კრიპტოგრაფიაში ცნობილი ასიმეტრიული სისტემის დიფიჰელმანმერკლეს ალგორითმის გატეხვის მცდელობა (ნაწილი II)

გულნარა კოტრიკაძე,
სტუ-ს აკად. დოქტ.

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 შიფროტექსტის ცოდნის შემთხვევაში [1,5].

ძირითადი ნაწილი

დიფი-ჰელმან-მერკლეს ალგორითმის მედეგობის ხარისხი

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.

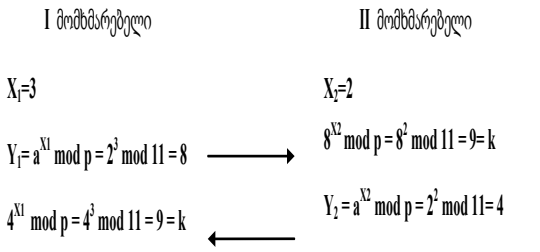
კრიპტოანალიტიკოსი ინფორმაციის დაშიფვრის გასაღების გამოსათვლელად, მის ხელთ არსებული საწყისი მონაცემებიდან გამომდინარე, ასრულებს ქვემოთ განხილული კრიპტოანალიზური შეტევებიდან ერთ-ერთს:

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, ასევე გამოიყენება დამატებითი პარამეტრი ნამდვილობის შესამოწმებლად.

სიმეტრიული სისტემის დიფი-ჰელმან-მერკლეს ალგორითმი ეყრდნობა გალუას GF(p) მარტივ ველში ლოგარითმების გამოთვლის სირთულეს [1,2].



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.

მესამე არაკანონიერი მომხმარებლისთვის (ჰაკერი) ცნობილია შემდეგი პარამეტრები: p, a, y1, y2. მიუხედავად ამისა, მესამე პირისათვის დღესდღეობით 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 x1 და x2 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 $k \times x = 1 \bmod (p-1)$, $1 \le k,x \le p-1$.

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 ა, ხ1 და ხ2 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 da 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 da 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 [3,6].

ზემოაღნიშნულ დაკვირვებას თუ გავაგრძელებთ, შეგვიძლია დავამტკიცოთ, რადგან დასაშიფრი და გასაშიფრი გასაღებთა წყვილი გამოითვლება ლუწი მოდულით

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

ამიტომ ყოველთვის კ დასაშიფრი და ხ გასაშიფრი გასაღებთა წყვილი მიიღება კენტი რიცხვები, ოღონდ ისეთი რომელსაც არ ექნება საერთო ჯერადი (p-1)-თან. მესამე პირმა (ჰაკერმა) იცის p მოდული, აქედან გამომდინარე მისთვის შესაძლებელია საიდუმლო რიცხვების გარეშე (რომელიც აირჩიეს მომხმარებლებმა ერთმანეთის დამოუკიდებლად, რომელიც მას საერთოდ არ სჭირდება და მის ძებნას ნამდვილად არ დაიწყებს), p მარტივი რიცხვის(მოდულის) საშუალებით იპოვოს ყველა შესაძლო წყვილი გასაღებებისა, მაგრამ შემდეგ მოუწევს ამ გასაღებთა სიმრავლიდან გადარჩევა.

გარდა ამისა, რაც ასევე მნიშვნელოვანია ინფორმაციის დაშიფვრა-დეშიფრაციის დროს – ეს არის ინფორმაციის ნამდვილობის შემოწმება. ანუ საწყისმა მომხამარებელმა უნდა დაშიფროს ინფორმაცია

გასაღებთა წყვილიდან დასაშიფრი ღია გასაღებით, მიღებულ შიფროტექსტს უგზავნის მიმღებ მხარეს ღია ყველასათვის ხელმისაწვდომი არხით. შემდგომ მიმღები მიღებულ დაშიფრულ ინფორმაციას გაშიფრავს გასაღებთა წყვილიდან შესაბამისი მეორე გასაღებით (რომლებიც არის ურთიერთშებრუნებული) და მიიღებს საწყის ინფორმაციას.

ვთქვათ, ჰაკერმა ხელთ ჩაიგდო დაშიფრული ტექსტი, რომელიც ღიად იგზავნება და ქსელი არ არის დაცული. მიმღებ მხარეს უნდა შეეძლოს მიღებული დაშიფრული ინფორმაციის ნამდვილობის შემოწმება. ანუ ღიად გადაცემის პროცესში შესაძლებელია ჰაკერმა შეცვალოს დაშიფრული ტექსტი (მისთვის მეთოდი ცნობილია), ე.ი. ალგორითმი ცნობილია, ამიტომ მას შეუძლია თავისი ტექსტი დაშიფროს და ის გაუგზავნოს მიმღებ მხარეს, ამიტომ მიმღებს უნდა შეეძლოს მიღებული ტექსტის ნამდვილობის დადგენა, რაც აღნიშნულ მეთოდში არ არის გათვალისწინებული.

გარდა ამისა, რაც თავის მხრივ კიდევ უფრო მნიშვნელოვანია, გასაღების გამოთვლის პროცესიც ხდება ღია არხით, ეს დადებითი მხარეა ღია არხით რომ ხდება პროცედურები თუმცა, ჰაკერს შეუძლია გასაღების გამოთვლის პროცესში პირველი მომხმარებლის მიერ ღიად გაგზავნილი პარამეტრი შეცვალოს თავისი გამოთვლილით, მიმღები კი გააგრძელებს პროცესს მიიღებს გასაღებს, შემდეგ მოახდენს უკუპროცესს. ასე რომ გასაღებს მიიღებს ჰაკერი და მიმღები მხარეები, რაც რათქმაუნდა მიუღებელია. ამიტომ გარდა იმისა, რომ დაშიფრულ ინფორმაციასაც სჭირდება შემოწმება, ასევე სჭიდება გასაღების გამოთვლის პროცესსაც, რაც მეთოდში არ არის ჩადებული, რაც მის საიმედოობას საეჭვოს ხდის [4-6].

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

ე.ი. ჰაკერს, რადგან ალგორითმში არ არის გათვალისწინებული ნამდვილობის შემამოწმებელი კოდები, შეუძლია გასაღებთა ყველა შესაძლო წყვილის გამოთვლა, გარდა ამისა შეუძლია ჩაერთოს როგორც გასაღების გამოთვლის პროცესში ასევე შიფროტექსტის შეცვლაში, რაც მეტყველებს მეთოდის დაბალ მედეგობაზე.

გამოყენებული ლიტერატურა

1. Т. Касами, Н. Ток ура, Е. Ивадари, Я. Инагаки, Теория кодирования, М., Мир, 1978г.
2. B. Shneier, Applied Cryptography, John Wiley and Sons. Inc. New York. 1996г.
3. Б. Шнайер. „Прикладная криптография“. Издательство ТРИУМФ. 2003г.
4. Андерсон. Джеймс. „Дискретная математика и комбинаторика“. Издательство дом „Вильямс“. 2003г.
5. ვ.კუციავა, გ.კაცაძე, ქ.დიაკონიძე, „ინფორმაციის დაცვა“, სტუ, 2005წ.
6. Н. Смарт, Криптография, М., Технисфера, 2005г.

Summary

G. Kotrikadze

In an Attempt to Break the Cryptography Algorithm of Dipi-Helman–Merkle

The paper presents the possibility of cryptography, meaning and purpose. The crypto requirements and ways cryptography attacks. The dipi - helman - merkles method described in the examples and ways of breaking the algorithm and verifying the authenticity of options.

რეზიუმე

ნაშრომში წარმოდგენილია კრიპტოგრაფიის შესაძლებლობა, არსი და მიზანი. მოცემულია შიფრის მოთხოვნები და კრიპტოანალიზური შეტევების გზები. მოცემულია დიფი—ჰელმან-მერკლეს მეთოდი თავისი მაგალითით და აღწერილია ალგორითმის გატეხვის გზები და ნამდვილობის დამადასტურებელი პარამეტრები.