# კრიპტოგრაფიაში ცნობილი დიფი-ჰელმან-მერკლეს ალგორითმის გატეხვის მცდელობა

*გულნარა კოტრიკაძე*
სტუ-ს აკადემიური დოქტორი

მოგეხსენებათ, რომ კრიპტოგრაფია ინფორმაციის დაცვისა და დასაიდუმლოების სამეცნიერო ტექნიკური დარგია. კრიპტოგრაფია წარმოადგენს მონაცემების გარდაქმნის ისეთი მეთოდების ერთობლიობას, რომელთა გამოყენების შედეგად, მიღებული გარდაქმნილი მონაცემების გადაცემისას, შესაძლებელი ხდება კონფიდენციალურობისა და ინფორმაციის მთლიანობის დაცვის პრობლემების გადაწყვეტა.

კონფიდენციალურობის ქვეშ იგულისხმება პირადი ინფორმაციის (გამოძიების, სამხედრო ინფორმაციის და ა.შ.) საიდუმლო გადაცემა. არაკანონიერი მიმღები (ჰაკერი), კავშირის არხიდან, ვერ იღებს მისთვის სასურველ ინფორმაციას მთლიანობაში. ინფორმაციის მთლიანობაში იგულისხმება მისი შეუცვლელობა.

საზოგადოდ, ინფორმაციული უსაფრთხოების ქვეშ იგულისხმება, როგორც გადასამუშავებელი ასევე, შესანახი და გადასაცემი მონაცემების დაცვა არაკანონიერი მომხმარებლისგან. ინფორმაციის დაცვის საშუალებათა უმეტესობა ემყარება კრიპტოგრაფიული შიფრებისა და დაშიფვრა-გაშიფვრის პროცედურების გამოყენებას. შიფრის განსაზღვრების ქვეშ იგულისხმება შიფრის გასაღებისა და კრიპტოგრაფიული ალგორითმით მოცემული შექცევადი გარდაქმნის საშუალებით, ღია მონაცემების სიმრავლის ასახვა, დაშიფრული მონაცემების სიმრავლეზე. შიფრის ძირითადი მახასიათებელია კრიპტომედეგობა, რომელიც განსაზღვრავს შიფრის სიმტკიცეს კრიპტოანალიზის მეთოდებით მისი გაშიფვრის მცდელობისას. ეს მახასიათებელი განისაზღვრება იმ დროის ინტერვალით, რომელიც საჭიროა შიფრის გასახსნელად. კრიპტოგრაფიული შიფრი ითვლება უდავოდ მედეგად, თუ კრიპტოანალიტიკოსისთვის ღია ტექსტის აღდგენა შეუძლებელია ნებისმიერი მოცულობის შიფრტექსტის ცოდნის შემთხვევაში. არაკანონიერ მიმღებად იგულისხმება ბოროტგანმზრახველი (ჰაკერი).

ინფორმაციის კრიპტოგრაფიული დაცვისთვის გამოყენებული შიფრი უნდა აკმაყოფილებდეს შემდეგ მოთხოვნებს:

- უნდა ხასიათდებოდეს მაღალი კრიპტომედეგობით;
- დაშიფვრისა და გაშიფვრის პროცესი უნდა იყოს ასიმეტრიული;
- დაშიფვრისა და გაშიფვრის პროცედურა უნდა იყოს მარტივი და სწრაფი;
- დაშიფრული ინფორმაციისათვის დასაშვებია უმნიშვნელო სიჭარბე;
- შიფრი არ უნდა იყოს მგრძნობიარე დაშიფვრის პროცესში დაშვებული მცირეოდენი შეცდომების მიმართ;
- კრიპტომეთოდის ალგორითმის უკუ გზა არ უნდა არსებობდეს.

კრიპტოანალიტიკოსი ინფორმაციის დაშიფვრის გასაღების გამოსათვლელად, მის ხელთ არსებული საწყისი მონაცემებიდან გამომდინარე, ასრულებს ქვემოთ განხილული კრიპტოანალიზური შეტევებიდან ერთ-ერთს:

1. კრიპტოანალიზური შეტევა, როცა ცნობილია მხოლოდ შიფრტექსტი;
2. კრიპტოანალიზური შეტევა, როცა ცნობილია ღია ტექსტი;
3. კრიპტოანალიზური შეტევა ღია ტექსტის არჩევის შემთხვევაში;
4. კრიპტოანალიზური შეტევა ღია ტექსტის ადაპტური შერჩევით;
5. კრიპტოანალიზური შეტევა არჩეული შიფრტექსტის გამოყენებით;
6. კრიპტოანალიზური შეტევა გასაღებების ყველა შესაძლო ვარიანტების გადარჩევის მეთოდით;
7. ბანდიტური კრიპტოანალიზი (შანტაჟი, წამება, ქრთამი და ა.შ.).

კრიპტოგრაფიაში არსებობს ორი სახის სისტემა - სიმეტრიული (დახურული) და ასიმეტრიული (ღია). სიმეტრიულ სისტემებში გამოიყენება ერთი გასაღები, როგორც დასაშიფრად ასევე გასაშიფრად, ხოლო ასიმეტრიულში გამოიყენება ორი გასაღები, ერთი დასაშიფრად და მეორე გასაშიფრად.

**დიფი-ჰელმანის მეთოდის გატეხვის შესაძლებლობა**

ალგორითმი ეყრდნობა გალუას GF(p) მარტივ ველში ლოგარითმების გამოთვლის სირთულეს.

ვთქვათ, $y = a^x mod\, p\ (1 \le x \le p-1)$, $a$ საიდაც ველის პრიმიტიული ელემენტია. ამბობენ, რომ $x$ არის y-ის ლოგარითმი $a$ ფუძით GF(p) ველში: $x = log_a Y\ (modp)\ (1 \le y \le p-1)$. y-ის გამოთვლა x-ის მეშვეობით არ წარმოადგენს სირთულეს

და მოითხოვს მაქსიმუმ $2 \cdot log_2 p$ - გამრავლების ოპერაციას, მაგალითად: $a^{18} = (((a^2)^2)^2)^2 \cdot a^2$. მეორეს მხრივ, $x$-ის გამოთვლა y-ის მეშვეობით გაცილებით უფრო რთულია და მოცემული p-სთვის ცნობილი საუკეთესო ალგორითმების გამოყენებითაც კი $p^{1/2}$ ოპერაციათა რაოდენობას მოითხოვს.

გასაღების გაცვლა ხორციელდება შემდეგი სქემით:

ცნობილია ორი პარამეტრი: p (მარტივი) და $a$ (მთელი) და $1 \leq X_i, X_j \leq p-1$.

i-ური მომხმარებელი გამოთვლის $y_i = a^{x_i} mod\, p$ რიცხვს და ღია ფაილით უგზავნის მას j-ურ მომხმარებელს. თავის მხრივ, j-ური მომხმარებელი გამოითვლის $y_j = a^{x_j} mod\, p$ რიცხვს და ღიად უგზავნის მას i-ურ მომხმარებელს.

i-ური მომხმარებელი $y_j$-ის მეშვეობით აფორმებს გასაღებს: $g_{ji} = y_j^{x_i} mod p$

j-ური მომხმარებელი $y_i$-ის მეშვეობით აფორმებს გასაღებს: $g_{ij} = y_i^{x_j} mod p$

ეს გასაღებები იდენტურია, რადგან:

$$y_j^{x_i} = (a^{x_j})^{x_i} = a^{x_j x_i} = (a^{x_i})^{x_j} = y_i^{x_j} (mod p)$$

ე.ი. $g_{ij} = g_{ji} = k$

ე.ი. ორივე კანონიერმა მომხმარებელმა მიიღო ერთიდაიგივე $k$ გასაღები, რომელიც გამოიყენება ინფორმაციის დასაშიფრად. ეხლა კი უნდა გამოვთვალოთ მეორე გასაღები, რომელიც დაგვეხმარება ინფორმაციის გასაშიფრად.

ქვემოთ მოცემული ფორმულის საშუალებით ფიქსირდება გასაშიფრი გასაღები:

$$k \times x = 1 \; mod \; (p-1),$$

სადაც $k$ არის დასაშიფრი $k$<p, ხოლო $x$ არის გასაშიფრი გასაღები $x$<p.

მაგალითად: ცნობილია p=11 , $a$= 2

| I მომხმარებელი | | II მომხმარებელი |
|---|---|---|
| $X_1=3$ | | $X_2=2$ |
| $Y_1= a^{X1} \bmod p = 2^3 \bmod 11 = 8$ | $\longrightarrow$ | $8^{X2} \bmod p = 8^2 \bmod 11 = 9= k$ |
| $4^{X1} \bmod p = 4^3 \bmod 11 = 9 = k$ | $\longleftarrow$ | $Y_2 = a^{X2} \bmod p = 2^2 \bmod 11= 4$ |

დასაშიფრი გასაღები k=9, ეხლა ვიპოვოთ გასაშიფრი გასაღები $k \times x = 1 \bmod (p-1)$ .

$9 \times x = 1 \bmod (11-1)$ ანუ $9 \times x = 1 \bmod (10)$, $x = 9$. ამის შემდეგ დავშიფროთ და შემდგომ გავშიფროთ ტექსტი. ტექსტიდან ამოვიღოთ რაიმე ციფრი, მაგალითად, როგორიცაა m=5. დაშიფვრის შედეგად მიიღებს შემდეგ სახეს: $m^k(modp) = 5^9(mod11) = 9$, ღია არხით ეგზავნება მეორე მომხმარებელს, მეორე მომხმარებელი გამოიყენებს მეორე გასაშიფრ გასაღებს: $9^x(modp)=9^9(mod11)= =5=m$, რ.დ.გ.

**გატეხვის მცდელობა.**

მესამე არაკანონიერი მომხმარებლისთვის (ჰაკერი) ცნობილია შემდეგი პარამეტრები: p, a, $y_1$, $y_2$. მიუხედავად ამისა, მესამე პირისათვის დღეს-დღეობით რეალურ დროში, შეუძლებელია ალგორითმის გატეხვა, რადგან $x_1=log_a y_1(modp)=log_2 8(mod11)$, $x_2= =log_a y_2(modp)=log_2 4(mod11)$, ძალიან ბევრი $x_1$ და $x_2$ მოიძებნება ისეთი, რომლებიც დააკმაყოფილებენ აღნიშნულ ტოლობებს. ანალოგიურად, $m^k(modp)= =m^{k<p}(mod11)=9$, აღნიშნული ტოლობიდან $k= =log_m 9(mod11)$, ძალიან ბევრი k გასაღები მოიძებნება ისეთი, რომელიც დააკმაყოფილებს აღნიშნულ ტოლობას, მაგრამ პარალელურად ამისა უნდა მოიძებნოს გასაშიფრი გასაღები $k \times x=1 \bmod (p-1)$, $1 \leq k,x \leq p-1$.

თუ აღნიშნული კუთხით მიუდგებით მეთოდის გატეხვის მცდელობას, რეალურ დროში მეთოდი არ გატყდება, ამიტომ ალგორითმის გატეხვისათვის უმჯობესია მივმართოთ სხვა გზას. ავიღოთ კონკრეტული p მოდულის მნიშვნელობა, ჩამოვწეროთ ყველა შესაძლო k და x გასაღებთა წყვილების მნიშვნელობები, ამოვყაროთ (p-1) მოდულის ჯერადი რიცხვები და დარჩენილი წყვილებიდან დავადგინოთ კანონზომიერება.

როცა p=11, მაშინ ნებისმიერი $a$, $x_1$ და $x_2$ პარამეტრებისათვის არსებობს მხოლოდ ოთხი წყვილი გასაღებებისა, როგორიცაა $(K_1,X_1)=(1,11)$, $(K_2,X_2)=(3,7)$ , $(K_3,X_3)=(7,3)$, $(K_4,X_4)=(9,9)$. გასაღებთა წყვილი ყოველთვის შედგება კენტი რიცხვებისაგან k<p, x<p .

როცა p=13, მაშინ ნებისმიერი $a$, $x_1$ და $x_2$ პარამეტრებისათვის არსებობს მხოლოდ ოთხი წყვილი გასაღებებისა, როგორიცაა $(K_1,X_1)=(1,13)$, $(K_2,X_2)=(5,5)$, $(K_3,X_3)=(7,7)$, $(K_4,X_4)=(11,11)$. გასაღებთა წყვილი ყოველთვის შედგება კენტი რიცხვებისაგან k<p, x<p .

როცა p=17, მაშინ ნებისმიერი $a$, $x_1$ და $x_2$ პარამეტრებისათვის არსებობს მხოლოდ რვა წყვილი გასაღებებისა, როგორიცაა $(K_1,X_1)=(1,17)$, $(K_2,X_2)=(3,11)$, $(K_3,X_3)=(5,13)$, $(K_4,X_4)=(7,7)$, $(K_5,X_5)=(9,9)$, $(K_6,X_6)=(11,3)$, $(K_7,X_7)=(13,5)$,

$(K_8,X_8)=(15,15)$. გასაღებთა წყვილი ყოველთვის შედგება კენტი რიცხვებისაგან $k<p$, $x<p$ .

როცა $p=19$, მაშინ ნებისმიერი $a$, $x_1$ და $x_2$ პარამეტრებისათვის არსებობს მხოლოდ ექვსი წყვილი გასაღებებისა, როგორიცაა $(K_1,X_1)=(1,19)$, $(K_2,X_2)=(5,11)$, $(K_3,X_3)=(7,13)$, $(K_4,X_4)=(11,5)$, $(K_5,X_5)=(13,7)$, $(K_6,X_6)=(17,17)$. გასაღებთა წყვილი ყოველთვის შედგება კენტი რიცხვებისაგან $k<p$, $x<p$ .

როცა $p=23$, მაშინ ნებისმიერი $a$, $x_1$ და $x_2$ პარამეტრებისათვის არსებობს მხოლოდ ათი წყვილი გასაღებებისა, როგორიცაა $(K_1,X_1)=(1,23)$, $(K_2,X_2)=(3,15)$, $(K_3,X_3)=(5,9)$, $(K_4,X_4)=(7,19)$, $(K_5,X_5)=(9,5)$, $(K_6,X_6)=(13,17)$, $(K_7,X_7)=(15,3)$, $(K_8,X_8)=(17,13)$, $(K_9,X_9)=(19,7)$, $(K_{10},X_{10})=(21,21)$. გასაღებთა წყვილი ყოველთვის შედგება კენტი რიცხვებისაგან $k<p$, $x<p$ .

როცა $p=29$, მაშინ ნებისმიერი $a$, $x_1$ და $x_2$ პარამეტრებისათვის არსებობს მხოლოდ თორმეტი წყვილი გასაღებებისა, როგორიცაა $(K_1,X_1)=(1,29)$, $(K_2,X_2)=(3,19)$, $(K_3,X_3)=(5,17)$, $(K_4,X_4)=(9,15)$, $(K_5,X_5)=(11,23)$, $(K_6,X_6)=(13,13)$, $(K_7,X_7)=(15,15)$, $(K_8,X_8)=(17,5)$, $(K_9,X_9)=(19,3)$, $(K_{10},X_{10})=(23,11)$, $(K_{11},X_{11})=(25,9)$, $(K_{12},X_{12})=(27,27)$. გასაღებთა წყვილი ყოველთვის შედგება კენტი რიცხვებისაგან $k<p$, $x<p$ და ა.შ.

გასაღებთა წყვილების მნიშვნელობები, ყოველთვის იქნება კენტი რიცხვები, რადგან $(p-1)$ მოდული ყოველთვის დაჯდება ლუწი რიცხვი და $(p-1)$-ის ჯერადი, ლუწი რიცხვები, გასაღებთა სიმრავლიდან ამოვარდება. შესაბამისად გასაღებთა წყვილის რაოდენობა საგრძნობლად შემცირდება, იქნება მხოლოდ კენტი რიცხვები და კენტი რიცხვებიდანაც არა ყველა, და არაკანონიერი მომხმარებელი საგრძნობლად მოიგებს დროში, გადარჩევის თვალსაზრისით და არა მხოლოდ.

გასაღებთა წყვილების რაიმე კანონზომიერების დადგენას $p$ მოდულთან მიმართებაში, იხილავთ შემდგომ ნომერში.

## ლიტერატურა


1. ვ.კუციავა, გ.კაცაძე, ქ.დიაკონიძე, "ინფორმაციის დაცვა", სტუ 2005წ.
2. Б. Шнайер. "Прикладная криптография". Издательство ТРИУМФ. 2003г.
3. Андерсон. Джеймс. "Дискретная математика и комбинаторика". Издательство дом "Вильямс". 2003г.


## რეზიუმე


ნაშრომში წარმოდგენილია კრიპტოგრაფიის შესაძლებლობა, არსი და მიზანი. მოცემულია შიფრის მოთხოვნები და კრიპტოანალიზური შეტევების გზები. მოცემულია დიფი-ჰელმანის მეთოდი თავისი მაგალითით და აღწერილია მეთოდის გატეხვის მცდელობის საწყისი მონაცემები. გაგრძელებას იხილავთ შემდეგ ნომერში.


*Gulnara Kotrikadze*

## IN AN ATTEMPT TO BREAK THE CRYPTOGRAPHY ALGORITHM OF DIPI-HELMAN-MERKLE

## PART I

## SUMMARY


The paper presents the essence of the meaning and purpose of Kriptography. Requirements and codes of shifr and ways of kriptoanaliz attacks are shown. There is the method of Dipi-Helman with it's example and a method described in an attempt to break from the data. Then you will see a continuation in the after number.