ინფორმაციის დაცვის მეთოდის დამუშავება საშუალო არითმეტიკულის გამოყენებით

გულნარა კოტრიკაძე, ნანული დანელია, გიორგი თაზიაშვილი
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

კრიპტოგრაფიაში არსებულ მეთოდებზე დაყრდნობით, შევიმუშავეთ ახალი მეთოდი, რომელშიც გარკვეული კანონზომიერებით ჩადებულია ქართული ანბანის ნუმერაცია ღია გასაღების სახით. საიდუმლო გასაღები გამოითვლება საშუალო არითმეტიკულის გამოყენებით. ამგვარად, გამოყენებულია როგორც ღია, ასევე საიდუმლო გასაღები, რომელსაც კანონიერი მომხმარებლები იღებენ გამოთვლების საფუძველზე ღია გასაღების გამოყენებით, ერთმანეთისაგან დამოუკიდებლად. გამოვთვალეთ სიმრავლე, ალბათობა და საიმედოობა, ანუ დავადგინეთ მეთოდის მედეგობა.

საკვანძო სიტყვები: კრიპტოგრაფია. საშუალო არითმეტიკული. მედეგობა.

1. შესავალი

კრიპტოგრაფიას დიდი ხნის ისტორია აქვს, თუმცა მისი თეორიული საფუძვლები, მხოლოდ XX საუკუნის პირველი ნახევრის ბოლოს იყო ჩამოყალიბებული კ. შენონისა და სხვა ავტორთა ნაშრომებში [1]. კრიპტო ... (ბერძნ. Kryptos - საიდუმლო, ფარული) ... გრაფია (ბერძნ. graho - ვწერ, ვხატავ, ვხაზავ) რთული სიტყვის ნაწილებია, ხოლო სიტყვა კრიპტოგრაფია (კრიპტო... და ... გრაფია) პირობითი საიდუმლო ნიშნებით წერას ნიშნავს [2].

კრიპტოგრაფია გახდა ერთ-ერთი ძირითადი საშუალება საიდუმლოების დასაცავად, საიმედოობისა და კონტროლისათვის, ელექტრონული გადარიცხვებისათვის, ორგანიზაციების დაცვისა და სხვა მრავალ სფეროში. რისთვის არის საჭირო ინფორმაციის დაცვა? რისი გაკეთება შეუძლია ინფორმაციის გამტაცებელს „ჰაკერი“? მას შეუძლია შეცვალოს ინფორმაცია თავისი მიზნებისათვის, გაიფართოვოს თავისი კანონიერი უფლებამოსილებანი, გაიგოს, ვის რა ინფორმაციასთან აქვს შეხება, შეუშალოს ხელი მომხმარებლებს შორის ინფორმაციის გაცვლას. კრიპტოგრაფია საიდუმლოს შენახვის მეცნიერებაა. კრიპტოანალიზი კოდის გატეხვის ხელოვნებაა, ე.ი. წერილის აღდგენა გასაღების წინასწარი ცოდნის გარეშე. კრიპტოგრაფიაში მომუშავე ადამიანებს კრიპტოგრაფები ეწოდებათ, ხოლო კრიპტოანალიზში მომუშავეებს - კრიპტოანალიტიკოსები [3].

2. ძირითადი ნაწილი

ინფორმაციის დასაცავად, სანამ შევიმუშავებდით ახალ მეთოდს, შევისწავლეთ არსებული მეთოდები, მათი მახასიათებლები და საიმედოობის ხარისხი. ზოგიერთ არსებულ მეთოდებში აღმოვაჩინეთ გარკვეული ნაკლოვანებები. მაგალითად როგორიცაა: უკუპროცესი (დაშიფრული ინფორმაციიდან საწყისამდე მისასვლელად უკუგზა არ უნდა არსებობდეს იგივე გზით და იგივე გასაღებით), დამოკიდებულება (დაშიფრულ ინფორმაციაში ყოველი მომდევნო არ უნდა იყოს დამოკიდებული წინა მონაცემებზე, რასაც იწვევს გასაღებში შემავალი პარამეტრების დამოკიდებულება). გარდა ამისა ზოგიერთი მეთოდები, იმ პირობების გათვალისწინებით, რომლებიც ცნობილია, ყოველთვის არ სრულდება, ანუ გარკვეული შეზღუდვებია საჭირო, რაც კიდევ უფრო უმარტივებს ინფორმაციის გამტაცებელს გაშიფრის პროცესს [4].

განვიხილეთ მრავალი ვარიანტი და ბოლოს მივიღეთ შემდეგი მეთოდი. გასაღების მიღების პროცესი: ავიღოთ ქართული ანბანი და დავნომროთ რიგითობით. მივიღეთ ერთი სტრიქონი 33 ციფრისაგან შემდგარი თანმიმდევრობით ჩაწერილი. შემდეგ ავიღეთ მეორე სტრიქონი და ჩაწერა ვაწარმოეთ ერთი პოზიციის წანაცვლებით, ანალოგიურად მოვიქეცით მესამე სტრიქონის შემთხვევაშიც და ა.შ. ანალოგიური გზით ჩავწერეთ 33 სტრიქონი, მივიღეთ 33/33–ზე კვადრატული მატრიცა, დიაგონალზე ერთიდაიგივე ციფრებისაგან შემდგარი (ნახ.1).

0	ა	ბ	გ	დ	ე	ვ	ზ	თ	ი	კ	ლ	მ	ნ	ო	პ	ჟ	რ	ს	ტ	უ	ფ	ქ	ღ	ყ	შ	ჩ	ც	ძ	წ	ჭ	ხ	ჯ	ჰ
ა	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
ბ	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	32
გ	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	32	31
დ	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	32	31	30
ე	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	32	31	30	29
ვ	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	32	31	30	29	28
ზ	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	32	31	30	29	28	27
თ	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	32	31	30	29	28	27	26
ი	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	32	31	30	29	28	27	26	25
კ	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	32	31	30	29	28	27	26	25	24
ლ	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	32	31	30	29	28	27	26	25	24	23
მ	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	32	31	30	29	28	27	26	25	24	23	22
ნ	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	32	31	30	29	28	27	26	25	24	23	22	21
ო	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	32	31	30	29	28	27	26	25	24	23	22	21	20
პ	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19
ჟ	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18
რ	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
ს	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
ტ	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15
უ	20	21	22	23	24	25	26	27	28	29	30	31	32	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14
ფ	21	22	23	24	25	26	27	28	29	30	31	32	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13
ქ	22	23	24	25	26	27	28	29	30	31	32	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12
ღ	23	24	25	26	27	28	29	30	31	32	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11
ყ	24	25	26	27	28	29	30	31	32	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10
შ	25	26	27	28	29	30	31	32	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9
ჩ	26	27	28	29	30	31	32	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8
ც	27	28	29	30	31	32	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7
ძ	28	29	30	31	32	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6
წ	29	30	31	32	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5
ჭ	30	31	32	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4
ხ	31	32	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3
ჯ	32	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2
ჰ	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

ნახ.1. ყველასათვის ცხობილი ღია გასაღები.

საბოლოო ჯამში მივიღეთ ქართულ ანბანზე აგებული ღია გასაღები და მიღებული მატრიცა განვაცხადეთ, ანუ ყველასათვის ცნობილია. აღნიშნული ღია გასაღების გამოყენებით კანონიერი მომხმარებლები, ერთმანეთისაგან დამოუკიდებლად, ითვლიან საიდუმლო გასაღებს, გარკვეული კანონზომიერების საფუძველზე, რომელიც მდგომარეობს შემდეგში: მატრიცა უნდა დავყოთ კვადრატებად 4/4–ზე, რომელიც შესაბამისად შეიცავს 16 ელემენტს, მიიღება 64 ასეთი კვადრატი. ცალკეული კვადრატებიდან უნდა გამოვთვალოთ საშუალო არითმეტიკული, მიიღება 4 კვადრატი 16–16 ციფრისაგან შემდგარი. ე.ი. სულ 64 ციფრი და ამ კვადრატების კვეთაზე მიიღება კიდევ 65–ე საერთო ციფრი (ნახ.2).

გასაღების მიღების პროცედურა: მიღებული საშუალო არითმეტიკულის (ნახ.2) კვადრატებიდან პირველ კვადრატის პირველ ელემენტს დავუმატებთ ერთს, შემდეგ მეორეს - ორს და ასე თანმიმდევრობით, ვიღებთ გასაღების პირველ კვადრატს. მეორე კვადრატის ელემენტებს ვუმატებთ მიღებული კვადრატის ელემენტებს პოზიციების მიხედვით თანმიმდევრობით და ვიღებთ გასაღების მეორე კვადრატს. რაც შეეხება მესამე და მეოთხე კვადრატებს, შეიძლება მივიღოთ ორი გზით: 1. რადგან თავდაპირველ ღია გასაღებში (ნახ.1) და ასევე საშუალო არითმეტიკულის კვადრატებში (ნახ.2) გვაქვს დიაგონალზე ერთიდაიგივე ელემენტები, ანალოგიურად პირველ და მეორე ცხრილში შემავალ ციფრებს უნდა შეიცავდეს ასევე მესამე და მეოთხე კვადრატებიც, ამიტომ მათი თანმიმდევრობის შებრუნებით დიაგონალზე, მიიღება მესამე და მეოთხე კვადრატები. 2. საშუალო არითმეტიკულის (ნახ.2) მეოთხე კვადრატის ელემენტებს, ქვედა მარჯვენა კუთხიდან, დაწყებული დავუმატოთ პირველ ციფრს ერთი, მეორეს - ორი და ა.შ. შესაბამისი თანმიმდევრობით, მივიღებთ მეოთხე კვადრატს. საშუალო არითმეტიკულის მესამე კვადრატს თუ დაუმატებთ მიღებულ მეოთხე კვადრატს გვაძლევს მესამე კვადრატს (ნახ.3).

4	8	12	16		21	25	29	32
8	12	16	20		25	29	32	29
12	16	20	24		29	32	29	25
16	20	24	28		32	29	25	21
				25				
21	25	29	32		28	24	20	16
25	29	32	29		24	20	16	12
29	32	29	25		20	16	12	8
32	29	25	21		16	12	8	4

ნახ.2. საშუალო არითმეტიკულების გამოყენებით ჩაწერილი კვადრატები

მაშასადამე, კანონიერი მომხმარებლები ერთმანეთისაგან დამოუკიდებლად იღებენ ერთიდა-იმავე საიდუმლო გასაღებს, 4 კვადრატსა და თანაკვეთას, საშუალო არითმეტიკულისა და გარკვეული კანონზომიერების საფუძველზე, სადაც პირველი და მეორე კვადრატის ელემენტებს შეიცავს მესამე და მეოთხე კვადრატის ელემენტები და თანაკვეთის ციფრი 25 საერთოა.

აღნიშნულიდან გამომდინარე, ერთ-ერთ მომხმარებელს შეუძლია გამოიყენოს, მაგალითად, პირველი და მეორე კვადრატები და მეორეს კი - მესამე და მეოთხე, ან პირიქით და კვეთა საერთოა. ე.ი. მიიღება ოცდაცამეტი ციფრისაგან შემდგარი გასაღები.

მიღებულ გასაღებს (ნახ.3) შევუსაბამოთ ქართული ანბანის ასოები და მიიღება გასაღები ჩაწერილი შესაბამისი ანბანის მიხედვით (ნახ.4).

5	10	15	20		26	35	45	52
13	18	23	28		38	47	55	57
21	26	31	36		50	58	60	62
29	34	39	44		61	63	64	65
				25				
65	64	63	61		44	39	34	29
62	60	58	50		36	31	26	21
57	55	47	38		28	23	18	13
52	45	35	26		20	15	10	5

ნახ.3. საიდუმლო გასაღები

ა	ბ	გ	დ		ს	ტ	უ	ფ
ე	ვ	ზ	თ		ქ	ღ	ყ	შ
ი	კ	ლ	მ		ჩ	ც	ძ	წ
ნ	ო	პ	ჟ		ჭ	ხ	ჯ	ჰ
				რ				
ჰ	ჯ	ხ	ჭ		ჟ	პ	ო	ნ
წ	ძ	ც	ჩ		მ	ლ	კ	ი
შ	ყ	ღ	ქ		თ	ზ	ვ	ე
ფ	უ	ტ	ს		დ	გ	ბ	ა

ნახ.4. ანბანის მიხედვით ჩაწერილი საიდუმლო გასაღები

განვიხილოთ კონკრეტული მაგალითი. ვთქვათ საწყისი ინფორმაცია არის:

„მე გავიმარჯვებ“.

გასაღების გამოყენებით ორივე მომხმარებელს შეუძლია ჩაწეროს ციფრების სახით, ანუ დაშიფროს, რასაც ექნება შემდეგი სახე: 36 13 15 5 18 21 5 25 64 18 13 10.

დაშიფრული ინფორმაცია განვაცხადეთ ღიად, ანუ გამატცებელმა ჩაიგდო ხელში. კანონიერი მომხმარებლები მათთვის ცნობილი გასაღების საფუძველზე, ინფორმაციის დეშიფრაციას მოახდენენ ძალიან სწრაფად და მარტივად. ინფორმაციის გამტაცებელს დაშიფრული ინფორმაციიდან გაუჭირდება საწყისი ინფორმაციის მიღება, რადგან მან არ იცის გასაღები.

ყველა შესაძლო ვარიანტი უნდა გაიაროს ყველა ასოს ამოცნობაში და ყოველ მომდევნოსთან მოიყვანოს კომბინაციაში, რასაც საკმაოდ ბევრი დრო დასჭირდება, რის გამოც ინფორმაცია აზრს დაკარგავს. გარდა ამისა, გასაღებში შემავალი ციფრებიდან ნაწილი ღია ცხრილში არ ფიგურირებს და ნაწილი კი ძალიან ბევრჯერ მეორდება და მათ სხვადასხვა ასოები შეესაბამება. ასევე, ერთი სიტყვა თუ ამოიცნო არ ნიშნავს იმას, რომ მომდევნოც ეცოდინება.

3. დასკვნა

- კრიპტოგრაფიის უკვე არსებულ მეთოდებში არის ნაკლოვანებები, როგორიცაა: უკუგზა გაშიფვრის დროს, ერთიდაიგივე გასაღები დასაშიფრად და გასაშიფრად, დამოკიდებულება, ნამდვილობის უარყოფა და ა.შ.;

- შევიმუშავეთ ახალი მეთოდი, სადაც გამოყენებულია, როგორც ღია, ასევე საიდუმლო გასაღები, გარკვეული კანონზომიერების საფუძველზე მიღებული;

- ორივე კანონიერი მომხმარებელი ერთმანეთისაგან დამოუკიდებლად იღებს ერთიდაიმავე საიდუმლო გასაღებს, გაცხადებულ გასაღებზე დაყრდნობით, საშუალო არითმეტიკულის გამოყენებით, რომელიც შეიცავს აბსოლუტურად განსხვავებულ ციფრებს და გასაღების არცერთი ციფრი არ მეორდება;

- მიღებული მეთოდი არის მაქსიმალურად დაცული და მესამე პირისათვის, რეალურ დროში, შეუძლებელია, ჩვენს მიღებული მეთოდით, დაშიფრული ინფორმაციის გატეხვა.

ლიტერატურა:

1. Шнайер Б. (2003). Прикладная криптография. М., Изд. “Триумф”.
2. მეგრელიშვილი რ. (2009). ინფორმაციის დაცვის სისტემები, თსუ.
3. კუციავა ვ., კაცაძე გ., დიაკონიძე ქ. (2005). ინფორმაციის დაცვა, სტუ, ,,ტექნიკური უნივერსიტეტი”.
4. ყიფშიძე ზ., ანანიაშვილი გ. (2003). ინფორმაციის თეორია, კოდირება და სინერგეტიკა. თსუ.

PROCESSING THE METHOD OF INFORMATION PROTECTION USING AVERAGE

Kotrikadze Gulnara, Danelia Nanuli, Taziashvili Giorgi

Georgian Technical University

Summary

The work is about describing Cryptography in general. Based on the existing methods, we have developed a new method which with some regularity includes Georgian alphabet numbering in the form of the public key. The secret key is calculated by using the average. This means that both the public and the secret keys are used. The rightful users receive both keys independently from each other on the basis of calculations and by using the public key. We have also calculated the set, the probability and the reliability. In another words, we identified the endurance of the method.

РАЗРАБОТКА СПОСОБА ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ СРЕДНЕГО ВЫЧИСЛЕНИЯ

Котрикадзе Г., Данелия **Н.**, **Тазиашвили Г.**

Грузинский Технический Университет

Резюме

Описываются методы криптографии. На основе существующих методов разработан новый метод, в который заложена с определенной закономерностью нумерация грузинского алфавита в виде открытого ключа, а секретный ключ вычисляется применением среднего арифметического. Т.е. применен как открытый, так и секретный ключ, который пользователь получает с помощью вычислений. Приведена оценка надежности метода.