ინფორმაციის დაშიფვრის არასტანდარტული სიმეტრიული კრიპტოგრაფიული ალგორითმი

ვასილ კუციავა, ანა კუციავა, გიორგი გოგოლაძე
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია ათობითი სისტემით წარმოდგენილი ***ASCII*** ან ***EBCDIC*** კოდის ნებისმიერი რაოდენობის სიმბოლოებისგან შედგენილი მონაცემთა ბლოკის დაშიფვრა არასტანდარტული სიმეტრიული კრიპტოსისტემის ალგორითმის გამოყენებით. დაშიფვრა მიმდინარეობს შემთხვევითი მნიშვნელობის და შემთხვევითი სიგრძის მქონე საიდუმლო გასაღებით, რომლის მიღება ხდება პროგრამულად გასაღების მაფორმირებელი ალგორითმის მიხედვით. დაშიფვრა ხორციელდება ვიჟინერის მეთოდით (ერთი და იმავე გასაღების მრავალჯერ გამოყენება ან ავტოგასაღების რეჟიმი, რომელშიც ძირითადი გასაღების ამოწურვის შემდეგ საიდუმლო გასაღებად გამოიყენება საწყისი ღია ტექსტი ან დაშიფვრის შედეგად მიღებული შიფრტექსტი).

საკვანძო სიტყვები: არასტანდარტული სიმეტრიული ალგორითმი. ვიჟინერის მეთოდი. საიდუმლო გასაღები. კრიპტომედეგობა. სწრაფქმედება.

1. შესავალი

კორპორაციულ ქსელებში ჩართულ კანონიერ მომხმარებლებს შორის გადაცემული ინფორმაციის კონფიდენციალურობის უზრუნველსაყოფად გამოიყენება როგორც სიმეტრიული, ისე ასიმეტრიული კრიპტოგრაფიული ალგორითმები. აქვე უნდა აღინიშნოს, რომ დიდი ბიუჯეტის (10 მილიონ დოლარამდე) მქონე კორპორაციებისათვის ადვილად განსახორციელებელია ისეთი სიმეტრიული კრიპტოგრაფიული ალგორითმების "გატეხა", რომელთა საიდუმლო გასაღების სიგრძე არ აღემატება **64** –ს ("გატეხა" ხორციელდება გასაღების ყველა მნიშვნელობის გადამრჩევი ***FPGA*** და ***ASIC*** მიკროსქემების ან სუპერკომპიუტერის გამოყენებით). ასეთ ალგორითმს წარმოადგენს **DES** ალგორითმი, რომლის გასაღების ყველა მნიშვნელობა 2^{56}-ის ტოლია. ამის გამო ***DES*** სტანდარტის ნაცვლად გამოიყენება ***AES*** სტანდარტი, რომლის საიდუმლო გასაღების სიგრძეა **128**, **192** ან **256** ბიტი, ხოლო დასაშიფრი ბლოკის - **128** ბიტი. მაგრამ გამოთვლითი ტექნოლოგიების განვითარებამ უახლოეს მომავალში შეიძლება მიაღწიოს ისეთ დონეს, რომ შესაძლებელი გახდეს ***AES*** სტანდარტის "გატეხაც".

არსებული კრიპტოგრაფიული ალგორითმების ერთ-ერთი ნაკლია ის გარემოებაც, რომ კორპორაციულ ქსელში ჩართული კანონიერი მომხმარებლების პერსონალისათვის ცნობილია როგორც საიდუმლო გასაღების მნიშვნელობა, ისე თვით ალგორითმი. ამ გარემოების გამო არაკანონიერ მომხმარებლებს შეუძლიათ ბანდიტური კრიპტოანალიზის შედეგად (დაშინების, წამების, შანტაჟის ან ქრთამის მიცემის გზით) მოიპოვონ გასაღების მნიშვნელობა და მონაცემთა დაშიფვრისათვის გამოყენებული ალგორითმი.

აღნიშნული ნაკლულოვანებების უგულებელსაყოფად მიზანშეწონილად ჩავთვალეთ კორპორაციულ ქსელებში გადაცემული ინფორმაციის კონფიდენციალურობის შესანარჩუნებლად ისეთი არასტანდარტული სიმეტრიული ალგორითმის შემუშავება, რომელიც მუშაობს გაცილებით დიდი გასაღებით, კავშირის ხაზში არ საჭიროებს როგორც დაშიფვრის, ისე გაშიფვრის პროცედურებში უშუალოდ მონაწილე არცერთი პარამეტრის მნიშვნელობის გადაცემას და მომსახურე პერსონალმა არ იცის დამშიფრავი საიდუმლო გასაღების მნიშვნელობა. შემუშავებული ალგორითმი გამოირჩევა მაღალი კრიპტომედეგობით.

2. ძირითადი ნაწილი

დასაშიფრი ღია ტექსტის მონაცემები $\boldsymbol{ASCII}$ ან $\boldsymbol{EBCDIC}$ კოდში შემავალი სიმბოლოებია წარმოდგენილი ათობითი სისტემის შესაბამისი ნომრებით. თითოეული სიმბოლო გამოსახულია სამთანრიგა ათობითი რიცხვით. ღია ტექსტის დაშიფვრისას მასში შემავალ სიმბოლოების შესაბამისი ათობითი ციფრების მიმდევრობის ქვეშ მოთავსდება ფორმირებული საიდუმლო გასაღების ციფრების მიმდევრობა.

გასაღების ფორმირებისას ხდება

$$\boldsymbol{K_{i-1} = \varphi_{i-1}(N_{i-1}) mod 10},\ \boldsymbol{T_{i-1} = \varphi_{i-1}(N_{i-1}) mod 15},\ \boldsymbol{S_{i-1} = \varphi_{i-1}(N_{i-1}) mod 3}$$

მნიშვნელობების გამოთვლა, სადაც $\boldsymbol{K_{i-1}, T_{i-1}, S_{i-1}}$ არაუარყოფითი მთელი რიცხვებია, $\boldsymbol{\varphi_{i-1}(N_{i-1})}$ ეილერის ფუნქცია, ხოლო $\boldsymbol{N_{i-1}}$ სამი მარტივი რიცხვის ნამრავლი [3]. რადგან ეილერის ფუნქციის მნიშვნელობა ლუწი რიცხვია, ამიტომ $\boldsymbol{K_{i-1}}$ –ის გამოთვლისას მიიღება $\boldsymbol{0, 2, 4, 6}$ ან $\boldsymbol{8}$ რიცხვებიდან ერთ-ერთი. $\boldsymbol{T_{i-1}}$ მიიღებს ერთ-ერთ მნიშვნელობას $\boldsymbol{[0, 14]}$ შუალედიდან, ხოლო $\boldsymbol{S_{i-1}}$ კი $\boldsymbol{0}$, $\boldsymbol{1}$ და $\boldsymbol{2}$ მნიშვნელობებიდან ერთ-ერთს (გამოთვლა ხორციელდება $\boldsymbol{i = 1, 2, 3}$ და $\boldsymbol{4}$ მნიშვნელობებისათვის).

ღია ტექსტის ქვეშ საიდუმლო გასაღების მოთავსების შემდეგ შესრულდება მარცხნიდან მარჯვნივ სამ-სამი, ოთხ-ოთხი ან ხუთ-ხუთი ციფრებით გამოსახული რიცხვების შეკრება $\boldsymbol{m}$ მოდულით. თითოეულ ჯგუფში შემავალი ციფრების რაოდენობის განსაზღვრა ხდება $\boldsymbol{S_3}$ –ის მნიშვნელობის მიხედვით ($\boldsymbol{S_3 = 0}$ –სამი ციფრი, $\boldsymbol{S_3 = 1}$ –ოთხი ციფრი, $\boldsymbol{S_3 = 2}$ – ხუთი ციფრი). მიმდევრობის სამ-სამად დაყოფისას თითოეული სამთანრიგა ჯგუფისათვის $\boldsymbol{m}$ წარმოადგენს ინდივიდუალურ მნიშვნელობას, ხოლო ოთხ-ოთხ და ხუთ-ხუთ ციფრიან ჯგუფებად დაყოფისას $\boldsymbol{m}$ –ის მნიშვნელობა, შესაბამისად, $\boldsymbol{10000}$ და $\boldsymbol{100000}$ –ის ტოლია. აქვე უნდა აღინიშნოს, რომ:

1) თუ დასაშიფრ ღია ტექსტის მონაცემებში შემავალი ციფრების რაოდენობა არაა ოთხის ან ხუთის ჯერადი, მაშინ დაყოფის შედეგად მიღებული ბოლო მარჯვენა ჯგუფი შეივსება საჭირო რაოდენობის ნულებით;

2) თუ საიდუმლო გასაღებში შემავალი ციფრების მიმდევრობაში შემავალი ციფრების რაოდენობა არაა $\boldsymbol{3}$ –ის, $\boldsymbol{4}$ –ის ან $\boldsymbol{5}$ –ის ჯერადი, მაშინ დაყოფის შედეგად მიღებული ბოლო მარჯვენა ჯგუფი გაუქმდება.

ციფრების მიმდევრობის სამ-სამად დაყოფისას $\boldsymbol{m}$ მოდულის ინდივიდუალური მნიშვნელობების განსაზღვრა ხდება $\boldsymbol{1}$, $\boldsymbol{2}$ და $\boldsymbol{3}$ მატრიცების საშუალებით. თითოეული მატრიცა $\boldsymbol{15 \times 5}$ განზომილებისაა და შეიცავს მოდულების $\boldsymbol{75}$ მნიშვნელობას.

ამ სამი მატრიციდან ერთ-ერთის არჩევა ხდება $\boldsymbol{S}$–ის მნიშვნელობის მიხედვით, ხოლო მატრიცის სვეტისა და სტრიქონის არჩევა, შესაბამისად, $\boldsymbol{K}$ და $\boldsymbol{T}$-ს მნიშვნელობის მიხედვით (თავდაპირველად სვეტი და შემდეგ სტრიქონი). რადგან ალგორითმის მიხედვით გამოთვლილია $\boldsymbol{S, K}$ და $\boldsymbol{T}$ სამეულების ოთხი მნიშვნელობა, ამიტომ მოდულების პირველი ოცი მნიშვნელობა შეირჩევა $\boldsymbol{K_0, T_0, S_0}$ სამეულით, მეორე ოცეული $\boldsymbol{K_1, T_1, S_1}$ სამეულით, მესამე - $\boldsymbol{K_2, T_2, S_2}$ სამეულით, ხოლო მეოთხე - $\boldsymbol{K_3, T_3, S_3}$ სამეულით. ე.ი. სულ მიიღება მოდულის $\boldsymbol{80}$ მნიშვნელობა ($\boldsymbol{S}$, $\boldsymbol{K}$ და $\boldsymbol{T}$-ს მნიშვნელობიდან გამომდინარე შეიძლება მოხდეს მოდულების მნიშვნელობების გამეორება). ოთხმოცი ჯგუფის შემდეგ დაიწყება გამეორება.

მატრიცა 1 ($S = 0$)

	K = 0	K= 2	K = 4	K = 6	K = 8
T = 0	713	444	961	518	318
T = 1	322	734	687	811	928
T = 2	438	612	568	293	871
T = 3	824	917	482	378	384
T = 4	374	712	728	648	311
T = 5	538	338	554	958	529
T = 6	628	934	817	558	283
T = 7	711	473	356	813	496
T = 8	268	588	638	976	733
T = 9	924	504	437	643	967
T = 10	821	638	578	715	658
T = 11	362	742	296	348	513
T = 12	938	278	753	478	684
T = 13	464	734	989	831	873
T = 14	803	393	621	929	492

მატრიცა 2 ($S = 1$)

	K = 0	K = 2	K = 4	K = 6	K = 8
T = 0	810	673	512	401	379
T = 1	733	643	578	938	268
T = 2	530	285	490	895	824
T = 3	967	713	283	612	811
T = 4	568	917	374	628	473
T = 5	529	356	588	924	384
T = 6	845	310	495	295	560
T = 7	728	554	817	356	638
T = 8	989	753	296	528	437
T = 9	515	905	940	780	505
T = 10	685	580	570	425	305
T = 11	734	568	378	3843	322
T = 12	444	687	293	704	713
T = 13	518	928	961	811	872
T = 14	619	783	708	521	654

მატრიცა 3 ($S = 2$)

	K = 0	K= 2	K = 4	K = 6	K = 8
T = 0	972	512	472	702	602
T = 1	382	768	572	649	889
T = 2	587	812	932	324	757
T = 3	843	313	613	988	501
T = 4	298	343	831	430	942
T = 5	745	971	281	893	301
T = 6	351	624	875	513	498
T = 7	968	527	770	561	712
T = 8	402	861	488	270	652
T = 9	635	462	582	961	318
T = 10	858	594	723	663	363
T = 11	539	952	460	791	803
T = 12	782	436	677	477	922
T = 13	451	682	320	713	572
T = 14	697	734	957	374	445

მაგალითად, თუ $S_0 = 0$, $K_0 = 2$, $T_0 = 11$, $S_1 = 1$, $K_1 = 0$, $T_1 = 1$, $S_2 = 2$, $K_2 = 4$, $T_2 = 8$, $S_3 = 0$, $K_3 = 6$ და $T_3 = 5$, მაშინ მიიღება მოდულების მნიშვნელობების შემდეგი ოთხმოცი მნიშვნელობა: **444, 734, 612, 917, 713,338, 934, 473, 588, 504, 638, 742, 278, 734, 393, 362, 742, 296, 348, 513, 810, 733, 530, 967, 568, 529, 845, 728, 989, 515, 685, 734, 444, 518, 619, 382, 768, 572, 649, 889, 472, 572, 932, 613, 831, 281, 875, 770, 488, 582, 723, 460, 677, 320, 957, 402, 861, 488, 270, 652, 518, 811, 293, 378, 648, 958, 558, 813, 976, 643, 712, 348, 478, 831, 929, 745, 971, 281, 893, 301.**

როდესაც ღია ტექსტში შემავალი ათობითი რიცხვების რაოდენობა აღემატება საიდუმლო გასაღებში შემავალი ციფრების რაოდენობას, მაშინ ხდება გასაღების თანამიმდევრობის გამეორება სარკული ანარეკლით (ციფრების წაკითხვა მოხდება მარჯვნიდან მარცხნივ) ან დაშიფვრა გაგრძელდება ავტოგასაღების რეჟიმში (შიფრტექსტის ან ღია ტექსტის ციფრების მიმდევრობის გამოყენება მარცხნიდან მარჯვნივ). ამ სამი რეჟიმიდან ერთ-ერთის არჩევა ხდება S_2–ის მნიშვნელობის მიხედვით შემდეგნაირად:

1) $S_2 = 0$ – გასაღები მეორდება საჭიროების მიხედვით;

2) $S_2 = 1$ – საწყისი გასაღების ამოწურვის შემდეგ გასაღების როლს ასრულებს მიღებული შიფრტექსტი დასაწყისიდან;

3) $S_2 = 2$ – საწყისი გასაღების ამოწურვის შემდეგ გასაღების როლს ასრულებს ღია ტექსტი დასაწყისიდან.

ალგორითმში გამოყენებული მატრიცები საიდუმლო გასაღებებია და მათი შედგენილობა ცნობილი უნდა იყოს მხოლოდ კორპორაციულ ქსელში ჩართული კანონიერი მომხმარებლებისათვის. ალგორითმის კრიპტომედეგობის გასაზრდელად მიზანშეწონილია ამ მატრიცების შედგენილობის ცვლილება დროის გარკვეული პერიოდის გასვლის შემდეგ.

შიფრტექსტის გაშიფვრის შესასრულებლად მიმღებში შიფრტექსტს ქვეშ მიეწერება საიდუმლო გასაღები და შესრულდება გამოკლება იმავე მოდულით. უარყოფითი რიცხვის მიღებისას ხდება მოდულის მნიშვნელობის მიმატება.

3. დასკვნა

ჩვენს მიერ შემოთავაზებულ ალგორითმს აქვს შემდეგი ღირსებები:

1. ალგორითმის პროცედურებში მონაწილე ნებისმიერი პარამეტრის მნიშვნელობა უცნობია მომსახურე პერსონალისათვის;

2. დაშიფვრა შეიძლება შესრულდეს როგორც მონაცემების ბლოკებად დაყოფით (ერთი გასაღების მრავალჯერ გამოყენებით), ისე დაყოფის გარეშე (ავტოგასაღების რეჟიმი შიფრტექსტის ან ღია ტექსტის გამოყენებით). ამ რეჟიმების არჩევა ხდება პროგრამულად გამოთვლილი პარამეტრების მნიშვნელობების მიხედვით;

3. ალგორითმში შესრულებული გამოთვლების შედეგად მიღებული შედეგების მიხედვით ხდება სამთანრიგა ათობითი რიცხვებით წარმოდგენილი დასაშიფრი სიმბოლოების შესატყვისი ათობითი ციფრების მიმდევრობის დაყოფა მარცხნიდან მარჯვნივ სამ, ოთხ ან ხუთციფრიან ჯგუფებად და შემდეგ თითოეული ჯგუფის დაშიფვრა მოდულის ინდივიდუალური მნიშვნელობის გამოყენებით. ამ უკანასკნელის არჩევა ხდება სპეციალური მატრიცებიდან გამოთვლით მიღებული პარამეტრების მნიშვნელობების მიხედვით.

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 სიმეტრიული კრიპტოალორითმი. სტუ-ს შრ.კრ., „მართვის ავტომატიზებული სისტემები", №1(19), გვ. 30-37.

3. 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", №1(21), გვ.70-77.

NON-STANDARD SYMMETRICAL CRYPTOGRAPHIC ALGORITHM OF INFORMATION ENCODING

Kutsiava Vasil, Kutsiava Ana, Gogoladze Giorge
Georgian Technical University

Summary

The paper describes encoding the block consisting from any number of symbols of ASCII or EBCDIC code represented by decimal system, using non-standard symmetrical cryptographic algorithm. Encoding process uses secret key with random value and random length, which is generated by the program with key forming algorithm. The encoding is performed using Visionery method (using the same key multiple times or auto key mode, where beginning open text or ciphered text is used as a secret key, after the main key is over).

НЕСТАНДАРТНЫЙ СИММЕТРИЧНЫЙ АЛГОРИТМ ШИФРОВАНИЯ ИНФОРМАЦИИ

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

Резюме

Рассмотрено шифрование блока данных, составленного из неограниченного количества символов ***ASCII*** или ***EBCDIC*** кодов, представленных в десятичной системе, с помощью алгоритма нестандартной симметричной криптосистемы. Шифрование производится секретным ключом, значение которого обеспечивается программно с использованием специального алгоритма и имеющего случайное значение и случайную длину. Шифрование осуществляется методом Виженера (многократное использование одного и тогоже ключа или режим автоключа, в котором используется исходный открытый текст или шифрованный текст после исчерпывания основного секретного ключа).