# კრიპტომეთოდი გასაღების გამოთვლისა და გამოყენების გარეშე

გულნარა კოტრიკაძე, თეონა ჯელაძე, ზინაიდა დვალიშვილი
საქართველოს ტექნიკური უნივერსიტეტი

**რეზიუმე**

მიღებულია ღია არხის მეთოდი, სადაც არც გამოყენებული არც გამოთვლილი, არც დასაშიფრი და არც გასაშიფრია გასაღები. ამავდროულად, მეთოდი, არსებულ მეთოდებთან შედარებით, მომხმარებლებისთვის მისაღები, პრაქტიკაში ადვილად გამოყენებადი და სწრაფია. ასევე „ჰაკერის" ტიპის მომხმარებლისაგან მაქსიმალურად დაცულია.

**საკვანძო სიტყვები:** დაცვა. ასიმეტრიული. გასაღები. ლოგარითმი.

## 1. შესავალი

კრიპტოგრაფია ანუ ინფორმაციის დაცვა გამოიყენება სამხედრო სამსახურში, ქვეყნის საშინაო და საგარეო პოლიტიკაში. აქედან გამომდინარე, მეთოდები, რომლებსაც იყენებენ ამათუიმ კონკრეტული დავალების შესასრულებლად, მაქსიმალურად დაცული უნდა იყოს უცხო პირებისაგან. ჩვენი მიზანიც იყო მაქსიმალურად დაცული ღია მეთოდის შექმნა გასაღების გარეშე. ამიტომ ნაშრომი მიეკუთვნება კრიპტოგრაფიას, რომელიც არის და ყოველთვის იქნება ერთ-ერთი აქტუალური საკითხი ყოველდღიურ ცხოვრებაში.

ჩვენ მიზნად გვქონდა, რომ შეგვექმნა ისეთი მეთოდი, რომელიც უგასაღებო იქნებოდა და რა თქმა უნდა, საიმედო. მივიღეთ მეთოდი, რომელიც მიეკუთვნება ასიმეტრიულ სისტემებს, არ გამოიყენება გასაღები და არანაკლებ საიმედოა, როგორც სხვა არსებული მეთოდები.

სამეცნიერო სიახლე: ასიმეტრიულ სისტემებში ყოველთვის გამოიყენება ან საერთო გასაღები, ან ცალცალკე დასაშიფრი და გასაშიფრი გასაღები. ჩვენს მიერ მიღებულ მეთოდში კი გასაღები საერთოდ არ გამოიყენება, არც გამოითვლება და არც საიდუმლოდ მიეწოდება.

## 2. ძირითადი ნაწილი

ჩვენ გავეცანით და შევისწავლეთ არსებული მეთოდები და დავდექით ასეთი ამოცანის წინაშე: შეგვექმნა ისეთი მეთოდი, სადაც მომხმარებლები არ გამოთვლიდნენ გასაღებს და არც საიდუმლოდ გადასცემდნენ ერთმანეთს. ანუ შეგვექმნა ისეთი მეთოდი, სადაც საერთო გასაღები არ გამოიყენება, მაგრამ მიუხედავად ამისა, არსებულ მეთოდებთან შედარებით, საიმედოობა მიღებული მეთოდის, იქნებოდა არანაკლები, ვიდრე არსებული მეთოდების.

მეთოდი მდგომარეობს შემდეგში:

გამოთვლა ხდება GF(p) გალუას ველზე. წინასწარ ცნობილია, ანუ ყველა მომხმარებელმა იცის p რიცხვი. ასევე ცნობილია, რომ ორივე კანონიერი მომხმარებელი ირჩევს ორ-ორ საიდუმლო მთელ რიცხვებს. მომხმარებლები ავღნიშნოთ X –ით და Y-ით.

X – მომხმარებელი აკეთებს შემდეგ ოპერაციას. აიღებს რაიმე მთელ რიცხვს და შემდგომ ითვლის მეორე მთელ რიცხვს, შემდეგი ტოლობის გამოყენებით:

$$a * c = 1 \ ( \mathrm{mod}(p-1) )$$

მიღებულ a და c რიცხვებს იტოვებს საიდუმლოდ [1,2].

ანალოგიურად იქცევა მეორე Y მომხმარებელიც:

Y – მომხმარებელი აკეთებს შემდეგ ოპერაციას. აიღებს რაიმე მთელ რიცხვს და შემდგომ ითვლის მეორე მთელ რიცხვს, შემდეგი ტოლობის გამოყენებით:

$$b * d = 1 \ ( \mathrm{mod}(p-1) )$$

მიღებულ b და d რიცხვებს იტოვებს საიდუმლოდ.

ამის შემდეგ, ვთქვათ X – მომხმარებელმა უნდა გააგზავნოს წერილი, შესაბამისად მან უნდა დაიწყოს ტექსტის დაშიფვრა. ტექსტი, ანუ ინფორმაცია ავღნიშნოთ M სიმბოლოთი.

X – მომხმარებელი გამოთვლის: $M^a \ (\mathrm{mod}p) = A$

მიღებულს უგზავნის ღია არხით მეორე მომხმარებელს.

Y – მომხმარებელი გამოთვლის: $A^b \ (\mathrm{mod}p) = B$

და რასაც მიიღებს უგზავნის ისევ პირველ მომხმარებელს,

X – მომხმარებელი გამოთვლის: $B^c \ (\mathrm{mod}p) = C$

მიღებულს გაუგზავნის მეორე Y მომხმარებელს

Y – მომხმარებელი გამოთვლის: $C^d \ (\mathrm{mod}p) = M.$

ჩავწეროთ გაშლილი სახით: $M^{a*b*c*d} (modp) = M^{(a*c)*(b*d)} (modp) = M^{1*1} (modp) = M$ მოვიყვანოთ მაგალითი, რადგან აღნიშნული მეთოდი უფრო მკაფიო და გასაგები გახდეს [1-3].

GF(p) ველზე, ვთქვათ $p = 11$, $p-1 = 10$ .

X – მომხმარებელი $a * c = 1 ( mod(p-1) )$. ვთქვათ $a = 3$, $3 * c = 1 ( mod(10) )$ , აქედან $c = 7$;

X – მომხმარებელი იღებს შემდეგ წყვილს (a,c) = (3,7).

Y – მომხმარებელი $b * d = 1 ( mod(p-1) )$, ვთქვათ $b = 1$, $1 * d = 1 ( mod(10) )$ , აქედან $d = 11$;

Y – მომხმარებელი იღებს შემდეგ წყვილს (b,d) = (1,11).

M = გ ე პ ე ი ანუ M = 2 4 14 4 8

ამის შემდეგ სიმბოლოები უნდა ავაზარისხოთ იმ საიდუმლო რიცხვების გამოყენებით [3,4].

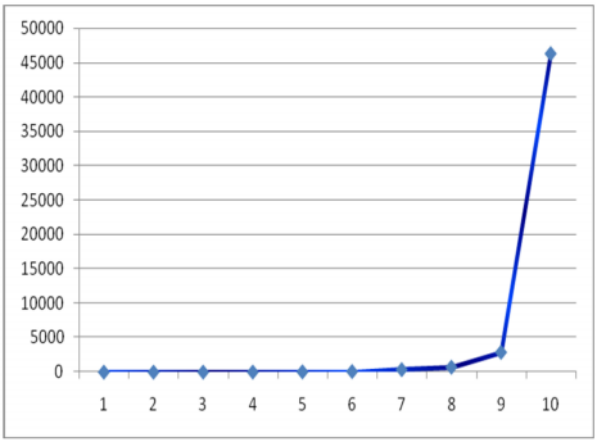
| X – მომხმარებელი | | Y – მომხმარებელი |
|---|---|---|
| $2^3 mod11 = 8$ | → | $8^1 mod11 = 8$ |
| $8^7 mod11 = 2$ | ← → | $2^{11} mod11 = 2$ |
| $4^3 mod11 = 9$ | → | $9^1 mod11 = 9$ |
| $9^7 mod11 = 4$ | ← → | $4^{11} mod11 = 4$ |
| $14^3 mod11 = 5$ | → | $5^1 mod11 = 5$ |
| $5^7 mod11 = 3$ | ← → | $3^{11} mod11 = 3 + (11)$ |
| $8^3 mod11 = 6$ | → | $6^1 mod11 = 6$ |
| $6^7 mod11 = 8$ | ← → | $8^{11} mod11 = 8$ |

მაშასადამე, მეორე მომხმარებელმა მიიღო ტექსტი, სრულიად ღია არხით და ყველასათვის ხელმისაწვდომი გზით, მაგრამ მიუხედავად ყველაფრისა, მაქსიმალურად დაცული გზით.

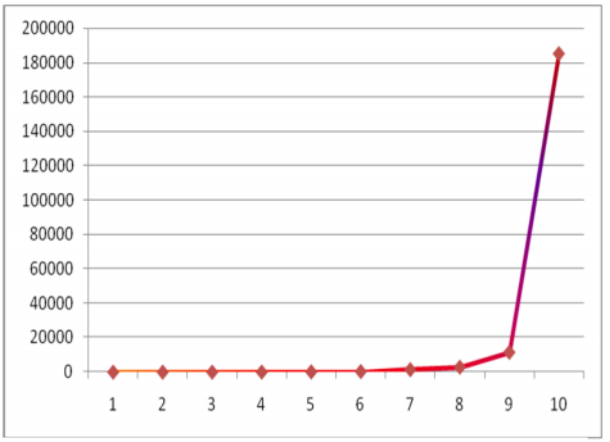
შეიძლება ითქვას, რომ ყველა ტოლობიდან უცნობი არის ხარისხის მაჩვენებელი, ანუ ის საიდუმლო რიცხვები, რომლებიც ამოირჩიეს და გამოთვალეს საიდუმლოდ მომხმარებლებმა, მოდულის გამოყენებით. მაგალითად: $\mathbf{M^a (modp) = A}$, $\mathbf{M^a (mod11) = 8}$, $\mathbf{a = \log_M 8 (mod11)}$.

სხვა ტოლობებში კი, ტექსტის ნაცვლად გვაქვს სხვა რიცხვი ღია არხით გაგზავნილი, მაგ: $9^7 mod11 = 4$. ამ ტოლობიდა, ჰაკერისათვის უცნობია მხოლოდ ხარისხის მაჩვენებელი, ამიტომ ჩავწეროთ ასეთი სახით $9^X mod11 = 4$, ამ ტოლობიდან გამომდინარე $x = \log_9 4 (mod11)$ .

ე.ი. 9 რა ხარისხში უნდა ავიყვანოთ, რომ მოდულით 11, მივიღოთ 4. ასეთი ძალიან ბევრი რიცხვი არსებებს, სხვადასხვა რიცხვები ერთიდაიგივე მოდულით მოგვცემს ერთიდაიგივე შედეგს. მაშასადამე, ამ მეთოდის საიმედოობა დამოკიდებულია ხარისხის, ანუ საიდუმლო რიცხვების ამოცნობის სირთულეზე. აღნიშნული კი, დამოკიდებულია მოდულის მაჩვენებელზე. საიმედოობა იქნება $\mathbf{2^{p/2}}$ –ზე დამოკიდებული, იხ. ცხრილი 1, გრაფიკები 1-2:




**გრაფიკი 1. არსებული დიფი-ჰელმან-მერკლეს მეთოდის p მოდულის დამოკიდებულება N ჩასატარებელ ოპერაციებთან**




**გრაფიკი 2. მიღებული ახალი მეთოდის p მოდულის დამოკიდებულება N ჩასატარებელ ოპერაციებთან.**

**არსებული და მიღებული ახალი ასიმეტრიული მეთოდების მახასიათებლები.** **ცხრ.1**

| სიმეტრ. სისტ. | გამოყენ. ფუნქც. | შიფრაციის სიჩქარე | ჩასატარებელი ოპერაც. რაოდენობა | კრიპტო სირთულე |
|---|---|---|---|---|
| RSA ალგ. | ასიმეტრ. | დაბალი | $\approx 2^*2^{p/2}$ | მამრავლებად დაშლა |
| ელ-გამალ. ალგ. | ასიმეტრ. | დაბალი | $\approx 2^*2^{p/2}$ | მამრავლებად დაშლა |
| დიფი-ჰელმან | ასიმეტრ. | დაბალი | $\approx 2^{p/2}$ | მამრავლებად დაშლა |
| ახალი მეთოდი | ასიმეტრ. | დაბალი | $\approx 4 * 2^{p/2}$ | მამრავლებად დაშლა |

p მოდულის ზრდა, რათქმაუნდა იწვევს ჩასატარებელი ოპერაციების რაოდენობის გაზრდას, ანუ გადარჩევას მარტივ რიცხვთა სიმრავლეში. როცა P≥37-ზე, N ჩასატარებელ ოპერაციათა რაოდენობამ დაიწყო ძალიან სწრაფი ზრდა, რაც ნათლად ჩანს გრაფიკზე და მეტყველებს მეთოდის საიმედოობაზე. თუმცა აღსანიშნავია ის ფაქტი, რომ უკვე არსებულ დიფი-ჰელმან-მერკლეს მეთოდში, ჩასატარებელი ოპერაციების რიცხვი, საგრძნობლად მცირეა ვიდრე ჩვენს მიერ მიღებულ მეთოდში [5-7].

## 3. დასკვნა

მიღებული მეთოდი არის ასიმეტრიული, პროცესი ღია არხით მიმდინარეობს. უკვე არსებულ ასიმეტრიულ მეთოდებში ღია არხით ხდება გასაღების გამოთვლის პროცესი, მიიღება საერთო გასაღები და შემდგომ მიღებული საერთო გასაღები გამოიყენება გასაგზავნი ტექსტის დასაშიფრად და კიდევ მიმღები მხარე ითვლის საერთო გასაღების შებრუნებულს, ანუ გასაშიფრ გასაღებს, როგორც ეს დიფი-ჰელმან-მერკლეს მეთოდში ხდება და მიღებულით ახდენს დაშიფრული ტექსტის გაშიფვრას ანუ საწყისი ტექსტის მიღებას, რაც დიდ დროს მოითხოვს. ჩვენს მიერ მიღებულ მეთოდში კი, საერთო გასაღების გამოთვლა არ არის საჭირო და არც საიდუმლოდ გადაიცემა. საერთოდ მეთოდს გასაღები არ სჭირდება. უბრალოდ მომხმარებლები ირჩევენ საიდუმლო რიცხვებს, რომლებიც გამოითვლება ყველასათვის ცნობილი ფორმულის საშუალებით. მაგრამ მიუხედავად ამისა, მეთოდი მაქსიმალურად დაცულია და საიმედოობა დამოკიდებულია ლოგარითმის გამოთვლის სირთულეზე. დიფი-ჰელმან-მერკლეს მეთოდში საერთო გასაღების მიღებისათვის ტარდებოდა ოთხი ოპერაცია. ჩვენს მიერ მიღებულ მეთოდში კი, ოთხი ოპერაციის შედეგად, მიმღები მხარე იღებს საწყის ტექსტს. ე.ი. მიღებული მეთოდი სიჩქარითაც გამოირჩევა, უფრო სწრაფია.

## ლიტერატურა:


1. Shneier B., Applied Cryptography, John Wiley and Sons. Inc. New York. 1996y.
2. Смарт Н., Криптография, М., Технисфера, 2005y.
3. კოტრიკაძე გ., ინფორმაციის დაცვის ასიმეტრიული სისტემის ახალი მეთოდის შემუშავება, თბ. სტუ, შრომები მართვის ავტომატიზებული სისტემები, 2009წ, №1(6), გვ.53.
4. კოტრიკაძე გ., ასიმეტრიული მატრიცული მეთოდის სინთეზი სიმეტრიულ მეთოდთან, თბ. სტუ, პერიოდული სამეცნიერო ჟურნალი "ინტელექტი", 2009წ. №1(33), გვ.110.
5. Application of volumetric matrix in cryptography, PROBLEMS OF MECHANICS, I nternational Federation for the Promotion of Mechanism and Machine Science, Tbilisi 2010y.
6. Касами Т., Токура Н., Ивадари Е., Инагаки Я., Теория кодирования, М., Мир, 1978г.
7. კოტრიკაძე გ., ინფორმაციის დაცვა კომპიუტერულ სისტემებში, სადისერტაციო ნაშრომი, თბ. სტუ, 2009წ., ელექტრონული ვერსია - http://www.gtu.ge/sad_nash.php.


## KRYPTOMETOD WITHOUT THE USE AND CALCULATION OF KEYS


Gulnara Kotrikadze, Teona Jeladze, Zinaida Dvalishvili
Georgian Technical University


**Summary**


We developed a new method of the open channels, which is operating without the usage/calculating neither general keys, nor coded/decoded keys. At the same time, the method is rather convenient and simple for practical purposes in comparison with other methods. Besides, it is more protected from the intervention of the third party – co-called «hacker».


## КРИПТОМЕТОД БЕЗ УПОТРЕБЛЕНИЯ И ВЫЧИСЛЕНИЯ КЛЮЧЕЙ


Котрикадзе Г., Джеладзе Т., Двалишвили З.
Грузинский Технический Университет


**Резюме**


Нами был получен новый метод открытого канала, в котором не употребляется и не вычисляется общий ключ и, вообще, не употребляется как зашифрованный, так и расшифрованный ключ. Метод весьма приемлем для потребителя, на практике, по сравнению с другими методами он прост. Кроме того, максимально защищен от третьего лица - «хаккера».