large amount of data encrypted with the same key.

The existing methods can not provide protection from these problems because the key is known to every legal user and every information block is encoded by the same key.

According the algorithm the value of the key is not fixed, so we do not have it at the initial stage. Therefore, nobody knows anything about him. Every encryption session generates a random key with a random length, and then uses it, ie every time we want to encrypt any information, we have dealing with different keys.

Product of the three simple numbers (known as N) are required to get a secret key. The use of large numbers will provide a longer key. Also, any N corresponds to the only one of the keys. That's why legitimate users involved in the network can independently create the same secret key.

The encryption and decryption operations discussed in the algorithm differ significantly from the methods used in both standard and nonstandard cryptosystems. After formation of the key, it is used indirectly. An accidentall fragments of the key are used to encrypt every block of data. As a result of all this, finding a private key is not enough to break the information.

We have manufactured the device that represents the realization of the reviewed algorithm. It can successfully encrypt and decrypt text messages, video and audio files, pictures, etc. The device is characterized by simplicity, efficiency and mobility of use. It connects the personal computer via the internet cable.

Interaction with it is carried out by a special computer program, which is also created by us.

It is possible to produce any number of devices that have the same secret options. It is also possible to produce any number of devices that have different secret options.

Those devices which have the same options can encrypt each other encrypted information, and those who have different options can not do that. Therefore, there may be two networks, where users involved in the network will be able to decrypt the information encrypted by each other, but they will not be able to decrypt the encrypted data in another network.

Advantages of algorithm can be as follows:

- The parameters in the procedures are unknown;
- The options used in encryption are not transmitted in the line of the connection;
- An undesirable person can gain an initial parameter N, but with this data he will not be able to generate the secret key.
- In each new session of communication between legitimate users a new secret key is generated;
- If the undesirable person obtains the value of the secret key, he will not be able to decrypt the information;
- Algorithm is characterized by high reliability and efficiency.

As we have already mentioned, we do not have a constant secret key, but in his role there are many secret parameters that are reviewed in the algorithm, they have a completely different role and they should not fall into the hands of the undesirable person.