ინფორმაციის დაცვის მეთოდის დამუშავება რიცხვთა გაბნევით

გულნარა კოტრიკაძე, ნანული დანელია, გიორგი თაზიაშვილი
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

შევისწავლეთ კრიპტოგრაფია და აღნიშნულის საფუძველზე, მივედით დასკვნამდე, რომ მიგვეღო ახალი ორიგინალური მეთოდი, რომელიც იქნებოდა გამორჩეული მაღალი საიმედოობით. გამოვიყენეთ ღია გასაღები ნებისმიერი ტექსტის სახით, რომლის საფუძველზეც კანონიერი მომხმარებლები იღებენ საიდუმლო გასაღებს, ღია ტექსტის თანმიმდევრობითი დანომრვითა და რიცხვთა გაბნევით. გამოვთვალეთ სიმრავლე, ალბათობა და საიმედოობა.

საკვანძო სიტყვები: კრიპტოგრაფია. ღია ტექსტი. რიცხვთა გაბნევა. საიმედოობა.

1. შესავალი

კრიპტოგრაფიას დიდი ხნის ისტორია აქვს. მას ჯერ კიდევ ცეზარის დროს იყენებდნენ სამხედრო საქმიანობის წარმართვისათვის. თუმცა მისი თეორიული საფუძვლები, მხოლოდ XX საუკუნის პირველი ნახევრის ბოლოს იყო ჩამოყალიბებული კლოდ შენონისა და სხვა ავტორთა ნაშრომებში [1,5].

კრიპტოგრაფიული ტერმინოლოგიით ადრესატისადმი გასაგზავნ წერილს (ჩვეულებრივ შეტყობინებას) ეწოდება დაუშიფრავი ან ღია ტექსტი. წერილის ისეთი სახით კოდირებას, რომლის დროსაც საიდუმლო ხდება ტექსტის შინაარსი გარკვეული კოდირების გამოყენებით, ეწოდება დაშიფვრა, კოდირებულ ტექსტს - დაშიფრული ტექსტი. დაშიფრული ტექსტიდან საწყისი ტექსტის აღდგენას - დეშიფრაცია [2,4]. დაშიფვრისა და გაშიფვრის (დეშიფრაციის) შემთხვევაში ადგილი აქვს ტექსტის გარდაქმნას განსაზღვრული ალგორითმის შესაბამისად. გარდაქმნის ტიპი ამოირჩევა გარდაქმნების სიმრავლიდან, რომელიც ქმნის კრიპტოგრაფიულ სისტემას. სისტემის ნაწილს, რომელიც ახორციელებს ინფორმაციული ტექსტის კონკრეტული გარდაქმნის კოდს, ეწოდება გასაღები. როგორც წესი (თუმცა, არა ყოველთვის), გასაღების სიგრძე გაცილებით ნაკლებია ტექსტის სიგრძეზე [3].

2. ძირითადი ნაწილი

ჩვენს მიერ მიღებული ახალი მეთოდი.

ავიღეთ ნებისმიერი ტექსტი და დავნომრეთ თანმიმდევრობით თავისი გამოტოვებით, სასვენი ნიშნებით და მივიღეთ მატრიცა, რომელიც შეიცავს 33 სვეტს და 33 სტრიქონს და გავჩერდით, რადგან 33/33-ზე მატრიცა საკმარისია საიმედოობისათვის. თუმცა შეგვიძლია გავაგრძელოთ გასაღების სტრიქონთა რაოდენობა, რადგან არ მოხდეს გამეორება, თუმცა არც გამეორება აიოლებს ჰაკერისათვის საქმეს. ე.ი. მივიღეთ გასაღები 33/33-ზე (ნახ.1). მიღებული გასაღები ანუ ამ შემთხვევაში მხოლოდ ტექსტი, ნუმერაციის გარეშე, რომელიც გარკვეული დროის შემდეგ უნდა შეიცვალოს, განვაცხადეთ, ანუ ყველასათვის ცნობილია, თუმცა რიცხვთა ამორჩევის კანონზომიერება იცის მხოლოდ კანონიერმა მომხმარებლებმა.

გასაღები შევადგინეთ შემდეგნაირად: აღნიშნულ ღია ტექსტში (შემდგომში ღია გასაღები), ხდება ასოების დანომრვა, ასოებს ვანიჭებთ სხვადასხვა ციფრებს, მისი ადგილმდებარეობიდან გამომდინარე. მაგალითად: ასო „ა“-ს პირველად მიენიჭა ციფრი 11, შემდეგ - 25 და ა.შ., ანალოგიურად - სხვა დანარჩენ ასოებსაც. მიღებული გასაღებიდან ამოვარჩიეთ, ასოების მიხედვით, მათი ნუმერაციები ანუ ყველა შესაძლო ვარიანტი. თვალსაჩინოებისათვის, ავიღოთ ასო „ა“, რომელსაც შეესაბამება აბსოლუტურად ერთმანეთისაგან დამოუკიდებლი სხვადასხვა ციფრები, ასევე სხვა დანარჩენ ასოებსაც (ნახ.2).

მ	ო	გ	ე	ზ	ს	ე	ნ	ე	ბ	ა	თ	,
1	2	3	4	5	6	7	8	9	10	11	12	13
	რ	ო	მ		ი	ნ	ფ	ო	რ	მ	ა	ც
14	15	16	17	18	19	20	21	22	23	24	25	26
ი	ი	ს		დ	ა	ც	ვ	ა	-	დ	ა	ს
27	28	29	30	31	32	33	34	35	36	37	38	39
ა	ი	დ	უ	მ	ლ	ო	ე	ბ	ა	,		ა
40	41	42	43	44	45	46	47	48	49	50	51	52
რ	ი	ს		ს	ა	კ	მ	ა	ო	დ		ა
53	54	55	56	57	58	59	60	61	62	63	64	65
ქ	ტ	უ	ა	ლ	უ	რ	ი		თ	ე	მ	ა

ნახ.1. ღია გასაღები, ნებისმიერი ტექსტი (ნაწილი 33/33-ზე მატრიციდან)

ა																
11	25	32	35	38	40	49	52	58	61	65	69	76	101	107	110	120
270	286	290	297	302	304	310	324	338	340	393	412	414	422	432	434	440
597	612	619	622	625	631	635	637	645	647	655	658	660	668	670	676	686

ბ								
10	48	100	114	128	191	228	238	266
943	969	979	997	1000	1028	1045	1078	1080

ნახ.2. ღია გასაღებიდან ასოების ამორჩევა, საიდუმლო გასაღების გენერირება (ნაწილი)

განვიხილოთ თუ როგორ ხდება ინფორმაციის დაშიფვრა აღნიშნული გასაღებით. ვთქვათ საწყისი ინფორმაცია არის - „გამარჯობათ. ხვალ ჩამოვდივარ საქართველოში და უნდა გნახოთ აუცილებლად". მიღებული გასაღების გამოყენებით ასოებს თანმიმდევრობით მივანიჭოთ ღია გასაღებში მინიჭებული ციფრები, შესაძლებელია როგორც თანმიმდევრობით ასევე გაბნევით (ნებისმიერად), მივიღებთ შემდეგი სახის დაშიფრულ ინფორმაციას:

3 11 1 25 15 17 2 10 32 12 138 5 34 35 45 483 38 24 16 85 31 19 97 49 23 6 52 66 58 53 79 111 4 70 22 102 37 61 43 8 42 65 119 20 69 80 46 109 76 68 26 27 87 7 48 179 101 63 195

მივიღეთ საბოლოო სახის დაშიფრული ინფორმაცია. იგი მოვათავსეთ მართკუთხედში გარკვეული კანონზომიერებით (ნახ.3), რომელიც იგზავნება მეორე მომხმარებელთან ღია არხით, ანუ გამტაცებლისათვის ხელმისაწვდომია (ნახ.4). ე.ი. ჰაკერმა იცის ღია გასაღები (ნებისმიერი ტექსტი) ნახ.1 და დაშიფრული ინფორმაცია ნახ.4. მისთვის უცნობია მხოლოდ, დაშიფვრისა და მართკუთხედში ჩაწერის კანონზომიერება.

	3								
11				1		25	15		
	17				2				10
			32				12		
	138								
		5			34	35			45

483			38	24			16		
								85	
		31				19			
97				49				23	
		6	52		66				58
								53	

								79	
		111	4		70				22
102				37				61	
		43				8			
								42	
65			119	20			69		

		80			46	109			76
	68								
			26				27		
	87				7				48
179				101		63	195		
	195								

ნახ.3. დაშიფრული ინფორმაციის მართკუთხედში ჩაწერის კანონზომიერება

დეშიფრაციისათვის მეორე, კანონიერი მომხმარებელი, რომელიც ფლობს კანონზომიერებას, ჰაკერისაგან განსხვავებით, მიღებულ დაშიფრულ ინფორმაციას ციფრების სახით, მართკუთხედიდან, შემდეგ მატრიციდან შეუსაბამებს ასოებს და მიიღებს საწყის ინფორმაციას.

483	3	80	38	24	46	109	16	79	76
11	68	11	4	1	70	25	15	85	22
102	17	31	26	37	2	19	27	61	10
97	87	43	32	49	7	8	12	23	48
179	138	6	52	101	66	63	195	42	58
65	195	5	119	20	34	35	69	53	45

ნახ.4. დაშიფრული ინფორმაციის საბოლოო სახე

რაც შეეხება გამტაცებელს, მან იცის დაშიფრული ინფორმაცია და ღია ტექსტი, იგი შეეცდება მიმართოს ყველა გზას. მაგალითად: ვთქვათ დანომრა ღია გასაღები, რადგან გასაღებში გამოიყენება ოთხნიშნა რიცხვებიც, გააჩნია დასაშიფრი ინფორმაციის ზომაც, ამიტომ იგი გამოყოფს მაქსიმუმ ყოველ 4 ციფრს (თუმცა ციფრებით არ ხდება გასაღების გავრცელება) და გაივლის ყველა შესაძლოს, რაც შეადგენს ერთი ასოს ამოცნობისათვის 16 ვარიანტს. ე.ი. ერთი ასოს ამოცნობაში 16 ოპერაცია არის საჭირო, ყოველი ოთხი ციფრიდან რომ ამოიცნოს და ამის შემდეგ, ყოველ მომდევნოსთან მისი კომბინაცია, ეს კი გაცილებით დიდი რიცხვია $16\times1089!$. თუმცა ყოველი ოთხი ციფრიდან ამორჩევა არ გამოადგება, შესაძლოა იყოს სამი ციფრი ერთად აღებული, ან ნაკლები, მაშინ დარჩენილი მეოთხე ციფრი, მომდევნო ციფრებთან უნდა მოიყვანოს კომბინაციაში და ა.შ.

ე.ი. შეგვიძლია ვთქვათ, რომ სიმრავლე იქნება $n\times1089!$, სადაც n არის ყველა განსხვავებული შემთხვევა აღებული ღია გასაღებიდან, (იხ.ნახ.1), ხოლო გატეხვის ალბათობა - $1/n\times1089!$. კრიპტოგრაფიაში საიმედოობის ქვედა ზღვარი შეიძლება ვთქვათ, რომ არის $\cong 2^{100} \cong 10^{30}$. მიღებული რიცხვი კი გაცილებით აღემატება ქვედა ზღვარს, რის საფუძველზეც შეგვიძლია ვთქვათ, რომ მეთოდი საიმედოა.

3. დასკვნა

- არსებულ მეთოდებში აღმოვაჩინეთ გარკვეული ნაკლოვანებები, როგორიცაა: დაბალი საიმედოობა, დაბალი სიჩქარე, გარკვეული შეზღუდვები;
- შევიმუშავეთ ახალი მეთოდი, რომელიც დაყრდნობილია ქართულ ანბანზე, თუმცა სხვა ანბანისთვისაც მისაღებია;
- მიღებული მეთოდი მიეკუთვნება ასიმეტრიულ სისტემას. გამოიყენება როგორც ღია გასაღები, ასევე საიდუმლო გასაღებიც;
- ინფორმაციის დასაშიფრად გამოვიყენეთ გასაღები – ღია ტექსტისა და მართკუთხედის სახით და სხვადასხვა კანონზომიერებები;
- დაშიფრული ინფორმაცია იგზავნება ღია არხით, ყველასათვის ხელმისაწვდომია, თუმცა მესამე პირისათვის შეუძლებელია რეალურ დროში მისი გატეხვა;
- მიღებული მეთოდი მაქსიმალურად დაცულია, რასაც გვიდასტურებს სიმრავლე.

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.
5. Касами Т., Токура Н., Ивадари Е., Инагаки Я. (1978). Теория кодирования. М., “Мир”.

PROCESSING THE METHOD OF INFORMATION PROTECTION BY SCATTERING THE NUMBERS

Kotrikadze Gulnara, Danelia Nanuli, Taziashvili Giorgi

Summary

As we have examined and studied the Cryptography with its methods, our goal has become to receive new methods without the disadvantages which had been in the existing, well-known methods before. In addition, our desire was our method to be the original and different from the other methods. We used the public key with any form of text and based on this the rightful users would receive the secret key by successively numbering the open text and by scattering the numbers.We also calculated the set, the probability and the reliability.

РАЗРАБОТКА МЕТОДА ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ РАССЕЯНИЯ ЧИСЕЛ

Котрикадзе Г., Данелия Н., Тазиашвили Г.
Грузинский Технический Университет

Резюме

Изучив методы криптографии, пришли к выводу, чтобы разработать новый оригинальный метод с высокой надежностью. Используется открытый ключ в качестве любого текста, на основе которого законные пользователи получают секретный ключ, с последовательной нумерацией открытого текста и рассеянием чисел. Представлены расчеты множества, вероятностей и надежности.