რიცხვთა წონის მიხედვით ინფორმაციის დაცვის მეთოდის დამუშავება

გულნარა კოტრიკაძე, თაბუკა ციმინტია
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

მიღებულია დახურული არხის ახალი მეთოდი, რომელიც მომხმარებლებისთვის, არის სწრაფი და გასაშიფრადაც მარტივია. ამავდროულად, მესამე პირისთვის „ჰაკერისთვის" რთულად გასატეხია, ანუ მაქსიმალურად დაცული სხვა არაკანონიერი მომხმარებლებისაგან. მიმღებ მხარეს შეუძლია დაადგინოს მიღებული დაშიფრული ტექსტის ნამდვილობა. აღნიშნული მეთოდის მისაღებად კი გამოყენებულია რიცხვთა წონები.

საკვანძო სიტყვები: დაცვა. სიმეტრიული. გასაღები. რიცხვთა წონები.

1. შესავალი

რისთვისაა საჭირო ინფორმაციის დაცვა ? რისი გაკეთება შეუძლია ინფორმაციის გამტაცებელს – „ჰაკერს" ? მას შეუძლია შეცვალოს ინფორმაცია თავისი მიზნებისათვის, გაიფართოვოს თავისი კანონიერი უფლებამოსილებანი. გაიგოს, ვის რა ინფორმაციასთან აქვს შეხება, შეუშალოს ხელი მომხმარებლებს შორის ინფორმაციის გაცვლას.

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. 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. უმეტეს შემთხვევებში გასაღების სიგრძე გაცილებით ნაკლებია ტექსტის სიგრძეზე.

კრიპტოგრაფია საიდუმლოს შენახვის მეცნიერებაა. კრიპტოანალიზი – კოდის გატეხვის ხელოვნებაა, ე.ი. ნაწერის აღდგენა გასაღების წინასწარი ცოდნის გარეშე. კრიპტოგრაფიაში მომუშავე ადამიანებს კრიპტოგრაფები ეწოდებათ, ხოლო კრიპტოანალიზში მომუშავეებს – კრიპტოანალიტიკოსები.

2. ძირითადი ნაწილი

2.1. რიცხვთა წონის გამოყენება ინფორმაციის დაცვისათვის

გავეცანით და შევისწავლეთ ყველა არსებული მეთოდი, როგორც დახურული, ასევე ღია არხის მეთოდები, დავადგინეთ მათი მახასიათებლები და პარამეტრები. დახურული და ღია არხის ყველა მეთოდი შევადარეთ ერთმანეთს მახასიათებლების მიხედვით.

ზემოაღნიშნულიდან გამომდინარე, დაისვა ამოცანა: შეგვექმნა სიმეტრიული, ანუ დახურული არხის ისეთი მეთოდი, რომელიც თვით მომხმარებლებისათვის, როგორც დასაშიფრად, ასევე გასაშიფრად იქნებოდა სწრაფი და მარტივი, მაგრამ ამავდროულად, მესამე პირისათვის („ჰაკერი") იქნებოდა რთულად „გასატეხი", ანუ მაქსიმალურად დაცული სხვა არაკანონიერი მომხმარებლებისაგან. ასევე მიმღები მხარე დაადგენდა მიღებული დაშიფრული ტექსტის ნამდვილობას [1-3].

2.2. მიღებული მეთოდი ორობით სისტემაში

ამოცანა მიეკუთვნება სიმეტრიულ სისტემებს. დავუშვათ, საწყისი მომხმარებელია X, მიმღები კი –Y. როგორც უკვე აღვნიშნეთ, ეს მეთოდი მიეკუთვნება დახურულ არხს, რაც ნიშნავს, რომ გამოიყენება გასაღები, რომელსაც ირჩევს საწყისი მომხმარებელი და საიდუმლოდ, დახურული გზით, აწვდის მეორე მომხმარებელს, ანუ მიმღებ მხარეს, გასაღები არის ორობითი სახის (გამოთვლა ხდება GF(2) ველზე). ასევე ორივე მომხმარებლისათვის წინასწარ ცნობილია რიცხვის წონის განსაზღვრის ხერხი, რომელიც გამოიყენება მეთოდში, ნამდვილობის შესამოწმებლად. მაშასადამე, გამოიყენება ორი სახის გასაღები, აქედან ერთი გამოიყენება დასაშიფრად, ხოლო მეორე კი ტექსტის ნამდვილობის შესამოწმებლად და დაშიფვრის საბოლოო სახე დადის ორობითზე [3,4].

განვსაზღვროთ რიცხვის წონა. მაგალითად: რიცხვი 14 გადავიყვანოთ ორობითში 14=1110, დავთვალოთ ორობით ჩანაწერში რამდენი ერთიანია. ამ შემთხვევაში არის 3, ე.ი. 14 ის წონა არის 3(4) – დან. ამის შემდგომ მიღებულს შევხედოთ როგორც რიცხვებს და ცალცალკე გადავიყვანოთ ორობითში და მივიღებთ 3=11 და 4=100 და ჩავწეროთ ასეთი სახით 11(100), ე.ი. 14–ის წონა მივიღეთ 11(100). მიღებული კი გამოიყენება დაშიფრული ტექსტის ნამდვილობის და სიმბოლოების რაოდენობის დასამოწმებლად. მოვიყვანოთ მაგალითი, რათა აღნიშნული მეთოდი უფრო მკაფიო და გასაგები გახდეს.

X მხარე აგზავნის წერილს, წერილიდან ამ ეტაპზე ამოვიღოთ ერთი სიტყვა და ეს სიტყვა იყოს, ვთქვათ: გ ე პ ე ი. X მხარეს ეს დასაშიფრი სიტყვა გადაჰყავს ათობითში, ათვლას იწყებს 0-დან ანუ ა=0, ყოველ სიმბოლოს შეუსაბამებს ანბანის რიგით ნომერს და მიიღებს: 2 4 14 4 8.

- შემდგომ მიღებული გადაჰყავს ორობითში და მიიღებს: 2=10 4=100 14=1110 4=100 8=1000;
- მიღებულ ჩანაწერს შეუსაბამებთ წონებს, ზემო აღნიშნულიდან გამომდინარე და მივიღებთ: 1θ2θ 1θ3θ 3θ4θ 1θ3θ 1θ4θ;
- ამის შემდეგ, მიღებული წონები გადაგვყავს ორობითში, შესაბამისად გვექნება: 1θ10θ 1θ11θ 11θ100θ 1θ11θ 1θ100θ;
- შემდეგ ჩაწერას განვახორციელებთ შემდეგნაირად: რიცხვის წონა θ, სიმბოლოების რაოდენობა θ, ანუ სიტყვა გ ე პ ე ი მიიღებს ასეთ სახეს: 101θ10θ 100θ11θ 11101θ100θ 100θ11θ 100θ1θ100θ
- ამის შემდეგ, ვიყენებთ დასაშიფრ გასაღებს: 110θ10θ 0011θ01θ 10111θ00111θ 100θ000θ 1101θ0111 და მიღებულს ვუმატებთ, შესაბამისად მივიღებთ: 011θ000θ 1010θ10θ 01010θ1111θ 0000θ11θ 0101θ1111θ;
- საბოლოო სახით ჩაწერილი დაშიფრული ტექსტი. 101θ10θ-დან – θ10θ – სიმბოლოების რაოდენობა, 1 – რიცხვის წონა (ანუ „ერთიანების რაოდენობა“), 10 – რიცხვი.
- მიღებულს უგზავნის მეორე მომხმარებელს, ანუ მიმღებ მხარეს - კანონიერ მომხმარებელს, რომელიც ადვილად და სწრაფად ახდენს მის გაშიფრვას შემდეგნაირად:

1-ეტაპი: მიღებულს გამოაკლებს გასაღებს და მიიღებს: 101θ10θ 100θ11θ 11101θ100θ 100θ11θ 1000θ100θ;

2-ეტაპი: სიმბოლოების რაოდენობას ანუ ყოველ მეორე (θθ) – ამ სიმბოლოებს შორის, გადაიყვანს ათობითში და რა ციფრსაც მიიღებს, იმ რაოდენობის სიმბოლოებს აიღებს წინა ჩანაწერიდან და ათვლას დაიწყებს თავიდან, თანაც დარჩენილი სიმბოლოები კი აღნიშნავს საწყისის წონას. ანუ მიმღები მხარე წონის პარამეტრების მიხედვით ადგენს ყოველ ასონიშანში შემავალ სიმბოლოების რაოდენობას და ამავდროულად მის წონას. მაშასადამე, ამტკიცებს მიღებული ინფორმაციის ნამდვილობას [5,6];

3-ეტაპი: მიღებულ ორობითს გადაიყვანს ათობითში, შემდგომ შეუსაბამებს ანბანის შესაბამის ასონიშნებს და მიიღებს სიტყვას ანუ გაშიფრავს, მოახდენს მის დეშიფრაციას;

ახლა კი რაც შეეხება არაკანონიერ მომხმარებელს ანუ ჰაკერს;

აღნიშნულ მეთოდში გასაღების სიგრძე არის 100, სიმრავლე იქნება 2^{100}, ამ სიმრავლიდან კონკრეტული გასაღების ამორჩევას, უხეში ძალით ამორჩევით, რამდენიმე წელი დასჭირდება, ასევე რაც ხარჯებთან და დიდ დროსთან არის დაკავშირებული. 2^{128} გადარჩევას დასჭირდება $\approx 10^{18}$ ჯ. ენერგია, რაც 1 წლის განმავლობაში დახარჯული 30 გიგავატი სიმძლავრის ენერგიის ტოლფასია. მაგრამ, თუკი „ჰაკერი” მიუდგება ამ მეთოდს არა უხეში ძალის გატეხვის პრინციპით, არამედ სხვა კუთხით, მაშინ, რადგან ქართულში გვაქვს 33 ასონიშანი, თითოეულ ორობითს უნდა შეუსაბამოს რიგითი ნომერი. ორობითი უნდა გადავიყვანოთ ათობითში. მაქსიმალური სიმრავლე იქნება 2^6, მაგრამ „ჰაკერმა” არ იცის რამდენი სიმბოლო უნდა აიღოს თითოეული ასონიშნის ამოსაცნობად, ანუ გადარჩევა უნდა გააკეთოს სიმრავლიდან. აქედან გამომდინარე, ჩასატარებელი ოპერაციები გაიზრდება და გარდა ამისა, სიმრავლის დადგენის მერე, კომბინაციებიც ექნება დასადგენი და ეს ყველაფერი უნდა გააკეთოს თითოეული სიმბოლოს ამოსარჩევად. ამით ჩასატარებელი ოპერაციების რაოდენობა კიდევ უფრო გაიზრდება და იქნება $\approx \left(\sum_{n=1}^{6} 2^6\right)! \bullet 33 \bullet n$. ეს საკმაოდ დიდი რიცხვია, იმისათვის რომ ჰაკერმა რეალურ დროში მოახდინოს ტექსტის ამოცნობა.

ე.ი. უხეში ძალის მეთოდით გატეხვის შემთხვევაში სიმრავლე კიდევ უფრო გაიზრდება და კატასტროფულ რიცხვს მიაღწევს $\approx 2^{100} + \left(\sum_{n=1}^{6} 2^6\right)! \bullet 33 \bullet n$; $\left(\sum_{n=1}^{6} 2^6\right)! = 127!$ - ეს კი ძალიან დიდი რიცხვია $127! > 2^{127}$ – ზე, 2^{128} – ის გატეხვას კი სჭირდება $\approx$ 10,790,283,070,806 წელი. მეთოდი არის ადვილი, მარტივად და სწრაფად დასაშიფრი, მიმღები მხარისათვისაც სწრაფად გასაშიფრი და ამავდროულად, ჰაკერისაგან მაქსიმალურად დაცული (ნახ.1) [6].

2.3. მიღებული მეთოდი ათობით სისტემაში

აღნიშნული მეთოდი შეგვიძლია ასევე განვახორციელეოდ ათობითი სახით. მოვიყვანოთ შესაბამისი მაგალითი:

X მხარე აგზავნის წერილს, წერილიდან ამ ეტაპზე ამოვიღოთ ერთი სიტყვა და ეს სიტყვა იყოს, ვთქვათ გ ე პ ე ი. X მხარეს ეს დასაშიფრი სიტყვა გადაჰყავს ათობითში, ათვლას იწყებს 1-დან ანუ ა=1, ყოველ სიმბოლოს შეუსაბამებს ანბანის რიგით ნომერს და მიიღებს: 3 5 15 5 9;

შემდგომ იყენებს რიცხვის წონას. ორობითში, წონის სახით, ჩვენ ავიღეთ ერთიანების რაოდენობა, ათობითში ეს არ გამოგვადგება. ამიტომ ათობითში წონა იქნება რიცხვების ჯამი, ანუ

მაგალითად, 3–ის წონა იქნება 3, 9-ის წონა იქნება 9, 13-ის წონა იქნება 4, 25-ის წონა იქნება 7, და ა.შ. მიღებული რიცხვები კი, წონის გამოყენებით, ჩაიწერება შემდეგი სახით: 3 5 6 5 9;

წონის გამოყენებით ჩაწერა კი მოხდება შემდეგნაირად: 3*3 5*5 15*6 5*5 9*9;

მიღებული შეიძლება ჩავწეროთ შემდეგნაირად:

1*(3+2)*3 1*(5+4)*5 5*(3+3)*6 1*(5-2)*5 3*(3-3)*9

1*(3+2)*3 – აღნიშნული ჩანაწერი ნიშნავს: 1*(3 – საწყისი რიცხვი; +2 – შემთხვევითი რიცხვი; *3 – რიცხვის წონა;

მიღებულს დაემატება კიდევ საიდუმლო გასაღები და მივიღებთ:

1*(3+2)*3 1*(5+4)*5 5*(3+3)*6 1*(5-2)*5 3*(3-3)*9

1*(1+2)*2 2*(2-1)*3 5*(4+3)*5 1*(6-2)*5 7*(4-3)*7

გამრავლების ნიშანი სიმბოლურად არის ჩასმული, გამოთვლის დროს არ გამოიყენება, შევკრიბოთ და მივიღებთ:

2*(4+4)*5 3*(7+5)*8 10*(7+6)*11 2*(11-4)*10 10*(7-6)*16

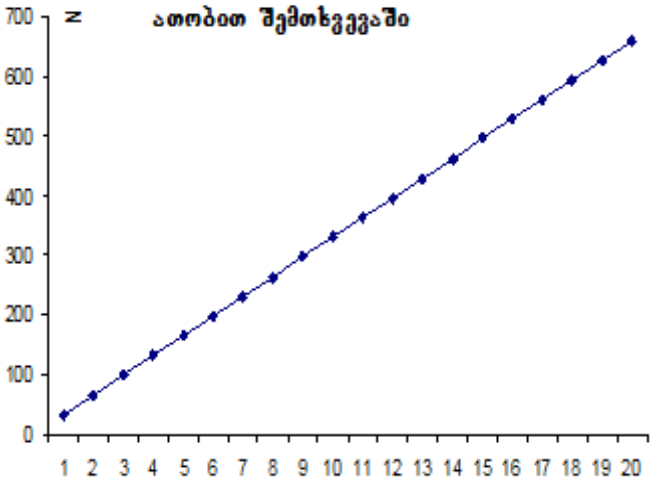
მივიღეთ საბოლოო ფორმა დაშიფრული ტექსტის და გაუგზავნეთ მეორე მომხმარებელს ღია არხით.

მიმღები მხარე მიღებულ ციფრებს გამოაკლებს მისთვის ცნობილ, ანუ საიდუმლოდ მიღებულ გასაღებს და მიიღებს

1*(3+2)*3 1*(5+4)*5 5*(3+3)*6 1*(5-2)*5 3*(3-3)*9

აქ კი მომხმარებელი ბევრ დროს არ დახარჯავს. მან იცის რა პრინციპით არის ჩაწერილი, ის რომ მათემატიკური მოქმედებები ზედმეტად არის ჩასმული, ანუ სიმბოლურად, ანუ მას რაიმე დატვირთვა არა აქვს. წონის მიხედვით დაადგენს მის ნამდვილობას, დარწმუნდება რომ არ არის შეცვლილი. მერე აიღებს ყოველ მესამე ელემენტს თანმიმდევრობით, შეუსაბამებს ანბანის ასონიშნებს და მიიღებს საწყის სიტყვას ანუ გაშიფრავს. ამ ყველაფერს, ანუ გაშიფვრას წამებში გააკეთებს [5,6,7].

რაც შეეხება „ჰაკერს", ანუ რამდენად საიმედოა მეთოდი [7,8]. რადგან საქმე გვაქვს ათობით ციფრებთან, ამიტომ გასაღების სიგრძე უნდა იყოს 30-ის ტოლი, სიმრავლე იქნება 10^{30}, ეს კი კრიპტოგრაფიაში არის საკმარისი სიმრავლე საიმედოობისათვის $2^{100} \approx 10^{30}$, "ჰაკერმა" ამ სიმრავლიდან უნდა ამოარჩიოს გასაღები, ეს იმ შემთხვევაში თუ „ჰაკერი" გამოიყენებს უხეში გატეხვის მეთოდს, სხვა შემთხვევაში კი მიღებულ დაშიფრულ ტექსტში უნდა დაადგინოს კომბინაციები, ამისათვის მან უნდა ჩაატაროს $(\sum_{k=1}^{33} K)!\bullet n$ ოპერაცია. ე.ი თუ უხეში გატეხვის მეთოდს მიჰყვება მას დასჭირდება დიდი დრო და ჩასატარებელი ოპერაციების რაოდენობა იქნება $\approx 10^{30} + (\sum_{k=1}^{33} K)!\bullet n$ (იხ. ნახ.2, ცხრ.1).



ნახ.2. ათობითი სახით დაშიფრის შემთხვევაში ტექსტის სიმბოლოების დამოკიდებულება ჩასატარებელი ოპერაციების რაოდენობასთან

არსებული და მიღებული სიმეტრიული სისტემების მახასიათებლები ცხრ.1

სიმეტრ. სისტ.	გამოყ. ფუნქც.	შიფრაციის სიჩქარე	ჩასატარებელი ოპერაც. რაოდენობა	რიპტო-სირთულე	გაშიფვრის დრო
ვერნამის მეთოდი	სიმეტ.	მაღალი	$33! * n$	გასაღ. სივრცეში მთლიანი გადარ.	$> 6.4 \times 10^{6}$ წელი
შებრუნ. მატრიც. მეთოდი	სიმეტ.	შედარებით დაბალი	2^{100}	გასაღ. სივრცეში მთლიანი გადარ.	$< 5.4 \times 10^{18}$ წელი
რიცხვთა წონის მეთოდი ორობითში	სიმეტ.	მაღალი	$2^{100} + \left(\sum_{n=1}^{6} 2^{6}\right) \bullet 33 \bullet n$	გასაღ. სივრცეში მთლიანი გადარ. და კომბინაციების დადგენა	$>> 5.9 \times 10^{30}$ წელი
რიცხვთა წონის მეთოდი ათობითში	სიმეტ.	მაღალი	$10^{30} + (\sum_{k=1}^{33} K)! \bullet n$	გასაღ. სივრცეში მთლიანი გადარ. და კომბინაციების დადგენა	$> 5.9 \times 10^{30}$ წელი

3. დასკვნა

მივიღეთ სიმეტრიული არხის ისეთი მეთოდი, რომელიც თვით მომხმარებლებისათვის, როგორც დასაშიფრად, ასევე გასაშიფრად არის სწრაფი და მარტივი, მაგრამ ამავდროულად, მესამე პირისათვის („ჰაკერი") არის რთულად გასატეხი, ანუ მაქსიმალურად დაცული სხვა არაკანონიერი მომხმარებლებისაგან. ასევე მიმღებ მხარეს შეუძლია დაადგენოს მიღებული დაშიფრული ტექსტის ნამდვილობა. მიღებული მეთოდები მომხმარებლებისათვის ხასიათდება მაღალი სიჩქარით, შესაბამისად მოითხოვს მცირე დროს, დიდი სიმრავლით და მცირე ალბათობით. გატეხვა ფაქტიურად ნულის ტოლფასია, რაც აგებულ გრაფიკებზეც ნათლად ჩანს. ორობითი უფრო საიმედოა ვიდრე ათობითი. თუმცა ათობითიც მაქსიმალურად დაცული მეთოდია, ვიდრე არსებული მეთოდები.

ლიტერატურა:

1. Смарт Н., Криптография, М., Технисфера, 2005
2. ვერულავა ო., ხუროძე რ., ამომცნობი სისტემების თეორიის საფუძვლები. თბ. სტუ, 2001
3. კუციავა ვ., კაცაძე გ., დიაკონიძე ქ., ინფორმაციის დაცვა. სტუ, თბ., 2005
4. Питерсон У., Уэлдон, Э., Коды, исправляющие ошибки, "Мир", I-II том 1976.
5. Берлекэмп Э., Алгебраическая теория кодирования, М. Мир, 1971
6. Касами Т., Токура Н., Ивадари Е., Инагаки Я., Теория кодирования, М., Мир, 1978
7. Бухштаб А.А., Теория чисел. М., Просвещение, 2-е изд., 1966
8. კოტრიკაძე გ., ინფორმაციის დაცვა კომპიუტერულ სისტემებში, დისერტ.შრ. ა-რეფ. თბ, სტუ, 2009. ელ-ვერსია - http://www.gtu.ge/sad_nash.php.

WORKING OUT OF A METHOD OF PROTECTION OF THE INFORMATION ON WEIGHT OF NUMBERS

Kotrikadze Gulnara, Cimintia Tabuka
Georgian Technical University

Summary

We developed a new method of the closed channel, which is very fast and simple to use for coding and decoding purposes. At the same time, it is very difficult for so-called «hackers » to crack it, and is highly protected from the illegal access. Besides, the receiving party can establish the validity of the coded text

РАЗРАБОТКА МЕТОДА ЗАЩИТЫ ИНФОРМАЦИИ ПО ВЕСУ ЧИСЕЛ

Котрикадзе Г., Цимintиа Т.
Грузинский Технический Университет

Резюме

Нами был разработан новый метод закрытого канала, который является очень быстрым методом и простым в потреблении как для шифрования, так и расшифрования. В то же время, третьему лицу - «хаккеру» очень трудно его взломать, иначе говоря, метод максимально защищен от незаконного пользователя. К тому же принимающая сторона может установить достоверность зашифрованного текста. Для получения данного метода использованы веса чисел.