ინფორმაციის დაცვა გასაღების გარეშე, მხოლოდ შავი ფერის გამოყენებით

გულნარა კოტრიკაძე, ეკატერინე როჭიკაშვილი,
გიორგი კუჭავა, ანდრო გაფრინდაშვილი, თეიმურაზ მამუკაშვილი
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

წარმოდგენილია ინფორმაციის დაცვის ალგორითმი RGB ფერთა შავი ფერის კოდის გამოყენებით. მთლიანად დაშიფრული ინფორმაცია არის წარმოდგენილი სხვადასხვა სიხშირის შავი ფერით. გამტაცებლისათვის, რომელიც ჩაიგდებს ხელთ დაშიფრულ ინფორმაციას, უკუგზა გაშიფვრისათვის არ არსებობს. მომხმარებლებისათვის დაშიფვრა-გაშიფვრის ალგორითმი არის მარტივი და სწრაფი, მესამე პირისათვის რთული და შეუძლებელი.

საკვანძო სიტყვები: კრიპტოგრაფია. შავი ფერი. თექვსმეტობითი კოდი.

1. შესავალი

კრიპტოგრაფია დღესდღეობით გამოიყენება ტექნოლოგიურად განვითარებულ ისეთ სფეროებში, როგორიცაა: საკრედიტო ბარათები, კომპიუტერული პაროლები, ელექტრონული კომერცია და სხვ.

ნებისმიერი კოდი მოიცავს გარკვეულ ინფორმაციას. ზოგიერთი მათგანი სტრუქტურული და ფუნქციონალური თვისებისაა, მაგალითად - გენეტიკური; ზოგი კი გამიზნულია მხოლოდ ინფორმაციის დამუშავებისა და გადაცემისათვის და სხვა, თუმცა მკვეთრი საზღვრის გავლება მათ შორის ხშირად შეუძლებელიცაა.

არსებობს ინფორმაციის მრავალი განსხვავებული განსაზღვრება ზოგად ფილოსოფიურად (როგორც რეალური სამყაროს ასახვა-გამოხატულება), ყველაზე კერძო პრაქტიკულ განსაზღვრებამდე (როგორც - მონაცემები, გამიზნული მათი დამუშავების, გადაცემისა და დამახსოვრებისათვის). აღსანიშნავია ტერმინ „ინფორმაციის“ მრავალმხრივი (უშუალო, მაგრამ ხშირად გაუცნობიერებელი) გამოყენება ყოველდღიურ ცხოვრებაში: „ინფორმაციული საშუალებები“, „მიღებული ინფორმაცია“, „არასრული ინფორმაცია“, „ინფორმაციული ომი“, „ინფორმაციული გარემო“, და ა.შ., რაც წარმოადგენს ტერმინ „ინფორმაციასთან“ დაკავშირებულ ცნებათა არასრულ ჩამონათვალს. მნიშვნელოვანია ნორბერტ ვინერის აზრი, რომ „ინფორმაცია არის ინფორმაცია და არა მატერია ან ენერგია“.

XXI საუკუნე ინფორმაციის საუკუნეა. ადამიანთა შორის ფრიად გაზრდილია კომუნიკაცია სხვადასხვა ტექნიკური საშუალებების გამოყენებით. არა მარტო პერსონალებს, არამედ სხვადასხვა დონის უწყებებსაც აქვთ ინფორმაციის გაცვლის გაზრდილი მოთხოვნილებები. ინფორმაციის ერთი ადგილიდან მეორეზე გადაცემა უკვე აღარაა საკმარისი. უნდა მოხდეს მისი აუცილებლად დაფარულად, დაშიფრულად გადაცემა, რათა დაცულ იქნეს მისი აუთენტურობა. ამდენადაა აქტუალური ინფორმაციის დაცულობის გაზრდის უზრუნველყოფა [1,2].

2. ინფორმაციის დაცვის მეთოდის ალგორითმი

მოცემულ მეთოდში გამოიყენება სხვადასხვა სიხშირის მხოლოდ შავი ფერი, რომელთაც შეესაბამება სხვადასხვა RGB ფერთა კოდები. კანონიერი მომხმარებლები წინასწარ ასო-ნიშნებს, ციფრებს, სასვენ ნიშნებსა და არითმეტიკულ ოპერაციებს მიანიჭებენ სხვადასხვა სიხშირის შავ ფერს. შესაბამისად, სხვადასხვა თექვსმეტობითი კოდებით იქნება წარმოდგენილი, არც-ერთი არ მეორდება. ასევე ყოველი მომდევნო წინა მონაცემზე არ იქნება დამოკიდებული, ანუ მათ შორის კანონზომიერება არ არსებობს. აღნიშნული, საბოლოო ჯამში წარმოდგენილი იქნება ცხრილის სახით და იცის მხოლოდ კანონიერმა მომხმარებლებმა, ანუ ცხრილი არის თავად ინფორმაციაც და გასაღებიც (იხ. ცხრილი 1).

გარდა აღნიშნულისა, ცხრილთან ერთად მომხმარებლები აწვდიან ერთმანეთს იმ პიქსელების რაოდენობას, რომელთა მიხედვით, მიღებული ინფორმაცია უნდა დაყონ ცალკეული ფერების სახით, რომელიც სხვადასხვა ასონიშანზე იქნება სხვადასხვა [5].

საიდუმლო ცხრილის ნაწილი **ცხრ.1**

ქართული ანბანი	**მინიჭებული ფერი**	**მათემატიკური მოდელი თექვსმეტობით თანრიგში (RGB ფორმატი)**
ა		000000
ბ		0b0102
გ		1d0807
დ		201718
ე		2f2929
ვ		2f2929
ზ		332a2b
თ		383435
ი		4c4a4b
კ		483c3c
ლ		493131
მ		432120
ნ		482a2a
ო		411313
პ		5c5656
ჟ		524c4c

შეტყობინების დაშიფვრის ალგორითმი: საწყის შეტყობინებასუნდა შევუსაბამოთ ცხრილიდან აღებული ფერები, მთლიანად გამოდის გრძივი შავი ფერი, რომელიც საბოლოო ჯამში შეიცავს ინფორმაციას და გადაეცემა მეორე მომხმარებელს. მაგალითად, ავიღო ინფორმაციის სახით შეტობინება - „კრიპტოგრაფია“ (ნახ.1).

ნახ.1. დაშიფრული შეტყობინება „კრიპტოგრაფია“

მიღებული დაშიფრული ინფორმაცია, წარმოდგენილი 1-ელი ნახაზის სახით, ეგზავნება მეორე კანონიერ მომხმარებელს. მეორე კანონიერი მომხმარებლის მიერ ჩასატარებელი გაშიფვრის ალგორითმი:

პირველ რიგში, მიღებულ შეტყობინებას შავი ფერის სახით, დაყოფს მისთვის ცნობილი პიქსელების მიხედვით. შემდგომ მიღებული დანაყოფის თითოეულ შავ ფერს შეუსაბამებს Photoshop-ის RGB თექვსმეტობით კოდს. მიიღებს შეტყობინებას ჩაწერილს თექვსმეტობითი კოდების სახით. თექვსმეტობითი კოდები კი, მისთვის უკვე ცნობილია საიდუმლოდ გაცვლილი ცხრილის საშუალებით. მიღებულს შეუსაბამებს მონაცემთა ბაზიდან (ცხრილი 1.) ასონიშნებს და მიიღებს საწყის შეტყობინებას, იხ. ცხრილი 2.

კანონიერი მომხმარებლის მიერ გაშიფრული საწყისი შეტყობინების სახე **ცხრ.2**

კ	რ	ი	პ	ტ	ო	გ	რ	ა	ფ	ი	ა
5c5656	514343	4c4a4b	5c5656	4d1b1c	411313	1d0807	514343	000000	343031	4c4a4b	000000

აღნიშნულს შევხედოთ მესამე პირის თვალით (ინფორმაციის გამტაცებელი). პირველ რიგში მან უნდა მოახდინოს მის ხელთ ჩაგდებული შავი ფერის სურათის დაყოფა პიქსელებად, აღნიშნული მისთვის უცნობია. შემდგომ უნდა შეუსაბამოს თექვსმეტობითი კოდები, რასაც თავისთავად გაცილებით დიდ დროს მოანდომებს, ვიდრე კანონიერი მომხმარებელი. გარდა ამისა, იმისათვის რომ ამოიცნოს შეტყობინება, წინასწარ შედგენილი მონაცემთა ბაზა (ცხრილი 1.) უნდა იცოდეს, მისთვის აღნიშნულიც უცნობია. აქედან გამომდინარე, იგი რეალურ დროში ვერ მოახდენს მის ხელთ ჩაგდებული დაშიფრული შეტყობინების გატეხვას (გაშიფვრა) [3,4].

მიღებული მეთოდის მახასიათებლები: გადასაცემი ინფორმაცია დავშიფრეთ შავი ფერით, აღნიშნული ფერი RGB ფორმატით წარმოვადგინეთ. რამდენიმე ასეული ათასი ოდენობის შავი ფერის გრადაცია არსებობს. წარმოდგენილ სტატიაში გამოვიყენეთ მხოლოდ შავი ფერის 55 ოდენობის გრადაცია. სხვაობის გამოთვლას არა აქვს აზრი, იმდენად უზარმაზარი მარაგი შავი ფერისა არსებობს, ინფორმაციის დაფარვა-გადასაცემად [5].

3. დასკვნა

ბუნებრივია, დგება საკითხი – როგორია მესამე პირის მიერ გადაცემული ინფორმაციის ხელში ჩაგდების შემთხვევაში, მისი გაშიფვრა-ამოკითხვის ალბათობა ?

გაშიფვრის ალგორითმის თანმიმდევრობა შემდეგნაირია:

1. თითოეულ წასაკითხ ბილიკზე განლაგებული ასონიშნის გამოჯვნა, მკაცრად წინასწარ შერჩეული პიქსელების მიხედვით;
2. თითოეული ასონიშნის წარმოდგენა სხვადასხვა სიხშირის შავი ფერით;
3. თითოეული ასონიშნის ჩაწერა თექვსმეტობითი კოდის გამოყენებით;
4. თითოეულ კოდისათვის ცხრილის მიხედვით ასონიშნების მინიჭება.

აღნიშნული ოთხივე პუნქტი გამტაცებლისათვის უცნობია. შესაბამისად, იგი ვერ შეძლებს შეტყობინების ამოცნობას.

ლიტერატურა:

1. Shneier B. Applied Cryptography, John Wiley and Sons. Inc. New York. 1996
2. Application of volumetric matrix in cryptography. Problems of Mechanics. I-ntern. Federation for the Promotion of Mechanism and Machine Science, Tb., 2010
3. Шнайер Б. Прикладная криптография. М., Изд. ТРИУМФ. 2003
4. Смарт Н. Криптография, М, Технисфера, 2005
5. Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования. М., Мир, 1978.

PROTECTION OF INFORMATION WITHOUT KEY USE ONLY BLACK COLORS

Kotrikadze Gulnara, Rodjikashvili Ekaterine,
Kudjava Giorgi, Gaprindashvili Andro, Mamukashvili Teimuraz

Georgian Technical University

Summary

The paper presents algorithm of the security by using RGB blackcolor code. The encrypted information is presented in different density black color. For robber, who interception the encrypted information, alternative Decrypt way does not exist. For customer to encrypt and decoding algorithm is simple and fast, and it is difficult or impossible for third person.

ЗАЩИТА ИНФОРМАЦИИ БЕЗ КЛЮЧА ИСПОЛЬЗУЯ ТОЛЬКО ЧЁРНЫЙ ЦВЕТ

Котрикадзе Г., Рочикашвили Е.,
Кучава Г., Гаприндашвили А., Мамукашвили Т.

Грузинский Технический Университет

Резюме

Рассмотрен алгоритм защиты информации с использованием кода чёрного цвета RGB цветов. Полностью зашифрованная информация представлена чёрным цветом разных частот. Для похитителя, завладевшего зашифрованной информацией, не существует обратного пути для расшифровки. для потребителя алгоритм шифровка-расшифровка простой и быстрый, а для третьего лица - сложный и невозможный.