ასიმეტრიული კრიპტოსისტემის RSA-ს მეთოდის გატეხვა

გულნარა კოტრიკაძე, ეკატერინე როჭიკაშვილი,
ზვიად ჯობავა, ნუგზარ ყანდაშვილი, თეიმურაზ მამუკაშვილი
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

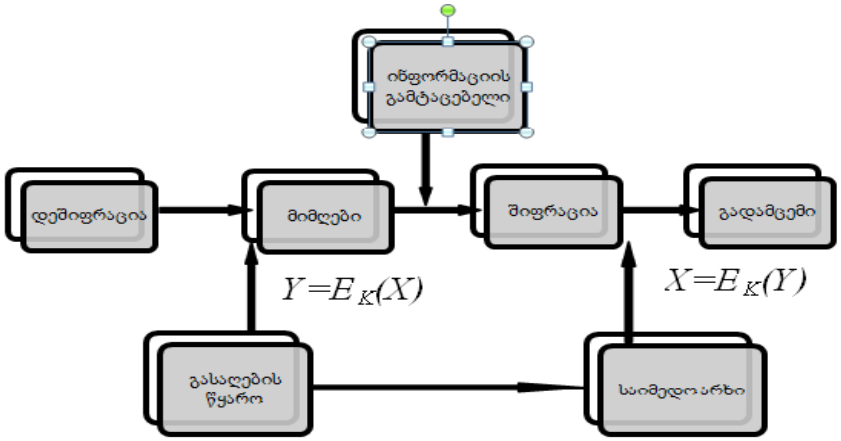
კრიპტოგრაფიის RSA მეთოდში, მესამე არაკანონიერი მომხმარებლისათვის, შესაძლებელია, საიდუმლო გასაშიფრი გასაღების გარეშე, მისთვის ცნობილი პარამეტრების საფუძველზე, უკუპროცესით დაშიფრული ინფორმაციის გაშიფვრა და საწყისის მიღება. ასევე ინფორმაციის გამტაცებელს, დაშიფრული ინფორმაციიდან, დეშიფრაციის გარეშე, ჩვენს მიერ დადგენილი კანონზომიერების საფუძველზე, შეუძლია საწყისი შეტყობინების მიღება.

საკვანძო სიტყვები: კრიპტოგრაფია. მედეგობა. კოდის გატეხვა.

1.შესავალი

ინფორმაცია ცხოვრების აუცილებელი ატრიბუტია. ადამიანი ცხოვრობს ინფორმაციულ გარემოში და გამუდმებით მონაწილეობს ინფორმაციულ პროცესებში. ინფორმაციული ეწოდება ისეთ პროცესს, რომელიც დაკავშირებულია ინფორმაციის მიღებასთან, შენახვასთან, გარდაქმნა-ანალიზსა და გადაცემასთან. ასეთ პროცესს ინფორმაციის დამუშავების პროცესსაც უწოდებენ. ნებისმიერი კოდი, ინფორმაციის მატარებელია. კოდირების სისტემები ინფორმაციის დამუშავების, გადაცემისა და დამახსოვრებისათვის იქმნება [1].

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 (ნახ.1).



ნახ. 1. დაშიფვრა-დეშიფრაციის სქემა

ინფორმაციის გადაცემის პროცესში მონაწილეობს კანონიერი მომხმარებლები და ინფორმაციის გამტაცებლები. გამტაცებლები ცდილობენ დაშიფრული ინფორმაციის ხელში ჩაგდებასა და საწყისი ინფორმაციის მიღებას.

კრიპტოგრაფია საიდუმლოს შენახვის მეცნიერებაა. კრიპტოანალიზი - კოდის გატეხვის ხელოვნებაა, ე.ი. წერილის აღდგენა გასაღების წინასწარი ცოდნის გარეშე. კრიპტოგრაფიაში მომუშავე ადამიანები კრიპტოგრაფებია, ხოლო კრიპტოანალიზში მომუშავეები – კრიპტოანალიტიკოსები [2,6].

2. ასიმეტრიული RSA მეთოდის ალგორითმი

თავდაპირველად განვიხილოთ RSA კრიპტოსისტემა და შემდგომ მისი გატეხვის ალგორითმი.

RSA კრიპტოსისტემაში საიდუმლო გასაღები $Z_ს$, ღია გასაღები $Z_ღ$, X შეტყობინება და Y კრიპტოგრამა მიეკუთნება მთელ რიცხვთა {0,1,2,....N-1) სიმრავლეს, სადაც N=p×q არის მოდული.

p და q შემთხვევითი დიდი მარტივი რიცხვებია. მაქსიმალური უსაფრთხოების უზრუნველსაყოფად ისინი შეირჩევა ერთნაირი სიგრძის და ინახება საიდემლოდ.

ღია გასაღების მნიშვნელობა შეირჩევა შემთხვევით შემდეგი პირობების გათვალისწინებით: $1< Z_ღ ≤ φ(N)$, უსგ $(Z_ღ, φ(N))=1$, $φ(N)=(p-1)×(q-1)$, სადაც φ(N) ეილერის ფუნქციაა და გამოიყენება ორივე გასაღების გამოსათვლელად.

საიდუმლო გასაღების მნიშვნელობა გამოითვლება ევკლიდეს ალგორითმით: $Z_ს×Z_ღ=1(\text{mod } φ(N))$ ან $Z_ს=Z_ღ^{-1} (\text{mod}(p-1)×(q-1))$.

ღია გასაღები გამოიყენება მონაცემების დასაშიფრად, ხოლო საიდუმლო გასაღები ამ შიფროტექსტის გასაშიფრად.

დაშიფვრისას კრიპტოგრამა მიიღება $y=Ez_ღ(x)=x^{Zღ}(\text{mod}N)$ გამოსახულებით, ხოლო ამ უკანასკნელის გაშიფვრა ხდება $x=Dz_ს(y)=y^{zს}(\text{mod } N)$ გამოსახულებით.

X შეტყობინების განსაზღვრა, როცა ცნობილია y, $z_ღ$ და N(N=2512) პრაქტიკულად შეუძლებელია, ამბობენ მეთოდის ავტორები, თუმცა ჩვენ აღმოვაჩინეთ, რომ შესაძლებელია, თანაც საკმაოდ მარტივად [5].

3. RSA (რაივეს-შამირ-ეიდელმანის) ალგორითმის გატეხვა

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 უკუგზა არ უნდა არსებობდეს. აღნიშნულ მოთხოვნებს RSA მეთოდი არ აკმაყოფილებს [3].

მეთოდის გატეხვის ალგორითმი. კრიპტოგრაფიაში ყველაფერი დადის მათემატიკაზე ანუ ციფრებზე, ამიტომ გასაგზავნი შეტყობინება უნდა ჩავწეროთ ციფრების სახით. ანბანი ჩავწეროთ რიგითი ნომრების მიხედვით (ცხრილი 1).

ქართული ანბანი და შესამამისი ნუმერაცია ცხრ.1

ა	2	მ	13	ღ	24
ბ	3	ნ	14	ყ	25
გ	4	ო	15	შ	26
დ	5	პ	16	ჩ	27
ე	6	ჟ	17	ც	28
ვ	7	რ	18	ძ	29
ზ	8	ს	19	წ	30
თ	9	ტ	20	ჭ	31
ი	10	უ	21	ხ	32
კ	11	ფ	22	ჯ	33
ლ	12	ქ	23	ჰ	34

განვიხილოთ კონკრეტული მაგალითი:

$q=5$ და $p=7$; მაშინ $N=q\times p=5\times 7=35$, $\varphi(N)=(p-1)\times(q-1)=(7-1)\times(5-1)=6\times 4=24$;

შეტყობინება M=(2....34), ავიღეთ ყველა შესაძლო ვარიანტი 35-მდე, რადგან მოდული არის 35. ღია გასაღები შევარჩიეთ 5 და დავშიფრეთ ყველა ციფრი 35-მდე. შედეგიდან ამოვიღეთ მოდული 35-ით.

მიღებული გავშიფრეთ იგივე ღია გასაღებით, მესამე პირის მიერ ცნობილი პარამეტრის საფუძველზე, ანუ საიდუმლო გასაღების გარეშე და მივიღეთ საწყისი შეტყობინება. აგრათვე დავადგინეთ კანონზომიერება, გაშიფვრის დროს პირველი ოთხი ციფრისათვის დაგვჭირდა უკუპროცესი, შემდეგმა სამმა ციფრმა მოგვცა თავისი თავი, ანუ გაშიფვრისათვის არ დაგვჭირდა უკუპროცესი და ა.შ. [4,6].

ყოველივე ზემოაღნიშნული თვალსაჩინოებისათვის მოცემულია ცხრილის სახით, იხ. ცხრილი 2.

დაშიფრვა-დეშიფაცია, როცა ღია გასაღები არის 5 **ცხრ.2**

ტექსტი	ხარისხი (გასაღები)	მოდული	დაშიფვრა ტექსტი5	Mod 35	გაშიფვრა mod 35	საწყისი ტექსტი
2	5	35	32	32	33554432	2
3			243	33	39135393	3
4			1024	9	59049	4
5			3125	10	100000	5
6			7776	6	7776	6
7			16807	7	16807	7
8			32768	8	32768	8
9			59049	4	1024	9
10			100000	5	3125	10
11			161051	16	1048576	11
12			248832	17	1419857	12
13			371293	13	371293	13
14			537824	14	537824	14
15			759375	15	759375	15
16			1048576	11	161051	16
17			1419857	12	248832	17
18			1889568	23	6436343	18
19			2476099	24	7962624	19
20			3200000	20	3200000	20
21			4084101	21	4084101	21
22			5153632	22	5153632	22
23			6436343	18	1889568	23
24			7962624	19	2476099	24
25			9765625	30	24300000	25
26			11881376	31	28629151	26
27			14348907	27	14348907	27
28			17210368	28	17210368	28
29			20511149	29	20511149	29
30			24300000	25	9765625	30
31			28629151	26	11881376	31
32			33554432	2	32	32
33			39135393	3	243	33
34			45435424	34	45435424	34

3. დასკვნა

1. როდესაც P და Q არის მარტივი რიცხვები და N არის მათი ნამრავლი, რომელიც გამოიყენება დაშიფვრა-გაშიფვრისათვის და N იცის მესამე პირმა, მხოლოდ ის ორი კონკრეტული P და Q დააკმაყოფილებს N-ის მნიშვნელობას. აქედან გამომდინარე, მესამე პირს შეუძლია იპოვოს P და Q, ასევე გამოთვალოს φ(N)-ის მნიშვნელობა. იცის ღია გასაღები და გამოთვლის საიდუმლოც;

2. მესამე პირისათვის ცნობილი პარამეტრების საფუძველზე, როგორიცაა ღია გასაღები და მოდული, შესაძლებელია შეტყობინების მიღება უკუპროცესით, ანუ საიდუმლო გასაღების გარეშე. მეთოდის დეშიფრაციაში, როცა შესაძლებელია უკუპროცესი, აქ უკვე საიმედოობა ანულირდება;

3. დაშიფრულ ინფორმაციაში გამოისახება კანონზომიერება, როდის არის საჭირო დეშიფრაცია და როდის არა, ანუ როდის რჩება დაშიფვრის შედეგად თავად ინფორმაცია;

4. აგრეთვე, მესამე პირს შეუძლია გაშიფვრის გარეშე, როდესაც იგი ხელთ ჩაიგდებს დაშიფრულ ინფორმაციას, მისთვის ცნობილი ღია გასაღებისა და დაშიფრული ინფორმაციის პერიოდულად შეკრება-გამოკლებით, მიიღოს საწყისი ინფორმაცია.

ლიტერატურა:

1. Shneier B. Applied Cryptography, John Wiley and Sons. Inc. New York. 1996
2. Шнайер Б. Прикладная криптография. М., Изд. ТРИУМФ. 2003
3. Андерсон Дж. Дискретная математика и комбинаторика. Изд. „Вильямс“. 2003
4. Питерсон У., Уэлдон, Э. Коды, исправляющие ошибки. I-II том. М., „Мир". 1976
5. Берлекэмп Э. Алгебраическая теория кодирования. М., Мир, 1971
6. Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования. М., Мир, 1978.

KRIPTOSISTEMIS ASYMMETRIC METHOD RSA-BREAK

Kotrikadze Gulnara, Rodjikashvili Ekaterine,
Jobava Zviad, Kandashvili Nugzar, Mamukashvili Teimuraz
Georgian Technical University

Summary

RSA cryptography method, a third illegal for consumers, it is possible to decipher a secret key known to him without any parameters, based on retreat decrypt the encrypted information and the initial reception. Besides, even without retreat based on the known parameters of a certain regularity of the initial information.

ВЗЛОМ RSA МЕТОДА АСИММЕТРИЧНОЙ КРИПТОСИСТЕМЫ

Котрикадзе Г., Рочикашвили Е.,
Джобава З., Кандашвили Н., Мамукашвили Т.
Грузинский Технический Университет

Резюме

В RSA методе криптографии, для третьего, незаконного потребителя возможно, без тайного ключа дешифровки, на основе известных ему параметров, обратным процессом, дешифровка шифрованной и получение исходной информации. Похититель информации без дешифрации шифрованной информации может также, на основе установленных нами закономерностей, получить начальное сообщение.