თანამედროვე კრიპტოგრაფიული მეთოდები

კახაბერ ჟამურაშვილი, რომან სამხარაძე
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განიხილება თანამედროვე კრიპტოგრაფიული მეთოდები, კერძოდ შემოთავაზებულია ღია და ასიმეტრული გასაღებების დაშიფრვის მეთოდები განხილული მათი დადებითი და უარყოფითი მხარეები, შედეგად შემოთავაზებული შიფრაციის თანამედროვე პრაქტიკული გადაწყვეტები. ღია გასაღების კრიპტოსისტემები ძირითადად გამოიყენება, როგორც ჰიბრიდული სისტემები, სადაც ინფორმაციის შიფრაცია/დეშიფრაციისათვის გამოიყენება სწრაფი სიმეტრიული ალგორითმები, ხოლო მისი გასაღების მართვისა და გადაცემისათვის გამოიყენება შედარებით ნელი ასიმეტრიული ალგორითმები. როგორც ვხედავთ, ცალმხრივი ფუნქციები ძირითადად წარმოადგენს რიცხვთა თეორიის ისეთ ამოცანებს, რომელთა ამოხსნის ალგორითმი არაპოლინომიურია. ამიტომ მოწინააღმდეგისათვის შეუძლებელი ხდება ღია გასაღებიდან საიდუმლო გასაღების აღდგენა, რაც წარმოადგენს ასეთი კრიპტოსისტემების საიმედოობის საფუძველს.

საკვანძო სიტყვები: კრიპტოგრაფული მეთოდები. ღია გასაღები. დახურული გასაღები.

1. შესავალი

ხშირად გვხვდება სიტუაციები, როდესაც ჩვენთვის არა იმდენად მთავარია ინფორმაციის კონფიდენციალურობის დაცვა, რამდენადაც იმის ცოდნა, მოაღწია თუ არა ჩვენამდე ინფორმაციამ შეუცვლელი სახით. მართლაც, ინტერნეტი შეიქმნა არა ინფორმაციის დასამალად, არამედ ინფორმაციის გასაცვლელად ადამიანებს შორის. ამიტომაც ამ შემთხვევაში მთავარია ინფორმაციის მთლიანობის პრობლემა, დამახინჯდა თუ არა ინფორმაცია (უნებლიედ თუ წინასწარი განზრახვით) ქსელში გადაცემის დროს და არა კონფიდენციალობის პრობლემა. ასევე შესაძლებელია სიტუაცია, როდესაც შეტყობინებას თქვენი პარტნიორის სახელით აგზავნის სრულიად სხვა პირი, ანუ ხდება იმიტაცია.

2. ძირითადი ნაწილი

ინფორმაციის მთლიანობისა და იმიტაციისაგან თავის დასაცავად საჭიროა გადაიჭრას ინფორმაციისა და ავტორობის იდენტიფიკაციისა და აუთენტიფიკაციის პრობლემა, რომელიც შეიძლება სულაც არ იყოს დაკავშირებული კონფიდენციალობის პრობლემასთან. ასევე ადვილი შესაძლებელია, რომ შეტყობინება გამოგიგზავნოთ ნამდვილად თქვენმა საქმიანმა პარტნიორმა, მაგრამ მეორე დღეს მან უარყოს ამ შეტყობინების ავტორობა. არც ეს მომენტი იქნება თქვენთვის სასიამოვნო, ამიტომ უნდა შეგეძლოთ დაუმტკიცოთ თქვენს პარტნიორს, რომ წერილი მის მიერ იყო გამოგზავნილი. ანუ შეტყობინების ავტორს ვერ უნდა შეეძლოს უარყოს თავისი ავტორობა.

ამ პრობლემის გადაჭრა სიმეტრიული კრიპტოგრაფიის საშუალებით არაეფექტურია, ამიტომ დღეს ასეთი ამოცანების გადასაჭრელად გამოიყენება ღია გასაღებიანი კრიპტოგრაფია . ღია გასაღებიან კრიპტოგრაფიაში გვაქვს ორი გასაღები, ერთი საიდუმლო (დეშიფრაციის გასაღები), რომელიც ცნობილია მხოლოდ ინფორმაციული ურთიერთობის ერთი სუბიექტისათვის და მეორე, ღია გასაღები (დაშიფრვის გასაღები), რომელიც ცნობილია ყველა დანარჩენი სუბიექტისათვის. ღია გასაღები გამოქვეყნებულია ქსელში და ნებისმიერ სუბიექტს შეუძლია დაშიფროს ამ გასაღებით

ინფორმაცია. დაშიფრული ინფორმაციის დეშიფრაცია შესაძლებელია მხოლოდ საიდუმლო გასაღებით, ამიტომ მხოლოდ ამ გასაღების მფლობელს შეუძლია გაშიფროს ინფორმაცია. ღია გასაღებიანი კრიპტოგრაფიის საფუძველს წარმოადგენს ე.წ. ცალმხრივ მიმართული ფუნქცია.

სიმეტრიული კრიპტოგრაფია იყენებს მეთოდებს, რომლის დროსაც ინფორმაციის გამგზავნი და მიმღები იყენებენ ერთსა და იმავე გასაღებს (იშვიათად სხვადასხვას, მაგრამ ამ შემთხვევაში ერთი გასაღები იოლად გამოითვლება მეორიდან). 1976 წლამდე ეს შიფრაციის ერთადერთი მეთოდი იყო.

თანამედროვე სიმეტრიული კრიპტოგრაფია დაკავშირებულია ძირითადად ბლოკურ შიფრებთან, ნაკადურ შიფრებთან და მათ გამოყენებასთან [1]. ბლოკური შიფრი ფაქტობრივად პოლიალფაბეტური შიფრის მოდიფიკაციაა: აიღება საწყისი ტექსტის გარკვეული სიგრძის ნაწილი (ბლოკი) და გასაღები, შედეგად მიიღება იგივე (იშვიათად განსხვავებული) სიგრძის შიფროტექსტი. შიფროტექსტის შემადგენელი ბლოკების ერთმანეთთან შერწყმისათვის გამოიყენება სხვადასხვა მეთოდები, რომლებსაც მთლიანობაში ქმედების რეჟიმი ეწოდება.

მონაცემთა შიფრაციის სტანდარტი(Data Encryption Standard – DES) და გაუმჯობესებული შიფრაციის სტანდარტი (Advanced Encryption Standard – AES) ბლოკური შიფრებია[2].

DES (და მისი ნაირსახეობა3DES) ჯერაც რჩება ერთერთ ყველაზე პოპულარულ ალგორითმად და ფართოდ გამოიყენება. თუმცა მისი გასაღების სიგრძის არასაკმარისობის გამო, ხდება მისი ჩანაცვლება სხვა, უფრო თანამედროვე ალგორითმებით.

დღემდე გამოგონილია მრავალი ბლოკური შიფრი, მათი უმეტესობა გატეხილია წარმატებული კრიპტოანალიზის შედეგად. ნაკადური შიფრი ქმნის განუსაზღვრელი სიგრძის გასაღებს, რომელიც შემდგომ უერთდება საწყის ინფრომაციას (ბიტობრივად ან ბაიტობრივად). გამომავალი ინფორმაცია დამოკიდებულია შიფრის შინაგან მდგომარეობაზე, რომელიც მოქმედების მიმდინარეობისას იცვლება. საწყისი მსგომარეობა დამოკიდებულია შიფრის გასაღებზე (ზოგიერთ ნაკადურ შიფრში ტექსტზეც). ნაკადური შიფრის მაგალითია RC4.კრიპტოგრაფიული ჰეშ-ფუნქციები (ტექსტის ანაბეჭდის ფუნქციები) კრიპტოგრაფიული ალგორითმების მნიშვნელოვანი კლასია. ისინი იღებს საწყის მნიშვნელობად ტექსტს და უკან აბრუნებს ფიქსირებული სიგრძის ჰეშს, რომლის დაკავშირება საწყის მნიშვნელობასთან პრობლემაა.

ასეთ ფუნქციებს ცალმხრივ ფუნქციებსაც ეძახიან. საუკეთესო ალგორითმებისათვის კოლიზიები (ორი ტექსტი, რომელთა ჰეში ერთი და იგივეა) რთული მოსაძებნი უნდა იყოს და ამის ალბათობა მინიმუმამდე უნდა იყოს დაყვანილი. შეტყობინების აუთენტიფიკაციის კოდები ჰეშ-ფუნქციების მსგავსია, იმ განსხვავებით, რომ ჰეშ-მნიშვნელობის შესამოწმებლად გამოიყენება საიდუმლო გასაღები.

ქსელში ყოველ სხვადასხვა წყვილს უწევს იქონიოს ცალკე გასაღები, რაც წყვილთა რაოდენობის გაზრდისას გასაღებების რაოდენობის კვადრატული პროპორციით გაზრდას იწვევს. ორ მოკავშირე მხარეს შორის გასაღების გაცვლა, მაშინ, როცა ჯერ არ არსებობს დაცული საკომუნიკაციო არხი, ,,კვერცხის და ქათმის'' პრობლემას ემსგავსება (გასაღების გაცვლა უნდა მოხდეს ფარულად, ფარულად გაცვლა ითხოვს დაშიფრვას, დაშიფრვა თავის მხრივ თხოულობს გასაღების გაცვლას და ა. შ.)

1976 წელს უიტფილდ დიფიმ და მარტინ ჰელმანმა წარმოადგინეს ასიმეტრიული კრიპტოგრაფია – კარდინალურად განსხვავებული კონცეფცია, რომელშიც გამოიყენება ორი

სხვადასხვა, მაგრამ მათემატიკურად ერთმანეთთან დაკავშირებული გასაღები – ღია და ფარული გასაღებები. ამავე დროს ფარული გასაღების მიღება ღია გასაღებიდან მოითხოვს კოლოსალურ გამოთვლით რესურსებს.

ასიმეტრიულ კრიპტოგრაფიაში ღია გასაღები შეიძლება ყველასთვის ცნობილი იყოს, ამავე დროს ფარული გასაღები საიდუმლოდ უნდა დარჩეს. ტიპურ შემთხვევაში ფარული გასაღები გამოიყენება შიფრაციის დროს, ხოლო ღია გასაღები დეშიფრაციის დროს. დიფიმ და ჰელმანმა ასევე წარმოადგინეს დიფი-ჰელმანის გასაღების გაცვლის პროტოკოლი.

1978 წელს კრიპტოგრაფების ჯგუფმა რონალდ რივესტის, ადი შამირის და ლენ ედლმანის შემადგენლობით შექმნეს მეორე ასიმეტრიული კრიპტოსისტემაRSA [5]. დიფი-ჰელმანის და RSA ალგორითმები დღეს ფართოდ არის გავრცელებული. არსებობს ასევე რამდენიმე სხვა კრიპტოსისტემა, რომელიც ღია გასაღების კონცეფციას იყენებს.

შიფრაციის გარდა ასიმეტრიული კრიპტოგრაფია გამოიყენება ციფრული ხელმო-წერებისათვისაც. ციფრული ხელმოწერა ჩვეულებრივ ხელმოწერას იმით წააგავს, რომ მისი მფლობელისათვის მისი შექმნა და განკარგვა მარტივია, ხოლო უცხო პირისათვის მისი დუბლირება – შეუძლებელი.

ციფრული ხელმოწერები გამოიყენება ორ ალგორითმში:

1) ხელმოწერა, სადაც ფარული გასაღები გამოიყენება ტექსტის ან ტექსტის ჰეშის შიფრაციისათვის;

2) შემოწმება, სადაც ღია გასაღების მეშვეობით ხდება დეშიფრაცია, მოწმდება ტექსტის ჰეში და ამდენად ტექსტის მთლიანობა და ხელმოწერის ნამდვილობა.

RSA და DSA წარმოადგნს ციფრული ხელმოწერის ყველაზე გავრცელებულ ალგორითმებს და ფართოდ გამოიყენება ისეთ პროტოკოლებში, როგორებიცაა SSL/TSL, VPN და სხვა.

3. დასკვნა

გასაღების მართვისა და გადაცემისათვის გამოიყენებაღია გასაღების კრიპტოსისტემები, რომელიც დაფუძნებულია „ძნელი“ პრობლემების გამოთვლით სირთულეზე. მაგალითადRSA ემყარება რიცხვის ფაქტორიზაციის პრობლემას (ანუ დიდი რიცხვის დაშლას მარტივ მამრავლებად), ხოლო დიფი-ჰელმანის ალგორითმი ეფუძნება დისკრეტული ლოგარითმების პრობლემას. ასეთი სისტემების უმეტესობაში ინტენსიურად გამოიყენება მოდულით გამრავლება და ახარისხება, შესაბამისად გაცილებით მეტი გამოთვლითი სიმძლავრეა საჭირო, ვიდრე სიმეტრიულ სისტემებში, რაც შესაბამისად კიდევ ურფო ართულებს დაშიფრული ინფორმაციის დეშიფრაციას და ზრდის შერჩეული მეთოდის სანდოობას.

ლიტერატურა - References - Литература:

1. Eneken Tikk, Kadri, Kaska, Liis Vihul. (2008). International Cyber Incidents: Legal Considerations. Cooperative Cyber Defence Centre of Excellence

2.Keir Giles. (2013). Electronic Warfare. US Joint Publication. Information Troops – a Russian Cyber Command .Conflict Studies Research Centre Oxford, UK.

3. Shneier B. (1996). Applied cryptography. John Wiley and Sons. Inc. New York.

4. Diffie W., Hellman M.E. (1976). New direction in cryptography. IEEE Trans. on Inf. Theory, v. IT-22, n.6., Nov. pp. 644-654.

5. Rivest R.L., Shamir A., Adleman L.M. (1978). A method for obtaining digital signature and public-key cryptosystems. Communications of the ACM, v.21, n.2. Feb. pp. 120-126, 1978.

MODERN CRYPTOGRAPHIC METHODS

Jamurashvili Kakhaber, Samkharadze Roman

Georgian Technical University

Summary

Modern cryptographic methods are discussed in the present article. In particular, methods of public and asymmetric key encryption are discussed as well as their advantages and disadvantages. As a result, modern, practical encrypting solutions are given. Public key cryptosystems are mainly used as hybrid systems, in which fast symmetric algorithms are used for encrypting/decrypting of information, while for the reason of managing and transmitting its key – relatively slow, asymmetric algorithms are used. As we can see, the one-way functions mainly represent such problems of number theory of which solution algorithm is non-polynomial. Therefore, it is impossible for the opponent to recover secret key using the public one wich is the basis for reliability of such cryptosystems.

СОВРЕМЕННЫЕ КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ

Жамурашвили К., Самхарадзе Р.
Грузинский Технический Университет

Резюме

Криптосистемы открытых ключей в основном используются в качестве гибридных систем, где для шифрования / дешифрования информации используются быстрые симметричные алгоритмы, а для управления и передачи ключей используются относительно медленные асимметричные алгоритмы. Как видно, односторонние функции в основном представляют такие задачи теории чисел, алгоритм решения которых неполиномный. Поэтому невозможно восстановить секретный ключ из открытого ключа, что является основой для обеспечения надежности таких криптосистем.