ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო

უნივერსიტეტი

მარიამ არჩვაძე

”ციფრული ხელმოწერის ორიგინალური ალგორითმი და მისი განხოციელება”

სამაგისტრო პროგრამა: ინფორმაციული სისტემები

მისანიჭებელი ხარისხი: ინფორმატიკის მაგისტრი

ხელმძღვანელი: **რიჩარდ მეგრელიშვილი**

ტექნ. მეცნიერებათა დოქტორი, პროფესორი,

ივანე ჯავახიშვილის სახელობის

თბილისის სახელმწიფო უნივერსიტეტი

თბილისი

2013

ანოტაცია

ნაშრომი ”ციფრული ხელმოწერის ორიგინალური ალგორითმი და მისი განხორციელება” წარმოადგენს ალტერნატიული ციფრული ხელმოწერის ალგორთმის აგების მცდელობას. ნაშრომში განხილული ციფრული ხელმოწერის თემატიკა დაკავშირებულია მაგისტრანტის ხელმძღვანელის მიერ ჩატარებულ კვლევებთან, წარმოადგენს ციფრული ხელმოწერის ალგორითმების შემდგომ შესწავლას, კვლევებს და მიღებული შედეგების პროტოკოლურ და პროგრამულ განხორციელებას. გამოკვლეული და მიღებულია ციფრული ხელმოწერის ალგორითმების ალტერნატიული ალგორითმი. როგორც სხვა ცნობილი სქემები, მოცემული ალგორითმიც წარმოადგენს ელგამალის ალგორითმის, როგორც პროტოტიპის, გარკვეულ მოდიფიკაციას. მთავარი არსი მდგომარეობს მასში რომ, ზოგიერთი პარამეტრის გარკვეულ ფუნქციონალური თვისების გამოყენებით, მიიღება საჭირო სტრუქტურული ალტერნატივა. როგორც სხვა ცნობილ და აღიარებულ შემთხვევებში-პროტოტიპში ერთი ელემენტის ცვლილებით მიიღება განსხვავებული სტრუქტურა, ჩვენს შემთხვევაშიც, პარამეტრის გარკვეული ფუნქციური თვისების გამოყენებით მიიღება ახალი სტრუქტურა, კერძოდ გამარტივებული და უფრო სწრაფქმედი. მიღებული ალტერნატიული ალგორითმის თვისობრივი უპირატესობა არის სიმარტივე და სწრაფქმედება.

Abstract

In the work “The original digital signature algorithm and its implementation”, an alternative algorithm for digital. The paper discussed issues related to the acquisition of the digital signature of the surveys, a digital signature algorithm further study, research and the results obtained from protocol and program implementation. signature is analyzed and obtained. Analogous to other well-known schemes, given algorithm is ElGamal. algorithm representing a certain modification of the prototype. The main idea is that by means of some functional properties of certain parameters, it’s possible to obtain needed structural alternative. Just as in other well-known and popular cases where a new structure is obtained by changing only one element in the prototype, we get more simplified and rapid structure with the aid of functional properties of the parameter. The main advantage of the obtained alternative algorithm is its simplicity and rapidness; however, it is less steady.

სარჩევი

შესავალი

წინამდებარე ნაშრომში გამოკვლეული და მიღებულია ციფრული ხლმოწერის ალგორითმების ერთ-ერთი ვარიანტი, რომლის თემატიკა დაკავშირებულია მაგისტრანტის ხელმძღვანელის მიერ ჩატარებულ კვლევებთან, წარმოადგენს ციფრული ხელმოწერის ალგორითმების შემდგომ შესწავლას, კვლევებს და მიღებული შედეგების პროტოკოლურ და პროგრამულ განხორციელებას. ციფრული ხელმოწერის ანუ აუთენტიფიკაციისა და ნამდვილობის თემატიკა აქტუალური საკითხია კრიფტოგრაფიაში. როგორც სხვა ცნობილი ალგორითმები, მოცემული ალგორითმიც წარმოადგენს ელგამალის ალგორითმის, როგორც პროტოტიპის გარკვეულ მოდიფიკაციას მთავარი აზრი მდგომარეობს მასში რომ ზოგიერთი პარამეტრის გარკვეული ფუნქციონალური თვისებების გამოყენებით მიიღება საჭირო სტრუქტურული ალტერნატივა.

როგორც სხვა ცნობილ და აღიარებულ შემთხვევებში, პროტოტიპში ერთი ელემენტის ცვლილებით და განსხვავებული ფუნქციური თვისებების გმოყენებით მიიღება ახალი სტრუქტურა, კერძოდ გამარტივებული და უფრო სწრაფქმედი. მაგალითად $S = (x+kRM) \bmod(p-1)$ ფორმულაში პირვანდელი სქემა გამარტივებულია და მიიღება საჭირო სტრუქტურა.

ციფრული ხელმოწერის ჩვენს მიერ განხილული ალგორითმის თვისობრივი უპირატესობა არის მისი განხორციელების კონსტრუქციულობა, სიმარტივე და სწრაფქმედება. ეს ალგორითმი განკუთვნილია ძირითადად იმ მომხმარებლებისათვის რომელთათვისაც მთავარი აქცენტი კეთდება სისწრაფეზე და არა სხვა რომელიმე პარამეტრზე.

როგორია კრიპტოგრაფიის მიზნები და პრობლემები? უპირველესად შევნიშნოთ, რომ კრიპტოგრაფიის ამოცანები დაისმის მხოლოდ იმ ინფორმაციისათვის, რომელიც საჭიროებს დაცვას. ასეთ შემთხვევებში ამბობენ, რომ ინფორმაცია შეიცავს საიდუმლოებას ან წარმოადგენს პრივატულს, კონფიდენციალურს და მოითხოვს დაცვას.

ინფორმაციის გასაიდუმლოების ყველაზე ტიპურ სფეროებს წარმოადგენს: სახელმწიფო, სამეხედრო, კომერციული, იურიდიული, სამედიცინო და ა.შ.

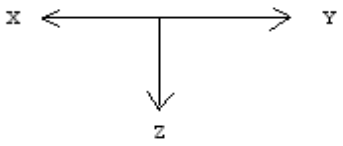
ქვემოთ საუბარი გვექნება ინფორმაციის შესახებ, რომლისთვისაც მხედველობაშია მიღებული შემდეგი გარემოებები:

 გვაქვს გარკვეული წრე კანონიერი მომხმარებლებისა, რომლებსაც აქვთ უფლება მოიხმარონ საიდუმლო ინფორმაცია.

 არის არაკანონიერი მომხმარებელი, რომელიც ცდილობს ხელში ჩაიგდოს საიდუმლო ინფორმაცია, რათა ის გამოიყენოს , საკუთარი ინტერესებისათვის კანონიერი მომხმარებლის საზიანოდ.

განვიხილოთ საშიშროება, როდესაც ადგილი აქვს დაცული ინფორმაციის გამჟღავნებას, თუმცა არსებობს დაცული ინფორმაციისათვის სხვა საფრთხეებიც: არაკანონიერი მომხმარებლის მიერ ჩანაცვლება, იმიტაცია, გაყალბება და სხვა.

დავუშვათ, რომ X და Y ინფორმაციის გაცვლის ორი მხარეა, ანუ ერთმანეთს დაშორებული ინფორმაციის ორი კანონიერი მომხმარებელია და ისინი ცვლიან ინფორმაციას კავშირის არხით. Z – არაკანონიერი მომხმარებელი (ანალიტიკოსი, ჰაკერი) ცდილობს ხელში ჩაიგდოს არხში გადაცემული საიდუმლო ინფორმაცია და გამოიყენოს თავის სასარგებლოდ.



ეს ფორმალური სქემა შეიძლება ჩაითვალოს ტიპურ სიტუაციად, სადაც გამოიყენება ინფორმაციის დაცვისა კრიპტოგრაფიული მეთოდები.

კრიპტოგრაფია – ეს არის სამეცნიერო-ტექნიკური დარგი, რომელიც უზრუნველყოფს ინფორმაციის გასაიდუმლოებას (უსაფრთხოებას). მისი ძირითადი ამოცანაა გადაწყვიტოს 4 ძირითადი პრობლემა: ინფორმაციის შიფრაცია-დეშიფრაცია, ანუ უსაფრთხოება-კონფედენციალურობა, აუთენტიფიკაცია, მთლიანობა და მონაწილეთა (მომხმარებლების) ურთიერთობის კონტროლი.

შიფრაცია – ეს არის მონაცემთა (ინფორმაციის) გარდაქმნა (ძირითადად მათემატიკური აპარატის მეშვეობით) არაწაკითხვად ფორმაში, შიფრაცია-დეშიფრაციის გასაღების მეშვეობით.

კრიპტოსისტემის საფუძველს შეადგენს: გარკვეული მეთოდოლოგია (პროცედურა) – იგი შედგება შიფრაცია-დეშიფრაციის ალგორითმისა და ერთი ან მეტი გასაღებისგან, რომელსაც იყენებს ალგორითმი. გასაღებების განაწილების შესაბამისი სისტემა. ღია (დაუშიფრავი) ტექსტი და დაშიფრული ტექსტის (შიფრო - ტექსტი). გასაღები არის ალგორითმის რეალიზაციის ერთ-ერთი კონკრეტული სახე. გასაღებთა სიმრავლის მაღალი რიგი წარმოქმნის სისტემის მედეგობას (მდგრადობას).

შემუშავებული მეთოდოლოგიით თავდაპირველად ღია ტექსტის მიმართ გამოიყენება შიფრაციის ალგორითმის გასაღები და მიიღება შიფრო ტექსტი. შემდგომ შიფრო - ტექსტი გადაიგზავნება დანიშნულების მხარეზე, სადაც ფაქტიურად იგივე გასაღები გამოიყენება დეშიფრაციისათვის, რათა მივიღოთ ღია ტექსტი.

ამ მეთოდოლოგიით შიფრაციის ალგორითმში განიხილება ღია ტექსტი გასაღებთან ერთად, რაც გვაძლევს შიფროტექსტს. ასეთი კრიპტოსისტემის უსაფრთხოება დამოკიდებულია გასაღების კონფიდენციალურობაზე, რომელსაც იყენებენ მოცემულ ალგორითმში და არა კრიპტოსისტემის ალგორითმის საიდუმლოებაზე.

საზოგადოდ კრიპტოალგორითმი საყოველთაოდ ცნობილია (ღიაა) და, შესაბამისად ამისა, კარგად აპრობირებული (მაგალითად, DES სტანდარტი DEA-ის ალგორითმით), მაგრამ გასაღები საიდუმლოა, რომელიც გარკვეული პერიოდის შემდეგ იცვლება.

ძირითადი პრობლემა მეთოდოლოგიაში დაკავშირებულია იმასთან, თუ როგორ დავაგენერიროთ და უსაფრთხოდ გადავცეთ გასაღები ინფორმაციის ურთიერთგაცვლის მონაწილეებს შორის.

ამავე დროს მნიშვნელოვანია, როგორ დავამყაროთ ინფორმაციის გადაცემის უსაფრთხო კავშირი მონაწილეებს შორის გასაღების გადაცემამდე? ამ პრობლემას წამოადგენს აუთენტიფიკაცია; რომელიც განიხილავს შემდეგ მნიშვნელოვან საკითხებს:

* შეტყობინებას (ინფორმაციას) აგზავნის სუბიექტი, რომელსაც სხვებისაგან განასხვავებს გარკვეული გასაღები. ის შეიძლება იყოს გასაღების ჭეშმარიტი მფლობელი, მაგრამ თუ სისტემა კომპრომეტირებულია, შეიძლება იყოს სხვა სუბიექტი (მაგალითად, მოწინააღმდეგე).
* როცა ინფორმაციის ურთიერთგაცვლის მონაწილეები გაცვლიან გასაღებს, მნიშვნელოვანია საკითხი იმის შესახებ, თუ რამდენად სანდოა მიღებული შედეგი, ანუ ვის ეკუთვნის გასაღები უფლებამოსლ პიროვნებას თუ მოწინააღმდეგეს?

არსებობს ორი სახის კრიპტოსისტემა: **სიმეტრიული** (საიდუმლო გასაღებით), როდესაც გასაღების გაცვლა X და Y მხარეებს შორის ხდება საიდუმლო არხით, ანუ კურიერის მეშვეობით; და **ასიმეტრიული** (ღია გასაღებით). ყოველი სისტემა იყენებს საკუთარ პროცედურას, გასაღებების ტიპს, მათი განაწილების მეთოდოლოგიას და შიფრაციის ალგორითმს.

სიმეტრიული კრიპტოსისტემის დროს გასაღები შიფარციის და დეშიფრაციისა ერთი და იგივეა, ხოლო ასიმეტრიული კრიპტოსისტემის დროს შიფრაციის გასაღები განსხვავდება დეშიფრაციის გასაღებისაგან.

სიმეტრიული კრიპტოსისტემის დროს დიდ პრობლემას გასაღების ფორმირება და მათი განაწილება წარმოადგენს, რადგან ყოველ წყვილ კანონიერ მომხმარებელს სჭირდება არა მარტო განსხვავებული გასაღები, არამედ კურიერი, რომლის მეშვეობითაც ხდება გასაღების გაცვლა (ეს კურიერის დამატებით საიმედოობის პრობლემას წარმოქმნის). ეს პრობლემა ბუნებრივად გადაწყვეტილია ასიმეტრიული კრიპტოსისტემის დროს: აქ კურიერი საჭირო არაა, რადგან დასაშიფრი გასაღები ღიაა და მისი მოხმარება

შეუძლია ყველას კანონიერ და არაკანონიერ მომხმარებელს (მოწინააღმდეგეს, ანალიტიკოსს, ჰაკერს), მაგრამ ღია გასაღებით დაშიფრული ინფორმაციის წაკითხვა შეუძლებელია, რადგან ღია გასაღებით შეუძლებელია საიდუმლო გასაღების მიღება. შესაბამისად, დაშიფრულ ინფორმაციას გაშიფრავს და წაიკითხავს მხოლოდ საიდუმლო მფლობელი (ანუ ვინც დააფორმირა საიდუმლო გასაღები).

შევნიშნოთ, რომ ისტორიულად კრიპტოგრაფიაში დამკვიდრდა ზოგიერთი სამხედრო ტერმინი (მოწინააღმდეგე, შეტევა ალგორითმზე და ა.შ.) კრიპტოგრაფია შეიმუშავებს ინფორმაციის გარდაქმნის მეთოდებს, რომელიც ხელს შეუშლის მოწინააღმდეგეს გაშიფროს საიდუმლო ინფორმაცია, ამიტომ კავშირის არხში გადაიცემა დაშიფრული ინფორმაცია და ამით მოწინააღმდეგის წინაშე დგას ალგორითმის (ანუ შიფრის) "გატეხვის" რთული ამოცანა:

შიფრის "გატეხვა" დაცული ინფორმაციის მოპოვებაა დაშიფრული შეტყობინებიდან გასაღების არცოდნის შემთხვევაში. თუმცა შიფრის "გატეხვისა" და გასაღების ხელში ჩაგდების გარდა მოწინააღმდეგეს (ჰაკერს) შეუძლია სხვა მეთოდებით მოიპოვოს დაცული ინფორმაცია. ცნობილი და პრაქტიკაში გამოყენებულია მეთოდი, როცა მოწინააღმდეგე სხვადასხვა საშუალებით შეძლებს დაიყოლიოს ერთ-ერთი კანონიერი მომხმარებელი და ამ აგენტის საშუალებით მოიპოვოს დაცული ინფორმაცია. ამ შემთხვევაში კრიპტოგრაფია უძლურია. Z მოწინააღმდეგეს შეუძლია არა მარტო მოიპოვოს დაცული ინფორმაცია, არამედ გაანადგუროს ან მოდიფიცირება გაუკეთოს ინფორმაციას ინფორმაციას გადაცემის პროცესში და ა.შ.

როგორც ვხედავთ, ერთი კანონიერი მომხმარებლისგან მეორე კანონიერ მომხმარებლისადმი კავშირის არხში გადაცემული ინფორმაცია უნდა იყოს დაცული სხვადასხვა მეთოდებით, რომელიც წინ აღუდგება მრავალ საშიშროებას. რასაკვირველია მოწინააღმდეგე (ანალიტიკოსი) შეეცდება იპოვოს ყველაზე სუსტი რგოლი, რათა ნაკლები დანახარჯებით მოიპოვოს ინფორმაცია. ეს უნდა გაითვალისწინონ კანონიერმა მოპმხმარებლებმა ინფორმაციის დაცვის დროს. რაც არ უნდა მდგრადი იყოს ინფორმაციის დაცვის მექანიზმის რომელიღაც რგოლი, ის ვერ დაიცავს სისტემას "გატეხვისაგან", თუ სხვა რომელიმე რგოლია სუსტი.

არ უნდა დაგვავიწყდეს ერთ-ერთი მთავარი პრობლემა: ინფორმაციის ფასი და ის ხარჯები, რომლითაც ვიცავთ ინფორმაციას (ან მოვიპოვებთ ინფორმაციას).

თანამედროვე ტექნიკის განვითარების კავშირის საშუალებანი, ინფორმაციის დაცვის მეთოდოლოგიები და მათი "გატეხვის" მეთოდები საკმაოდ ძვირადღირებულია.

სანამ გადავწყვეტთ, რომ დავიცვათ ინფორმაცია, პასუხი უნდა გავცეთ ორ შეკითხვას:

1) არის თუ არა ინფორმაცია მოწინააღმდეგისათვის უფრო ღირებული, ვიდრე შეტევის განხორციელების ფასი?

2) არის თუ არა ინფორმაცია ამდენად ღირებული, რომ მან გაამართლოს ინფორმაციის დაცვის საფასური?

ზემოაღნიშნული ითვალისწინებს ინფორმაციის შესაბამისი დაცვის მეთოდოლოგიის არჩევას. საერთოდ, კარგი შიფრის შერჩევა საკმაოდ შრომატევადი პროცესია. ამიტომ საჭიროა გავახანგრძლივოთ მისი "ცხოვრების დრო" და გამოვიყენოთ იგი რაც შეიძლება მეტი შეტყობინების დაშიფვრისათვის. თუმცა აქ არის საშიშროება, რომ მოწინააღმდეგე "გატეხავს" შიფრს და გამოიყენებს ინფორმაციას; მაგრამ თუ ალგორითმი (შიფრი) ითვალისწინებს ცვალებად გასაღებს (და, საზოგადოდ, ეს ასეა), გასაღების შეცვლისას მოწინააღმდეგეს თავიდან მოუწევს დაშიფრული ტექსტის ამოცნობის ანუ კრიპტოსისტემის "გატეხვის" მცდელობის განხორციელება.

გასაღების ქვეშ კრიპტოგრაფიაში, როგორც აღნიშნული იყო, იგულისხმება ალგორითმის (ანუ შიფრის) ცვალებადი ელემენტი, რომელიც გამოიყენება როგორც შეტყობინების შიფრაციის კონკრეტული საშუალება. საზოგადოდ, ინფორმაციის უსაფრთხოება განისაზღვრება უპირველესად გასაღებით. თვით შიფრი და შიფრაციის პრინციპები საყოველთაოდ ცნობილია და, რასაკვირველია, იცის მოწინააღმდეგემ (ანალიტიკოსმა), მაგრამ მისთვის უცნობია შიფრის გასაღები, რომლითაც ხდება ესა თუ ის კრიპტოგრაფიული გარდაქმნები. აქედან გამომდინარეობს, რომ, ვიდრე კანონიერი მომხმარებლები გაცვლიან დაშიფრულ ინფორმაციას, მანამ მხარეებმა მოწინააღმდეგისაგან ფარულად უნდა გაცვალონ გასაღებები. მოწინააღმდეგე ცდილობს

განსაზღვროს შიფრის გასაღები, რაც საშუალებას მისცემს წაიკითხოს დაშიფრული შეტყობინება.

აღვნიშნოთ, რომ არ არსებობს ერთიანი შიფრი რომელიც გამოსადეგი იქნება ყველა შემთხვევაში. შიფრაციის მეთოდი დამოკიდებულია ინფორმაციის თავისებურებაზე, მის ფასზე და მფლობელის შესაძლებლობაზე. არსებობს უამრავი სხვადასხვა სახის დასაცავი ინფორმაცია: დოკუმენტური, სატელეფონო, სატელევიზიო, კომპიუტერული და ა.შ. ინფორმაციის ყველა სახეობას გააჩნია თავისი სპეციფიკა და ეს განსაზღვრავს დაშიფვრის შესაბამის სახეს. დიდი მნიშვნელობა აქვს ინფორმაციის რაოდენობას და შიფრაციის სიჩქარეს. ასევე დიდი მნიშვნელობა აქვს იმას თუ რამდენ ხანს წარმოადგენს ინფორმაცია აქტუალურს.

თავი I

კრიპტოგრაფიის განვითარების ისტორიული და მეთოდოლოგიური მიმოხილვა

1.1 კრიპტოგრაფიის განვითარების ეტაპები

ინფორმაციის გასაიდუმლოება–დაცვა მისი გარდაქმნის მეშვეობით, რომელიც გამორიცხავდა მის წაკითხვას გარეშე პირის მიერ, აინტერესებდა კაცობრიობას უხსოვარი დროიდან. ინფორმაციის ამ საიდუმლო გადაქმნას ეწოდება კრიპტოგრაფია.

კრიპტოგრაფიის ისტორია – მეტყველების ისტორიის ხნისაა. თავდაპირველად დამწერლობა წარმოადგენდა კრიპტოგრაფიულ სისტემას, რადგან მას ფლობდნენ მხოლოდ რჩეულები: ძველი ეგვიპტისა და ძველი ინდოეთის წმინდა წიგნები და სხვა.

კრიპტოგრაფიის ისტორია პირობითად შეიძლება დაიყოს ოთხ ეტაპად:

- გულუბრყვილო კრიპტოგრაფია;
- ფორმალური კრიპტოგრაფია;
- მეცნიერული კრიპტოგრაფია;
- კომპიუტერული კრიპტოგრაფია.

გულუბრყვილო კრიპტოგრაფიისათვის (XVI საუკუნის დასაწყისამდე) დამახასიათებელი იყო პრიმიტიული მეთოდები ინფორმაციის დაშიფრისათვის. გამოყენებული შიფრების უმეტესობა დაიყვანებოდა მონოალფავიტურ გადანაცვლებაზე. პირველი მაგალითი დაფიქსირებული მეთოდისა არის ცეზარის შიფრი მოცემული ტექსტის ყოველი ასოს სხვა ასოთი ჩანაცვლებით, რომელიც მოცემული ასოსაგან დაშორებულია ფიქსირებული რაოდენობის პოზიციით (ანბანის ყოველ სიმბოლოს

შეესაბამება გარკვეული რიცხვი. მაგალითად, ანბანში მისი ადგილის შესაბამისი ნომერი. ტექსტის ყოველ სიმბოლოს ემატება ფიქსირებული სიმბოლო – იკრიბება მათი შესაბამისი რიცხვები ფიქსირებული მოდულით, რომლიც ტოლია ანბანში სიმბოლოების რაოდენობისა). ბუნებრივია ტექსტის დაშიფვრის შემდეგი იდეა: მოცემულ ტექსტურ სიტყვებში და მთლიანად წინადადებებში ასო-ნიშნებს შევუცვალოთ ადგილები. პოზიციების ცვლილება, ცხადია, გამოიწვევს ტექსტში ასო-ნიშნების არევას და ტექსტის შინაარსის გაბუნდოვნებას, რაც განსაზღვრების თანახმად არის ტექსტის გარდაქმნა, ანუ დაშიფვრა. ასეთიი დაშიფვრის წესია იულიუს ცეზარის ალგორითმი, რომელიც თავის მხრივ წარმოადგენს იმ დროის არსებული ალგორითმის ერთ-ერთ ვარიანტს.

წარმოვიდგინოთ, რომ ი. ცეზარი თავის გზავნილში ლათინური ანბანის პირველ A ასოს შეცვლიდა, ვთქვათ, მეოთხე D ასო-ნიშნით, მეორე B ასოს – მეხუთე E ასო-ნიშნით და ა.შ. ბოლო Z ასოს მესამეთი (სურ. 1.1.) ამრიგად, თუ პირველ სტრიქონში ჩავწერთ ლათინური ანბანის ასო-ნიშნებს ჩვეულებრივი რიგის მიხედვით, ხოლო მეორე სტრიქონში დავალაგებთ შიფრის შესაბამისი ასო-ნიშნებს, მივიღებს დაშიფვრის ალგორითმს:

ABCDEFGHIJKLMNOQRSTUVWXYZ

DEFGHIJKLMOPQRSTUVWXYZABC

ნახ 1.1. ცეზარის ალგორითმი

ი. ცეზარის ალგორითმში გასაღებს განსაზღვრავს გადანაცვლების წესი, კერძოდ ის რომ ყოველი ასო-ნიშანი ანბანურ მწკრივში გადაინაცვლებს სამი პოზიციით, ანუ, საზოგადოდ, – k პოზიციით, სადაც $k \in \{1,2, ,26\}$ (ი. ცეზარის ალგორითმში k =3). ცხადია, რომ შესაძლებელია გადანაცვლბის წესის გართულება, ვთქვათ სპეციალური ცხრილების (მატრიცების) შემოღება და სხვ.

მეორე შიფრი არის პოლიბეიის კვადრატი, რომელიც შექმნა ბერძენმა მწერალმა პოლიბიიმ. ეს მეთოდი წარმოადგენს ზოგად მონოალფავიტურ გადანაცვლებას

(კვადრატული ცხრილი 5X5 შევსებულია ბერძნული ალფავიტის შემთხვევითი განლაგებით. საწყისი ტექსტის ყოველი ასო ჩანაცვლდება კვადრატის შესაბამისი პოზიციით).

ფორმალური კრიპტოგრაფიის ეტაპი (XV საუკუნე – XX საუკუნის დასაწყისი) დაკავშირებულია ფორმალიზირებულ და შედარებით მდგრად ხელის (არამექანიკურ) კრიპტოშიფრებთან. ევროპულ ქვეყნებში ეს ეტაპი ემთხვევა აღორძინების ეპოქას, რომლის დროსაც მეცნიერებისა და ვაჭრობის მდგრადმა ზრდამ გამოიწვია მოთხოვნილება ინფორმაციის დაცვის საიმედო საშუალებებზე. ამ ეტაპზე განსაკუთრებული როლი ენიჭება იტალიელ არქიტექტორს ლეონ ბატისტა ალბერტს, რომელსაც ეკუთვნის პირველი მრავალ ალფავიტური გადანაცვლების მეთოდი. ეს შიფრი ცნობილია აგრეთვე ვიჟინერის სახელით (ბლეს ვიჟინერი – XVI საუკუნის დიპლომატი).

ვიჟინერმა (1586 წ) განავითარა ცეზარის ალგორითმი. ეს მოხდა ორი მიმართულებით.

ცეზარის ალგორითმში ტექსტის ყოველი ასო-ნიშანი ანბანში გადაადგილდება პოზიციათა ერთსა და იმავე რაოდენობით, რათა მივიღოთ დაშიფრული ტექსტი (k სიდიდე მუდმივია ყოველი ასო-ნიშნისათვის). ცხადია, ჩნდება აზრი რომ გადანაცვლება მოვახდინოთ არა მუდმივი სიდიდით, არამედ განსხვავებული წესით. ვთქვათ, პირველი ტექსტური ასო-ნიშნი გადაადგილდეს k_1 პოზიციით, მე-2-ე k_2 პოზიციით და ა.შ. შეიძლება შემოვიღოთ l სიგრძის k= k_1, , k_1 გასაღები , ანუ l სიგრძის გარკვეული სიტყვა ან l სიგრძის მთელი წინადადება.

მეორე მიმართულება გულისხმობს გარკვეული მატრიცის აგებას, რომელიც განახორციელებს დაშიფვრას. ასეთია ვიჟინერის მიერ შემოთავაზებული ალგორითმი, ანუ ცეზარის მოდიფიცირებული შიფრი.

მოსახერხებელია, რომ ასო-ნიშანთა განხილული გადანაცვლება ჩავწეროთ შემდეგი სახით. დავუშვათ, რომ ანბანის ასო-ნიშნებს შევუსაბამეთ რიცხვები ანბანში მათი რიგის პოზიციის მიხედვით (ქართული ანბანისათვის 1-დან 33-მდე). ღია ტექსტი განვათავსოთ

პირველ სტრიქონში, როგორც ცეზარის ალგორითმშია. მეორე სტრიქონში ჩავწეროთ ჩვენ მიერ შერჩეული "სიტყვა გასაღები" განმეორებით იმდენჯერ, რასაც მოითხოვს ტექსტი.

საინტერესოა ალგორითმი რომელიც მიიღო ვერნამმა.

ზემოთ განხილულ ალგორითმებს აერთიანებს საერთო იდეა, რომლის მიხედვით ტექსტის გარდაქმნისათვის (ანუ, საზოგადოდ, ტექსტის სიმრავლის სხვა სიმრავლეზე ასახვისათვის) გამოყენებულია გადანაცვლების ან ჩანაცვლების ჩვეულებრივი მათემატიკური ოპერაციები.

გ. ვერნამის ალგორითმი წარმოადგენს ცეზარის და ვიჟინერის ალგორითმების შემდგომ განვითარებას (1917). შესაძლოა გვეფიქრა, რომ სიტყვა "განვითარების" ხმარება აქ თავისი სრული მნიშვნელობით არც არის გამართლებული, იმდენად მარტივია ალგორითმის მიღება. მაგრამ, თუ გავითვალისწინებთ, რომ ვერნამის ალგორითმი არის ერთადერთი სრულყოფილი ალგორითმი, რომელიც აკმაყოფილებს კ. შენონის მიერ შემუშავებულ კრიტერიუმებს, გასაგები გახდება ალგორითმის მნიშვნელობა.

ვერნამის შიფრის სიმარტივე იმაში მდგომარეობს, რომ, თუ ცეზარის ალგორითმში გასაღების სიგრძეა k, ხოლო ვიჟინერის ალგორითმში გასაღების სიგრძე გარკვეული სიდიდეა (l >1), რომელიც, საზოგადოდ, გაცილებით ნაკლებია ტექსტის სიგრძეზე, და მეორდება შიფრაციის დროს, ვერნამის ალგორითმში გასაღების სიგრძე ტექსტის სიგრძის ტოლია და გამოიყენება მხოლოდ ერთჯერადად.

ალგორითმი შეიძლება შემდეგი სახით ჩავწეროთ. ვთქვათ, ანბანის ასო-ნიშნების, ციფრების, სასვენი და სხვა ნიშნების ერთობლიობა შეადგენს $a_i \in A$ სიმბოლოების სიმრავლეს, რომლის სიმძლავრეა N. ამ სიმრავლის ყოველ ასო-ნიშანს შევუსაბამოთ m_i რიცხვი; $m_i \in \{0,..., N-1\}$. დავუშვათ, რომ მოცემული M ღია ტექსტური a_1, a_2, a_3, შეტყობინება, C სპეციალური c_1, c_2, c_3... ტექსტით (გასაღებით) დაშიფვრის შემდეგ ღებულობს B შიფროტექსტის, ანუ b_1, b_2, b_3… მიმდევრობის სახეს. M ტექსტის a_{vi} სიმბოლოს შეესაბამება m_{vi} რიცხვითი მნიშვნელობა, C გასაღების c_{ui} სიმბოლოს-m_{vi} მნიშვნელობა, ხოლო B შიფროტექსტის b_{wi} სიმბოლოს-m_{wi} მნიშვნელობა, სადაც v_i, u_i, w_i, $\in \{0,...,N-1\}$. მაშინ თითოეული სიმბოლოს დაშიფვრა და დეშიფრაცია

$$m_{vi} + m_{ui} \equiv m_{wi} \pmod N,$$

$$m_{wi} + m_{ui} \equiv m_{vi} \pmod N$$

შესაბამისობებით განხორციელდება.

ცხადია, რომ ყოველი დაშიფვრის და დეშიფრაციის შემდეგ C სპეციალური სიმბოლოების ტექსტი, რომელიც მხოლოდ გადამცემ და მიმღებ მხარეებს გააჩნია, უნდა განადგურდეს.

ვერნამის შიფრი განსაკუთრებულ შემთხვევაში გამოიყენება. მაგალითად, ამ შიფრით სარგებლობდენ ამერიკისა და საბჭოთა კავშირის პრეზიდენტები. მთავარ პრობლემას მისთვის წარმოადგენს სინქრონიზაციისა და C გასაღების ფორმირების ამოცანა. ზოგჯერ C გასაღებს ფსევდოშემთხვევითი მიმდევრობის და ზოგჯერ კი გარკვეული მხატვრული ნაწარმოების მკაცრად შეთანხმებული ტექსტის სახე აქვს (რაც მარტივად ხორციელდება).

XIX საუკუნეში ჰოლანდიელმა კერკჰოპსმა ჩამოაყალიბა კრიპტოგრაფიის ძირითადი წესი: შიფრის მედეგობა უნდა განისაზღვრებოდეს მხოლოდ გასაღების საიდუმლოებით. ინფორმაციის გამტაცებელს ან კრიპტოანალიტიკოსს შეუძლია, იცოდეს ყველა მონაცემი, გარდა გასაღებისა. ითვლება, რომ კრიპტოსისტემა გატეხილია, თუ გამტაცებელს დასაშვებზე მეტი ალბათობით შეუძლია შემდეგი ოპერაციის ჩატარება: საიდუმლო გასაღების პოვნა, გარდაქმნის ალგორითმის ეფექტური შესრულება, რომელიც ფუნქციონალურად ექვივალენტურია საწყისი კრიპტოალგორითმისა. იმისათვის რომ კრიპტოსისტემა გატეხილად ჩაითვალოს, საჭიროა არა მხოლოდ გასაღების გახსნის (ანუ საიდუმლო გასაღების პარამეტრის მიღების) ალგორითმის ჩვენება, არამედ იმის ჩვენებაც, რომ ეს ალგორითმი შეიძლება შესრულდეს რეალურ დროში. ალგორიმის გახსნის სირთულე ითვლება კრიპტოსქემის ერთ-ერთ მთავარ მახასიათებლად და მას კრიპტომედეგობა ეწოდება.

მეოცე საუკუნის დასაწყისიდან კრიპტოგრაგფიული პროცესების ავტომატიზაციის მიზნით გამოიგონეს მოწყობილობები (მანქანები), რომლებშიც გამოყენებულია მბრუნავი როტორები. როტორს აქვს დისკოს ფორმა. მასზე სათანადო პოზიციებში ასო-ნიშნების განთავსება (ანუ ტექსტის ჩაწერა) და როტორების გარკვეული წესით შეერთება იწვევს ანბანის ასო-ნიშნების გადანაცვლება-ჩანაცვლებას, როგორც ეს ხდება ვიჟინერის ალგორითმში.

მაგალითად, ვთქვათ ღია ტექსტია:

“თუ ტექსტს არ დავშიფრავ მოწინააღმდეგე დაგვამარცხებს”;

მაშინ სათანადო ანაკრები დისკოზე არის:

თუტექსტსარ

დავშიფრავმო

წინააღმდეგ

ედაგამარცხ

ებს.

ხოლო დაშიფრული ტექსტია:

“თდწეეუაიდბტშნასეიაგქფაასრღმტამასვდრამეცრგოხ”.

აქ გამოყენებული გადაინაცვლება ადვილად შეიძლება გაიშიფროს, თუ პირველი “თ” ასოს შემდეგ წავიკითხავთ მეექვსე”უ” ასოს, შემდეგ მე-11 “ტ” ნაცვლად მე-16 “ე”-ს და ა.შ. ასო-ნიშნები შეიძლება ამოვიკითხით შიფროტექსტის იმ პოზიციებზე, რომლებიც ერთმანეთისგან დაშორებულია გარკვეული ინტერვალებით. ამიტომ როტორულ მანქანებში ითვალისწინებენ, აგრეთვე, ღია ტექსტის ასო-ნიშნების სხვა ასო-ნიშნებით ჩანაცვლებას. მაგალითად, ვთქვათ, პირველ როტორზე “ა” ჩაიწრება როგორც “კ”, ”ბ” როგორც “ლ” და ა.შ.; მეორე როტორზე იგივე “ა” ჩიწერება როგორც “ტ”, “ბ” როგორც

“ტ” და ა.შ. ამრიგად, ტექსტის ასო-ნიშნები წანაცვლებასთან ერთად აღმოჩნდება ჩანაცვლებული სხვა ასო-ნიშნებით განსხვავებული წესით.

ყველაზე ცნობილი როტორული მანქანა იყო “ენიგმა”, რომელიც შექმნა ევროპაში 1917 წელს და მისი გაუმჯობესებული ვარიანტი გამოიყენეს გერმანელებმა მეორე მსოფლიო ომში (გარდა გერმანული ვარიანტისა იმჟამად არსებობდა ამერიკული Sigama, ინგლისური Typex, ლათინური Red, Orange და Purple). პირველად “ენიგმა” გატეხეს პოლონელმა კრიპტოგრაფებმა და აცნობეს ინგლისელ კრიპტოანალიტიკოსებს, რომლებმაც განაგრძეს ახალი ვერსიების კრიპტოანალიზი.

მეოცე საუკუნის 60-იან წლებში მოწინავე კრიპტოგრაფიულმა კვლევებმა შექმნეს ბლოკური შიფრი, რომელიც უფრო მედეგია როტორულ კრპტოსისტემებთან შედარებით, თუმცა მისი რეალიზაციისათვის სჭიროა ციფრული ელექტრონული მოწყობილებანი.

კომპიუტერული კრიპტოგრაფია (XX 70-იანი წლებიდან) მთლიანად ჩამოყალიბდა გამოთვლითი საშუალებების (კომპიუტერი) განვითარების გარკვეული დონის პირობებში, როცა შესაძლებელი გახდა დიდი სიჩქარით რამდენიმე რიგით უფრო მედეგი კრიპტოსისტემის მიღება, ვიდრე ეს შესაძლებელი იყო “ხელის” ან “მექანიკური” შიფრაციის დროს.

პირველი კრიპტოლოგიური სისტემა, რომლის პრაქტიკული გამოყენება შესაძლებელი გახდა მძლავრი და კომპაქტური გამოთვლითი სშუალებების დროს (კომპიუტერი), არის ბლოკური შიფრები. 70-იან წლებში შემუშავებულ იქნა ამერიკული შიფრაციის სტანდარტი DES.

70-იანი წლების ნახევარში მოხდა გარღვევა თანამედროვე კრიპტოგრაფიაში – შეიქმნა შიფრაციის ასიმეტრიული კრიპტოსისტემა, რომელიც არ ითხოვდა საიდუმლო გასაღებების გადაცემას ინფორმაციის გაცვლის მხარეებს შორის. აქ ათვლის წერტილად ითვლება დიფი და ჰელმანის ნაშრომი “ახალი მიმართულებანი თანამედროვე კრიპტოგრაფიაში” (1976წ.). ამ ნაშრომში პირველად იყო ფორმულირებული დაშიფრული ინფორმაციის გაცვლის პრინციპები საიდუმლო გასაღების გარეშე.

შეტყობინება წარმოადგენს ღია ტექსტს, რომელსაც, საზოგადოდ შეიძლება ჰქონდეს ბუნებრივენოვანი ტექსტის ან გარკვეული სიმბოლოებისა და გამოსახულებების ერთობლიობის სახე (გამოთვლით ტექნიკასა და ინფორმაციულ სისტემებში ტექსტური ინფორმაციის ჩასაწერად ძირითადად გამოიყენება ორობითი სიმბოლოების n-მიმდევრობები, ანუ სასრულ GF(2) ველზე განსაზღვრული n განზომილებების ვექტორები). გასაიდუმლოების მიზნით ღია ტექსტის გარდაქმნას ეწოდება დაშიფვრა (შიფრაცია), ხოლო დაშიფრული ტექსტიდან ღია ტექსტის აღდგენას - დეშიფრაციას. შიფრაციისა და დეშიფრაციის მეთოდებისა და ალგორითმების კვლევას კრიპტოანალიზი ეწოდება, ხოლო მათემატიკის დარგს, რომელიც სწავლობს კრიპტოგრაფიასა და კრიპტოანალიზს – კრიპტოლოგია.

კრიპტოგრაფიულ ალგორითმს, როგოც წესი, აქვს გარკვეული მათემატიკური ფუნქციის სახე, რომელსაც, აგრეთვე შიფრსაც უწოდებენ.

კრიპტოგრაფიაში არ არის მიღებული საკუთრივ ალგორითმის (შიფრის) დამალვა-დასაიდუმლოება, თუმცა ასეთი მიდგომის მართებულობა კერძო შემთხვევაში არ არის გამორცხული.

ალგორითმის არა დასაიდუმლოება გაუმართლებელია იმის გამო, რომ მისი გამჟღამვნება გამოიწვევს დაშიფრული ტექსტის, ანუ, რგორც მას ასევე უწოდებენ, შიფროტექსტის გაშიფვრას. მას შემდეგ, რაც ალგორითმის გატეხვის ფაქტი ცნობილი გახდება, საჭიროა მთლიანად ახალი ალგორითმის შემუშავება, რაც ცხადია, გარკვეულ სირთულესთან არის დაკავშირებული. ამიტომ, ჩვეულებრივ, მიმართავენ სხვა მიდგომას. ამ მიდგომით იგულისხმება, რომ ალგორითმს სინთეზის დროს, კრიპტოგრაფი ქმნის ალგორითმის (შიფრს) ალტერნატიული განხორციელების უამრავ ვარიანტს (გასაღებების სიმრავლეს) და მოცემული სამოქმედო პერიოდისათვის შეირჩევს ერთ-ერთ მათგანს. ალტერნატიული ვარიანტის შერჩევა დაკავშირებულია გასაღების შერჩევაზე.

ზემოაღნიშნული შეიძლება განვიხილოთ სეიფის მაგალითზე. სეიფის დაცვის მოცემული წესი წარმოადგენს გარკვეული ალგორითმის განხორციელებას, ე.ი. ალგორითმის განხორციელებაა საიფზე განთავსებული (შესაძლოა რამდენიმე დისკოს სახის) და მათზე გამოსახული ციფრთა ანაკრები (გარკვეული კომბონაცია), რიცხვი

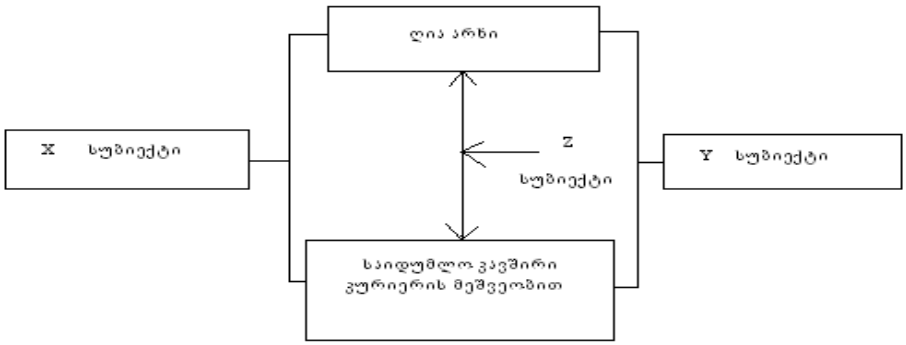
(გასაღები), რომელიც საიდუმლოა; მაგრამ ალგორითმი ღიაა. საჭიროების შემთხვევაში და დროის გარკვეული პერიოდის გავლის შემდეგ, შესაძლებელია გასაღების, ანუ შესაბამისი რიცხვის შეცვლა, რაც ადვილად განსახორციელებელია. პრინციპულად, ანალოგიურია ზოგადი მიდგომა თანამედროვე კრიპტოგრაფიაში.

განხილულ შემთხვევაში ციფრების ანაკრებთა საერთო რაოდენობა, ძირითადად, ქმნის კრიპტოგრაფიული დასაიდუმლოების მედეგობას. თანამედრვე კრიპტოგრაფიაში მედეგობის საიმედო ქვედა საზღვრად ითვლება $\approx 10^{30}$ მნიშვნელობა. სეიფის მოცემული მაგალითის მიხედვით სათანადო მედეგობის მისაღებად საჭიროა 30-თანრიგიან ელემენტთა ერთობლიობა, იმ პირობით რომ თითოეული თანრიგის ელემენტმა შეძლება მიიღოს ციფრების ნებისმიერი მნიშვნელობა.

1.2. კრიპტოგრაფიული მეთოდები და სისტემები

განვიხილოთ ინფორმაციის გაცვლის უმარტივესი მოდელი. ინფორმაციის გადამცემი და მიმღები მხარეები პირობითად ავღნიშნოთ როგორც X და Y სუბიექტები (შევნიშნოთ, რომ შესაძლებელია ამ ზოგად მოდელში ინფორმაციის გადამცემი იყოს Y-ი ან ორივე მხარე ახორციელებდეს ინფორმაციის გადაცემას და მიღებას).

სურათზე მოცემულია, პირობითად, ორ X და Y სუბიექტებს შორის ინფორმაციის კრიპტოგრაფიული გაცვლის პრინციპული სქემა. Z სუბიექტი განიხილება, როგორც X და Y სუბიექტების მოწინააღმდეგე მხარე.



ნახ 1.2. ინფორმაციის გაცვლის პრინციპული სქემა

საზოგადოდ X და Y ორივე მხარე დაინტერესებულია, რომ დაიცვას საიდუმლო; მათი მოქმედება მიზანდასახულია და ურთიერთშეთანხმებას ეფუძნება. Z მხარე (ანალიტიკოსი ან ჰაკერი) დაინტერესებულია ხელი შეუშალოს X და Y სუბიექტებს ინფორმაციის საიდუმლოების დაცვაში (ეს მისი პირდაპირი ამოცანაა), გახსნას დაშირული ინფორმაცია და, უფრო მეტიც, გამოიყენოს ინფორმაციის გაცვლის ფაქტი თავის სასარგებლოდ (შეცვალოს ინფორმაციის შინაარსი ადრესატი და სხვ.) თუმცა, კრიპტოგრაფიულ სისტემაში შესაძლებელია მიღებული ინფორმაციის სანდოობის მართვა და შემოწმება.

კრიპტოგრაფიული სისტემების მთავარი ინფორმაციის გარდაქმნა და X სუბიექტისაგან Y სუბიექტისთვის ისე გადაცემა, რომ იგი გაუგებარი და გამოუყენებადი იყოს ნებისმიერი Z სუბიექტისათვის. ეს არის ინფორმაციის საკუთრივ დასაიდუმლოების (დაშიფვრის) პრობლემა. მაგრამ ან ძირითად ამოცანის გარდა კრიპტოგრაფიას აქვს სპეციალური ამოცანები, რომელთა შორისაა:

ნამდვილობა (აუთენტიფკაცია). ინფორმაციის მიმღებს უნდა შეეძლოს შეამოწმოს შეტყობინების **ნამდვილობა (სანდოობა, დამაჯერებლობა)**, ხოლო ბოროტგანმზრახველს არ უნდა შეეძლოს ჩაერთოს შეტყობინების გადაცემის პროცესში და შეინიღბოს ვისიმე

სახელით. ნამდვილობის შესრულება დაკავშირებულია **ციფრული ხელმოწერის** და **კრიპტოგრაფიული პროტოკოლების** განხორციელებასთან.

მთლიანობა. მიმღებს უნდა შეეძლოს შეამოწმოს და გაარკვიოს, ხომ არ არის შეცვლილი შეტყობინება (გადაცემის პროცესში), ხოლო ბოროტგანმზრახველს არ უნდა შეეძლოს შეცვალოს ჭეშმარიტი შეტყობინება ყალბით.

ავტორობის ვერუარყოფა. გამგზავნს არ უნდა შეეძლოს უარყოს შეტობინების გზავნილობა; ანუ, თუ ეს საჭიროა, შესაძლებელია, რომ გამგზავნის ავტორობა ცალსახად დაფიქსირდეს.

ფარულობა. ეს მოთხოვნა შეიძლება შევადაროთ ფულადი ნიშნების (კუპიურების) მიმოქცევის პროცესს; ყოველ ფულად ნიშანს აქვს თავისი უნიკალური ნომერი, მაგრამ, საზოგადოდ, არ ხდება იმის გაკონტროლება, თუ ვინ ისარგებლა ფულადი კუპიურით და რა ანგარიშსწორების დროს; ანალოგიურად, აუცილებელია ინფორმაციულ ოპერაციაში მონაწილეთა დაცვა გარეშე თვალთვალისაგან.

კრიპტოგრაფიული მეთოდები შეიძლება ორ ძირითად კლასად დავყოთ:

1) მეთოდები, რომლებიც X და Y სუბიექტებს შორის კავშირს ახორციელებს საიდუმლო კურიერის მონაწილეობით და

2) მეთოდები, რომლებიც არ საჭიროებს კურიერის დახმარებას, ანუ კავშირი ხორციელდება მხოლოდ ღია არხის გამოყენებით.

პირველი კლასის მეთოდებს **სიმეტრიულ** მეთოდებს (სისტემებს) უწოდებენ, რაგდან X და Y სუბიექტებს შორის კავშირი ხორცელდება პრინციპულად ერთისა და იმავე გასაღების გამოყენებით. მეორე კლასის მეთოდებს უწოდებენ **ასიმეტრიულს,** რადგან X და Y სუბიექტებს შორის კავშირი ხორციელდება გასაღებით და ერთი გასაღებიდან მეორის მიღება პრაქტიკულად შეუძლებელია. მნიშვნელოვანია ისიც, რომ ამ სისტემებში კურიერი არ გამოიყენება.

დაშიფვრის, ნამდვილობის, მთლიანობის და სხვა ამოცანების გადაწყვეტა კურიერის მონაწილეობითაც შეიძლება. მაგრამ, რადგან კრიპტოგრაფიის მთავარი მიზანი

მაღალი საიმედოობაა, ამიტომ, საზოგადოდ, ის სისტემაა პრიორიტეტული, რომელშიც საიდუმლოება (საიდუმლო გასაღები) ერთი სუბიექტის მფლობელობაშია მოქცეული და არავითარ შუალედურ რგოლს (კურიერს თუ სხვ.) არ შეიცავს. თუმცა, რიგი ფაქტორების (ალგორითმის სიმარტივე, სწრაფქმედება და სხვ.) გათვალისწინებით თანამედროვე კრიპტოგრაფიაში ორივე სახის მეთოდებია გამართლებული.

ქვემოთ განხილულია შიფრაციის და დეშიფრაციის სისტემა DES; უ. დიფის და მ. ჰელენის ღია არხით და გასაღების გაცვლის პირველი ასიმეტრიული მეთოდი, აგრეთვე, შიფრაციის და ნამდვილობის დამადასტურებელი სისტემა RSA და ტ. ელგამალის ციფრული ხელმოწერის ასიმეტრიული ალგორითმი.

1.2.1 კრიპტოგრაფიული სისტემა DES

სიმეტრიული ყველა ალგორითმი საჭიროებს საიდუმლო კურიერის მონაწილეობას. მაგალითად, ი. ცეზარის მიერ გაგზავნილი დაშიფრული შეტყობინება სენატისათვის გასაგები რომ გამხდარიყო, ამ უკანასკნელს დეშიფრაციის გასაღები უნდა სცოდნოდა. მაშასადამე, ვიდრე ცეზარი სენატს დაშიფრულ შეტყობინებას გაუგზავნიდა, მას სენატისათვის საიდუმლოდ უნდა მიეწოდებინა გასაღები. მართალია, გასაღების საიდუმლო მიწოდება ერთჯერადად ხდება, ანუ ერთი და იგივე გასაღები გამოყენებულია გარკვეული პერიოდის განმავლობაში რამდენიმე (შესაძლო უამრავი) შეტყობინებისათვის, მაგრამ ამ პერიოდის წინ საიდუმლო კურიერის ერთჯერადი ჩართვის გარეშე კრიპტოგრაფიული კავშირი არ შედგება.

ანალოგიური ვითარებაა ტექნიკურ სისტემებშიც. აქ მეტად მნიშვნელოვანი და საინტერესო საკითხია გასაღებების გაცვლა სხვადასხვა მომხმარებელს შორის (ანუ გასაღებების მენეჯმენტი), მაგრამ ამ საკითხების განხილვა სცილდება წინამდებარე ნაშრომის მიზნებს.

სიმეტრული სისტემებიდან დღეისთვის ყველაზე წარმატებულია ამერიკული სისტემა DES-ი.

DES (Data Encryption Standard), მონაცემთა დაშიფვრის სტანდარტი, წარმოადგენს Federal Information Processing Standard (FIPS) 46-3-ის შესატყვის დასახელებას, რომელშიც აღწერილია მონაცემთა დაშიფვრის ალგორითმი (Data Encryption Algorithm-DEA); DEA, აგრეთვე, წარმოადგენს ANSI–ის (American National Standard Institute) სტანდარტს.

ალგორითმი DEA პირველად გამოკვლეული და დამუშავებულია ცნობილი IBM-ს ფირმის მიერ 1970 წელს (შემდგომ გაუმჯობესდა.) ალგორითმი ამუშავებს 64-ბიტიანი განზომილების ღია ტექსტურ ბლოკებს და იყენებს 56-ბიტიან გასაღებს. ალგორითმების განვითარებასა და სრულყოფაში დიდი წვლილი მიუძღვის, აგრეთვე, უშიშროების ეროვნულ სააგენტოს (National Institute of Standards and Techonogy – NIST a division of U.Ss Deopartment of Commerce. ყოფილი : NBS – National Bureau of Standards).

ალგორითმის ძირითადი ოპერაციებია: ჩანაცვლება, გადანაცვლება, მოდულით და ქვებლოკებად დაყოფის ლოგიკური ოპერაციები და სხვ. ალგორითმი მუშაობს ღია ტექსტის 64-ბიტიან ბლოკებზე, რის შედეგად გამოსავალზე მიიღება 64-ბიტიანი შიფროტექსტი. ტექსტის დაშიფვრა ხდება 16 ეტაპის განმავლობაში, რომლებშიც ოპერაციები მსგავსია. ოპერაციის ხანგრძლივობა დამოკიდებულია მხოლოდ $k_i(i=1,..,16)$ გასაღებებზე, რომელთაგან ყოველ ეტაპზე გამოიყენება მხოლოდ ერთი გასაღები. გასაღები 64-ბიტიანია, თუმცა გასაღების ყოველი მე-8 ბიტი მხოლოდ ლუწობაზე შემოწმებისთვის გამოიყენება. ამიტომ ძირითად ფუნქციას გასაღების 56 ბიტი ახორციელებს (ამასთან, შიფრაციის ეტაპზე გასაღებიც განიცდის გარკვეულ გადანაცვლებას).

დეშიფრაცია თითქმის არ განსხვავდება შიფრაციისაგან. დამახასიათებელია ძირითადად ის, რომ დეშიფრაციის დროს k_i გასაღები გამოიყენება საწინააღმდეგო თანამიმდევრიბით.

DES სისტემა მაღალ კრიპტოგრაფიულ მედეგობასთან ერთად ახასიათებს სწრაფქმედება, რაც (100-1000)-ჯერ მაღალია ასიმეტრიულ სისტემებთან შედარებით.

1.2.2 დიფი-ჰელმანის ასიმეტრიული მეთოდი

1976 წელი ისტორიული თარიღია, რომელიც აღნიშნავს ახალ ერას კრიპტოგრაფიაში. უ.დიფის და მ.ჰელმანის ნაშრომით დასაბამი დაედო ასიმეტრიული სისტემების განვითარებას, როდესაც კრიპტოგრაფიული სისტემა არ საჭიროებს საიდუმლო კურიერს; როდესაც გასაღების ფორმირება-გადაცემა და ინფორმაციის დაშიფვრა ხდება ღია არხის მეშვეობით, მაგრამ საჭირო საიდუმლოების დაცვით.

ეს ფაქტი შეიძლება იყოს უფრო გასაგები შემდეგი მარტივი მაგალითის განხილვის შედეგად. ვთქვათ, ორ პიროვნებას გიორგის და ირაკლის მიზნად აქვს დასახული, რომ საუბრის დროს ერთმანეთს შეატყობინოს საიდუმლო ინფორმაცია. მათთან იმყოფება ვახტანგი, რომელიც დაინტერესებულია შეიტყოს საიდუმლო ინფორმაციის შინაარსი. "თამაშის წესებით" საუბარი გიორგისა და ირაკლის შორის სრულიად ღიაა; ის უნდა იქნეს დაუფარავი ვახტანგის წინაშე, ანუ არ უნდა შეიცავდეს წინასწარ შეთანხმებულ ისეთ არაფერს, რაც შეიძლება უცნობი იყოს ვახტანგისათვის. განსახილველ შემთხვევაში ეს წესი სრულდება. მაგრამ, მიუხედავად იმისა, რომ საუბარი სრულიად ღიაა, გიორგი და ირაკლი მაინც შეძლებენ ერთმანეთს შეატყობინონ ინფორმაცია, რისი შინაარსიც ვახტანგისათვის გაუგებარი დარჩება.

ზემოაღნიშნულის მიზეზი და საფუძველი მდგომარეობს ე.წ. თანამიმდევრობითი გადარჩევის (გადასინჯვის) "სიმარტივესა" და, ამავე დროს, "სირთულეში". თანამიმდევრობითი გადარჩევის სიმარტივე ის არის, რომ მარტივია შესასრულებლად, მაგრამ "სირთულეა" ის, რომ შესაძლოა თანამედროვე კომპიუტერულმა სისტემებმაც კი ვერ შეძლოს რეალურ დროში გადარჩევის ოპერაციათა საჭირო რაოდენობის შესრულება.

დიფი-ჰელმანის მეთოდის შემდეგში მდგომარეობს:

X და Y ორი სუბიექტი (Z სუბიექტის არსებობის პირობებში) ღია არხით კურიერის გარეშე ამყარებს შემდეგ ინფორმაციულ კავშირს. დავუშვათ , რომ p მარტივი და a ნატურელური რიცხვები გაცხადებულია, ანუ ღიაა (p მაღალი რიგის $\approx 2^{500}$,

სიდიდის მარტივი რიცხვია; 1<a<p). ინფორმაციის გაცვლას X და Y მხარებს შორის აქვს შემდეგი სახე:

X მხარე საიდუმლო (კერძო) გასაღებად შეირჩევს x ნატურალურ რიცხვს (1<x<p); გამოითვლის:

$$a^x \equiv c_1 \bmod p$$

რიცხვს და ღია არხით გადაგზავნის Y მხარეზე.

Y მხარე საიდუმლო (კერძო) გასაღების სახით შეირჩევს y ნატურალურ რიცხვს (1<y<p); გამოთვლის

$$C_i^y \equiv a^{xy} \equiv k_1 \bmod p$$

რიცხვს. k_i რიცხვს Y მხარე მიიჩნევს საერთო გასაღებად.

Y მხარე გამოთვლის

$$a^y \equiv c_2 \bmod p$$

რიცხვს და ღია არხით გადააგზავნის X მხარეზე.

X მხარე გამოთვლის

$$C_2^x \equiv a^{xy} \equiv k_2 \bmod p$$

რიცხვს. k_2 რიცხვს X მხარე მიიჩნევს საერთო გასაღებად.

რადგან $k_1 \equiv k_2 \equiv k$, მაშასადამე ორივე მხარე შეირჩევს ერთსა და იმავე გასაღებს.

დიფი - ჰელმანის მეთოდში გამოყენებულია გალუას GF(p) სასრულ ველებზე ლოგარითმის გამოთვლის ცნობილი სირთულე. ვთქვათ,

$$c \equiv a^x \bmod p,\ 1 \le x \le p,$$

სადაც $a \in GF(p)$ ველის პრიმიტიული ელემენტია (ე. ი. ელემენტის ხარისხები წარმოადგენს GF(p) ველის ელემენტებს; ამბობენ, რომ x არის c ელემენტის ლოგარითმი GF(p) ველზე);

$$x = \log_a c \text{ GF(p) ველზე } 1 \le c \le p.$$

c ელემენტის გამოთვლა x ელემენტის მიხედვით არ წარმოადგენს სირთულეს და საჭიროებს მაქსიმუმ $2\log_2 p$ გამრავლების ოპერაციას.მაგალიტად, $a^{34} = ((((a^2)^2)^2)^2)^2 \cdot a^2$

მაგრამ, პირიქით, x ელემენტის გამოთვლა c ელემენტის მიხედვით გაცილებით რთულია და მოითხოვს დაახლოვებით $p^{1/2}$ ოპერაციას.

თუ p მარტივი რიცხვია და p შედარებით ნაკლებია 2^n რიცხვზე (სადაც n ინფორმაციული ორობითი სიტყვის სიგრძეა, ანუ შეტყობინების ვექტორის განზომილებაა), მაშინ ახარისხებას დასჭირდება არა უმეტეს 2n ოპერაცია GF(p) ველზე, ხოლო გალოგარითმების უკეთეს შემთხვევაში $2^{p/2}$ ოპერაცია.

როდესაც X მხარე Yმხარეს ღია არხით გადასცემს c_1 შეტყობინებას, მაშინ ანალიტიკოსს (ან ჰაკერს) x საიდუმლო გასაღების გამოსათვლელად დასჭირდება $2^{n/2}$ ოპერაციის შესრულება, რასაც ის ვერ შესძლებს (მაგალითად, თუ n=200, მაშინ საჭიროა 2^{100}, ანუ დაახლოვებით 10^{30} ოპერაცია, რისი განხორციელებაც პრაქტიკულად შეუძლებელია).

დიფი-ჰელმანის ალგორითმი გამოიყენება როგორც გასაღების გაცვლის, დაშიფვრის, აგრეთვე, აუთენტიფიკაციის მიზნით კრიფტოგრაფიული პროტოკოლის ამოცანებში და სხვ.

მაგალითი. დავუშვათ, რომ p=11, a=2, x=2, y=4, მაშინ

$$c_1 = 2^2 \equiv 4 \pmod{11}$$

$$c_2 = 2^4 \equiv 5 \pmod{11}$$

$$k_1 = 4^4 \equiv 5 \cdot 5 \equiv 3 \pmod{11}$$

$$k_2 = 5^2 \equiv 3 \pmod{11}$$

ე.ი. k=3.

გასაღების ფორმირების შემდეგ შეიძლება განხორციელდეს დაშიფვრის ოპერაცია.

ვთქვათ n =4, ხოლო ორობითი ინფორმაციაა m=(0111) ანუ M=7. X მხარე გამოიყენებს k=3 გასაღებს, რომ ცხადია, ცნობილი Y მხარისთვისაც. დავუშვათ, რომ X მხარე დაშიფრავს ინფორმაციას, ხოლო Y მხარე გაშიფრავს მას. ამისათვის Y მხარე წინასწარ გამოთვლის k' გასაღებს იმ პირობით, რომ (ფერმას მცირე თეორემა)

$$KK' \equiv 1 \ (\mathrm{mod}(p-1))$$

ე.ი.

$$3 \cdot x \equiv 1 (\mathrm{mod}\ 10)$$

X მხარე დაშიფრავს m=(0111) ღია ტექსტს თავისი k=3გასაღებით:

$$C = M^k = 7^3 \equiv 2 (\ \mathrm{mod}\ 11)$$

მიღებულ C შიფროტექსტს გადაუგზავნის Y მხარეს,რომელიც თავისი $k'=7$ გასაღებით გაშიფრავს მას:

$$M = C^{k'} \equiv 2^7 \equiv 7 (\mathrm{mod} 11)$$

1.2.3 რივესტ - შამირ - ეიდლმენის კრიპტოსისტემა (RSA)

1977 წელს რ.რივესტმა, ა. შამირმა და ლ. ეიდლემენმა დაამუშავეს შიფრაციის და ნამდვილობის (აუთენტიფიკაციის) ახალი მეთოდი. RSA დაპატენტებულია შეერთებულ შტატებში, ლიცენზირებულია სხვა ქვეყნებში და წარმოადგენს ფაქტიურ სტანდარტს მსოფლიოს მრავალ ქვეყანაში.

კრიპტოგრაფიული მეთოდი შემდეგში მდგომარეობს.

დავუშვათ, რომ X სუბიექტი საიდუმლოდ ირჩევს ძალიან დიდ მარტივ p და q რიცხვებს, გამოთვლის N=pq ნამრავლს და N რიცხვს აცხადებს (N რიცხვი ღიაა), მაგრამ p და

q რიცხვებს ინახავს საიდუმლოდ (p და q დასაიდუმლოებულია); გამოითვლება ეილერის ფუნქცია:

$$\varphi(N)=(p-1)(q-1) \text{ და } \varphi(N)$$

რიცხვს დაასაიდუმლოებს.

შემდეგ 2 - დან (φ(N)-1) - მდე ინტერვალში შეირჩევს e რიცხვს (როგორც შემთხვევით რიცხვს; თუ $(e,\varphi(N))\neq 1$, მაშინ შეირჩევა e რიცხვის სხვა მნიშვნელობას), რომელსაც აცხადებს (e რიცხვი ღიაა); $ed\equiv 1 \bmod \varphi(N)$ შედარებიდან გამოთვლის d რიცხვს და მას საიდუმლოდ ინახავს (d გასაღები დასაიდუმლოებულია). შეიძლება მივიღოთ d რიცხვი როგორც

$$ed\equiv 1 \bmod k\varphi(N)$$

შედარებიდან, აგრეთვე

$$ed=k\varphi(N)+1$$

შესაბამისობიდანაც.

ამის შემდეგ Y სუბიექტს შეუძლია M შეტყობინება გადაუგზავნოს X სუბიექტის დაშიფრული სახით:

$$M^e\equiv c \bmod N$$

c შრიფროტექსტს გაშიფრავს მხოლოდ X სუბიექტი, რადგან d, გასაღებს Z მხარე ვერ გამოთვლის:

$$c^d\equiv M \bmod N$$

Z მხარე d რიცხვის მნიშვნელობას ვერ გამოიითვლის, რიცხვის მნიშვნელობას ვერ გამოითვლის, რადგან ამისათვის მან უნდა გადაწყვიტოს ერთ - ერთი ამოცანა: ან φ(N) ფუნხციის მნიშვნელობა ან იპოვოს N რიცხვის ერთ - ერთი მარტივი მამრავლი (აქტორიზაციის ამოცანა), რაც დროის რეალურ მაშტაბში თანამედროვე კომპიუტერული სიმძლავრეებით შეუძლებელია.

მაგალითი. დავუშვათ, რომ p=3, q=5, M=3 მაშინ N=pq=15; φ(N)=(p-1)(q-1)=8

(1.1)თანაფარდობიდან

$$ed=\varphi(N)+1=9$$

ანუ

$$e=3,\ d=3$$

Y მხარე გაშიფრავს მას:

$$M=C^d\equiv 12^3\equiv 3(\text{mod } 15)$$

1.2.4. ელგამალის კრიპტოსისტემა

მოცემული სისტემა წარმოადგენს RSA - ს ალტერნატივას და მისგან განსხვავებით ეყრდნობა დისკრეტული ლოგარითმის პრობლემას. ამით იგი წააგავს დიფი - ჰემანის ალგორითმს. თუ რიცხვის აყვანა ხარისხში სასრულ ველში საკმაოდ მარტივია, პირიქით, არგუმენტის აღდგენა (ე. ი.ლოგარითმის აღება) საკმაოდ რთულია.

ელგამალის სისტემის საფუძველს წარმოადგენენ p და g<p რიცხვები, სადაც პირველი მარტივია, ხოლო მეორე - მთელი.

X აგენერირებს საიდუმლო x გასაღებს და გამოთვლის ღია $y=g^x \text{mod} p$. თუ y მხარეს სურს გაუგზავნოს X მხარეს m ტექსტი, ის ირჩევს შემთხვევით k რიცხვს (k<p) და გამოთვლის

$$y_1= g^k \text{ mod } p$$

და

$$y_2= m\oplus y^k$$

სადაც ⊕ არის ბიტური შეკრება მოდულით 2. ამის შემდეგ Y მხარე X მხარეს უგზავნის (y_1, y_2) - ს.

X მხარე მიღებულ დაშიფრულ შეტყობინებას აღადგენს: $m=(y_1^x \text{ mod } p) \oplus y_2$

თავი II

ელექტრონული (ციფრული) ხელმოწერის ალგორითმები

2.1. ციფრული ხელმოწერის დანიშნულება

ელექტრონული (ციფრული) ხელმოწერა ეწოდება ღია ტექსტზე (შეტყობინებაზე) კრიპტოგრაფიული გარდაქმნის მეშვეობით გარკვეული ციფრული ჩანაწერის (ხელმოწერის) მიბმას, რომელიც საშუალებას აძლევს მიმღებ მხარეს შეუსაბამოს მიღებული შეტყობინებას ტექსტის ავტორობა და ნამდვილობა (აუთენტიფიკაცია).

რაში მდგომარეობს მონაცემთა აუთენტიფიკაცია?

ყოველ ტექსტს ან დოკუმენტს ბოლოს თან ერთვის ხელმოწერა (სპეციალური ჩანაწერი), რომელითაც მიიღწევა ორი შედეგი:

ა) მიმღები მხარე დარწმუნდება წერილის (შეტყობინების) ნამდვილობაში, შეამოწმებს რა ხელმოწერას სათანადო ფორმულის (შემოწმების ფორმულის) მეშვეობით.

ბ) ხელმოწერა წარმოადგენს იურიდიულ გარანტიას დოკუმენტის ავტორობისა, რომ დოკუმენტი ეკუთვნის მოცემულ ავტორს და არა ვინმე სხვას. ეს ასპექტი ძალიან მნიშვნელოვანია სხვადასხვა კომერციული ხელშეკრულებების დადების დროს, მინდობილობის შედგენისა და სხვა.

თანამედროვე მსოფლიოში ძალიან გავრცელებულია დოკუმენტის ელექტრონული (ციფრული) ფორმა (მათ შორის კონფიდენციალურიც) და მათი დამუშავების ხარხებიც. ამასთან აქტუალურია ციფრული დოკუმენტაციის ნამდვილობის და ავტორობის პრობლემა.

ქაღალდზე ადამიანის ხელმოწერის გაყალბება საკმაოდ რთულია, ხოლო ციფრული ხელმოწერის გაყალბება, დოკმენტაციის შეცვლა, ავტორობის უფლების

დარღვევა და ა.შ. საკმაოდ ადვილია, თუ არ არის დაცული ციფრული ხელმოწერისათვის საჭირო გარკვეული პროტოკლებით. ამიტომ აუთენტიფიკაციის დროს აუცილებელია შესაბამისი კრიპტოალგორითმები.

ვთქვათ, გვყავს ორი მომხმარებელი: ამირანი და ბადრი. რა დარღვევებისაგან უნდა დაგვიცვას აუთენტიფიკაციის სიტემამ?

უარყოფა (რეგენატობა). ამირანი განაცხადებს, რომ მას არ გაუგზავნია შეტყობინება (ტექსტი) ბადრისათვის, თუმცა სინამდვილეში, მან ეს წერილი გააგზავნა.

ამ დარღვევის გამოსარიცხავად გამოიყენება ელექტრონული (ციფრული) ხელმოწერა.

მოდიფიკაცია (გადაკეთება). ბადრი ამრანისგან მიღებულ შეტყობინებას (ტექსტს) გადააკეთებს და ამტკიცებს, რომ გადაკეთებული შეტყობინება მიიღო ამირანისგან.

გაყალბება. ბადრი აფორმირებს მისთვის საჭირო შეტყობინებას და ამტკიცებს რომ, გადაკეთებული შეტყობინება მიიღო ამირანისგან.

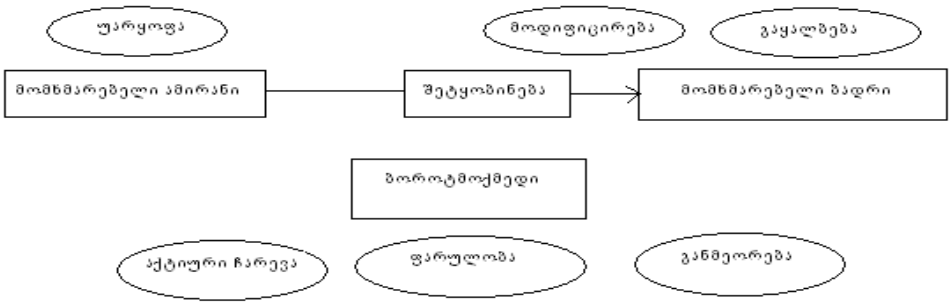
აქტიური ჩარევა. ლადო ხელთ იგდებს შეტყობინებას, რომელსაც ამირანი უგზავნის ბადრის და ფარულად ცდილობს შეცვალოს შეტყობინება თავის სასარგებლოდ.

ფარულობა (იმიტაცია). ლადო უგზავნის შეტყობინებას ბადრის ამრანის სახელით.

ამ შემთხვევაშიც დაცვის მიზნით გამოიყენება ელექტრონული (ციფრული) ხელმოწერა.

ინფორმაციის მოდიფიკაციის, გაყალბებისა და იმიტაციის ყველა შემთხვევაში თავის დასაცავად გამოიყენება ციფრული სიგნატურე (ხელმოწერა).

განმეორება. ლადო იმეორებს ამირანის მიერ ბადრისთვის ადრე გაგზავნილ შეტყობინებას. მართალია, ყოველ ღონეს ხმარობენ განმეორების წინააღმდეგ, მაგრამ ამ მეთოდზე მოდის უდიდესი ნაწილი იმ შემთხვევისა როდესაც ცდილობენ ფულის მოხსნას ელექტრონული "საფულედან".



ნახ.2.1. შესაძლო დარღვევები შეტყობინების დაცვისა, რომელსაც მომხმარებელი ამირანი უგზავნის მომხმარებელ ბადრის.

2.2.ელექტრონული ხელმოწერა RSA ალგორითმის ბაზაზე

ყველაზე მარტივი და გავრცელებული ინსტრუმენტი ელექტრონული ხელმოწერისა არის RSA კრიპტოალგორითმი. თუმცა, არსებობს ათობით კრიპტოალგორითმები ციფრული ხელმოწერისა.

ვთქვათ რომ, d, p, q - საიდუმლო გასაღებია, ხოლო e, n=pq - კი ღია; p, q - მარტივი რიცხვებია.

შენიშვნა,

1. N მამრავლების მიხედვით: მამრავლების მიხედვით: φ(n)=(p-1)(q-1); თუ ვიცით φ(n) და e, მაშინ ვიპოვით d - ს.

2. e და d - დან შეიძლება φ(n) ჯერადობის პოვნა; φ(n) ჯერადობის პოვნა კი საშუალებას გვაძლევს ვიპოვოთ n.

დავუშვათ ამირანი გადასცემს ბადრის შემდეგ შეტყობინებას: DATA.

ამირანი ხელს აწერს შეტყობინებას DATA - ს გადაცემის დროს ბადრისათვის:

$$Ee_b, n_b \{Ed_{a,\ na}\{DATA\}\}.$$

ამასთან იგი იყენებს:

ა) ამირანის საიდუმლო გასაღებს $Ed_a\ \ n_a$,

ბ) ბადრის ღია გასაღებს Ee_b, n_b.

ბადრის შეუძლია წაიკითხოს ხელმოწერილი შეტყობინება თავდაპირველად ბადრის საიდუმლო გასარებით Ed_b, n_b:

$$Ed_{a,\ } n_a\{DATA\}= Ed_{b,\ } n_b \{Ed_{b,\ } n_b \{Ed_{a,\ } n_a\{DATA\}\}\}$$

და შემდეგ ამირანის ღია გასაღებით (Ee_a,n_a) მიიღოს:

$$DATA = \ Ee_a,n_a\{ Ed_{a,\ } n_a\{DATA\}\}$$

ე. ი. ბადრი მიიღებს შეტყობინება DATA - ს, რომელიც გამოუგზავნა ამირანმა.

ნათელია, რომ ეს ალგორითმი საშუალებას იძლევა თავი დავიცვათ რამოდენიმე სახის დარღვევისაგან (ხელყოფისაგან).

ამირანი ვერ შეძლებს თავისი შეტყობინების უარყოფას, თუ ის აღიარებს, რომ საიდუმლო გასაღები ცნობილია მხოლოდ მისთვის.

ბოროტმოქმედი (ამ შემთხვევაში) საიდუმლო გასაღების გარეშე ვერ შეძლებს ცვლილებების შეტანას ტექსტში (შეტყობინებაში) რომელიც გადაეცემა.

მოცემული სქემა საშუალებას იძლევა შუამავლების გარეშე გადაწყვიტოს სხვადასხვა კონფლიქტური სიტუაცია.

2.3 ელგამალის ციფრული ხელმოწერის ალგორითმი

ელგამალის (ElGamal) ციფრული ხელმოწერის დროს გენერირდება მარტივი p რიცხვი და ორი შემტხვევითი g და x (g, x<p) - პარამეტრები. შემდეგ გამოითვლება

$$y \equiv g^x \bmod p$$

ღია გასაღებებია: y, g და p საიდუმლო გასაღებია x.

იმისათვის, რომ M_0 შეტყობინებას თან დაერთოს ხელმოწერა, ამისათვის ვირჩევთ შემთხვევით k რიცხვს, რომელიც ურთიერთმარტივია (p-1) - თან. შემდეგ გამოითვლება

$$R \equiv g^k \bmod p$$

და ევკლიდეს გაფართოებული ალგორითმის მეშვეობით გამოითვლება S - ის მნიშვნელობა შემდეგი განტოლებიდან:

$$M \equiv (xR+kS) \bmod (p-1)$$

ხელმოწერას წარმოადგენს შემდეგი წყვილი: R და S. შემთხვევითი რიცხვი k იქნება საიდუმლო. შემოწმებისათვის იყენებენ შემდეგ შესაბამისობას:

$$y^g e^s \bmod p \equiv g^m \bmod p.$$

ყოველი ახალი ხელმოწერის დროს ელგამალის ხელმოწერა მოითხოვს k - ს ახალ მნიშვნელობას.

2.4. ციფრული ხელმოწერის ალგორითმი DSA

1999 წლის აგვისტოში აშშ სტანდარტებისა და ტექნიკის ნაციონალურმა ინსტუტმა (National Institute of Standarts and Technology) თვისი ციფრული ხელმოწერის

სტანდარტისათვის (Digital Signature NIST) შემოიღო ციფრული ხელმოწერის სტანდარტი (Digital Signature Algorithm, DSA).

სანამ უშუალოდ გადავალთ DSA ალგროითმის აღწერაზე, მანამდე აღვნიშნოთ, რომ DSA - ეს არის ალგორითმი, ხოლო DSS - კი სტანდარტი. სტანდარტი იყენებს ალგორითმს. ალგორითმი სტანდარტის ნაწილია.

DSA ციფრული ხელმმოწერის ალგორითმი იყენებს შემდეგ პარამეტრებს:

p - მარტივი რიცხვი L ბიტის სიგრძის, სადაც L არის 64 ჯერადი 512 - დან 1024 - მდე დიაპაზონში.

– 160 ბიტიანი მარტივი რიცხვი, q|p-1.

$g \equiv h^{(p-1)/q} \bmod p$, სადაც h ნეისმიერი რიცხვია p-1 ნაკლები, ამასთან $h^{(p-1)/q} \bmod p > 1$.

x – რიცხვი, $x<q$.

$$y \equiv g^x \bmod p.$$

DSA ალგორითმში აგრეთვე გამოიყენება ცალმხრივი ჰეშ - ფუნქციები: H(m).

p, q, და g პარამეტრები ღიაა და ნებისმიერ მომხმარებლისათვის ხელმისაწვდომი. დაფარული (საიდუმლო) გასაღებია x, ხოლო ღიაა –y.

იმისათვის რომ მომხმარებელმა ამირანმა M შეტყობინებას თან დაურთოს ციფრული ხელმოწერა ამისათვის:

(1) ამირანი აგენერირებს შემთხვევით k რიცხვს, სადაც $k<p$,

(2) ამირანი აგენერირებს

$$r \equiv (g^k \bmod p) \bmod p,$$

$$s \equiv (k^{-1}(H(m)+xr)) \bmod q.$$

ამირანი ციფრული ხელმოწერის R და S პარამეტრებს, M შეტყობინებასთან ერთად უგზავნის ბადრის.

(3) ბადრი ამოწმებს ამირანის ხელმოწერას, გამოტვლის რა:

$$w \equiv s^{-1} \bmod q,$$

$$u_1 \equiv (H(m) * w) \bmod q,$$

$$u_2 \equiv (rw) \bmod q,$$

$$v \equiv ((g^{u1} * y^{½}) \bmod p) \bmod q.$$

თუ v= r, ციფრული ხელმოწერა სწორია.

ელგამალის ალგორითმი არ იყო დაპატენტებული, რადგან იგი ძირითადად (არსებითად) ეფუძნება დიფი-ჰელმანის ალგორითმს (ანუ მასში გამოყენებული შედარების $g^x \equiv y \bmod p$ ფუნქციას). მაგრამ შემდგომ მის ბაზაზე შეიქმნა ხელმოწერის ალგორითმი და შესაბამისი სტანდარტი.

ალგორითმის გატეხვა

არსებული ალგორითმების სახესხვაობები და ფუნქციონირება ითვალისწინებს გარკვეულ პროტოკოლურ შეზღუდვებსა და პირობითობას. ამის მაგალითია თუნდაც ის, რომ ელგამალის ალგორითმი კრძალავს ერთ-ერთი პარამეტრის სიდიდის განმეორებით გამოყენებას ხელმოწერის სხვადასხვა სეანსში. განვიხილოთ ეს კერძო შემთხვევა ზოგიერთი ფუნქციონალური დამოკიდებულების გამარტივებული წარმოდგენით. ვთქვათ, რომ პირველ და მეორე სეანსში პროტოკოლის საწინააღმდეგოდ $k_1=k_2$ (ანუ $R_1=R_2$); მაშინ პირველ სეანსში ელგამალის სინთეზის ფორმულას ექნება შემდეგი სახე:

$$M_1 \equiv (xR_1+k_1S_1) \bmod(p-1),$$

სადაც M_1 არის პირველი სეანსის M_{01} ინფორმაციის ჰეშირებული სიდიდე $M_1=H(M_{01})$; x- ინფორმაციის გამგზავნი სუბიექტის საიდუმლო გასაღები;

k_1 - ერთჯერადი შემთხვევითი საიდუმლო სიდიდე; $R_1 \equiv g^{k_1} \bmod p$ და S_1 - ხელმოწერის წყვილი, $1<g<p$; p - მაღალი რიგის მარტივი რიცხვი (g და p ღიაა). მეორე სეანსისათვის შესაბამისად გვექნება:

$$M_2 \equiv (xR_1 + k_1S_2) \bmod(p-1).$$

(3.7.) და (3.8.) - დან მიიღება:

$$M_1-M_2 \equiv (k_1S_1-k_1S_2) \bmod(p-1),$$

საიდანაც განისაზღვრება

$$k_1 \equiv M_1-M_2 / S_1-S_2 \bmod(p-1)$$

სიდიდე, თუ $(s_1-s_2, p-1)=1$; რაც ალგორითმის გატეხვას ნიშნავს, რადგან (3.7.)-დან შესაძლებელი იქნება x საიდუმლო გასაღების განსაზღვრა.

2.5ციფრული ხელმოწერის ალგორითმი ГОСТ Р 34.10-94

ამ რუსულ სატანდარტს ციფრული ხელმოწერისა, ოფიციალურად ჰქვია **ГОСТ** 34.10-94.

p- მარტივი რიცხვია, რომლის სიგრძეა 1020-დან 1024 ბიტამდე;

q - მარტივი რიცხვია, q|p-1, რომლის სიგრძეა 254-დან 256 ბიტამდე;

g – q ქვეჯგუფის წარმ. ელემენტია, $a<p-1$ და $g^q \bmod p=1$;

x - ნებისმიერი რიცხვია, $x<q$;

$y \equiv g^x \bmod p$.

ეს ალგორითმიც იყენებს ცალმხრივ ჰეშ-ფუნქციას: H(x)

პირველი სამი პარამეტრი p, q და g ღიაა და ნებისმიერი მომხმარებლისათვის ხელმისაწვდომი. დაფარული (საიდუმლო) გასაღებია x, ხოლო ღია - y.

იმისათვის რომ მომხმარებელმა ამირანმა m შეტყობინებას თან დაურთას ციფრული ხელმოწერა ამისათვის :

(1) ამირანი აგენერირებს შემთხვევით k -ს სადაც $k<q$,

(2) ამირანი აგენერირებს :

$$I\equiv(g^{*}\bmod p)\bmod q \quad s\equiv(ct+k(H(m)))\bmod q,$$

$$r \equiv (g^{k}\bmod p)\bmod q,$$

$$s \equiv (xr+k(H(m)))\bmod q,$$

თუ $H(m) \bmod q=0$, მაშინ ჰეშ-ფუნქციის მნიშვნელობა უდრის 1. თუ $r=0$, მაშინ შეირჩევა k-ს ახალი მნიშვნელობა. ხელმოწერას წარმოადგენს ორი რიცხვი: r და s. ამ პარამეტრებს უგზავნის ამირანი ბადრის კონკატენაციის სახით.

(3) ბადრი შაეამოწმებს ხელმოწერას, გამოთვლის:

$$v \equiv H(m)^{q-2} \bmod q,$$

$$z_1 \equiv (sv) \bmod q,$$

$$z_2 \equiv ((q-r) {}^{*}v) \bmod q,$$

$$u \equiv ((g^{z_1 *} y^{z_2}) \bmod p) \bmod q.$$

თუ $u=r$, მაშინ ხელმოწერა მართებულია.

მაგალითი. დავუშვათ, რომ $p=11$, $g=2$, $x=4$; ამიტომ

$$y \equiv g^{x} \equiv 2^{4} \equiv 5 \ (\mathrm{mod}\ 11).$$

X მხარე შეარჩევს, ვთქვათ $k=6$ შემთხვევით რიცხვს, მაშინ

$$R \equiv g^{k} \equiv 2^{6} \equiv 9 \ (\mathrm{mod}11).$$

ვთქვათ, $M'=H(M)=5$.

ხელმოწერის მეორე პარამეტრი არის:

$$S \equiv xR+kM' \equiv 4\cdot 9+6\cdot 5 \equiv 6 \pmod{10}.$$

Y მხარეზე შემოწმების შედეგია:

$$g^x \equiv y^R R^{M'} \pmod{11},$$

$$2^6 \equiv 5^9 9^5 \pmod{11},$$

$$9 \equiv 9\cdot 1 \pmod{11}.$$

მაშასადამე, შემოწმების პირობა სრულდება და მიღებული ინფორმაცია სანდოა.

ახლა დავუშვათ, რომ Z სუბიექტმა შეცვალა შეტყობინება და შედეგად მხარემ მიიღო შეტყობინება, რომლისთვისაც ჰეშირების შედეგად $M'=5$ მნიშვნელობის ნაცვლად გამოითვლება განსხვავებული $M''=4$ რიცხვი. მაშინ შემოწმების შედეგად მიიღება:

$$g' \neq y^R R^{M''} \pmod{p},$$

$$2^6 \neq 5^9 9^4 \pmod{11},$$

$$9 \neq 9\cdot 5 \pmod{11}.$$

მაშასადამე, ღია ტექსტში შეტანილი ცვლილება შემოწმების შედეგად გამოვლენილია.

თავი III

ციფრული ხელმოწერის ორიგინალური ალგორითმი და მისი განხორციელება

3.1. ელგამალის ალგორითმი, როგორც ერთ-ერთი ძირითადი პროტოტიპი ცნობილი ალგორითმების მისაღებად; ამერკული სისტემა DSA

1985 წელს ტახირ ელგამალმა გამოაქვეყნა ნაშრომი ციფრული ხელმოწერის შესახებ, რომელიც შემდეგში მდგომარეობს: ღია ტექსტურ M შეტყობინებას თან დაერთვის R და S ორი შეტყობინება, რომელიც წარმოადგენს ტექსტის ნამდვილობის დადასტურებას, ანუ ციფრულ ხელმოწერას. X მხარეზე მიიღება ე.წ. კონკატენცია

$$|M_0||R||S|$$

სადაც R და S ორობითი სიტრყვების სიგრძე მკაცრად განსაზღვრულია, როგორც განხილულ ასიმეტრიულ სისტემებში, მაქსიმალური რიცხვით, მაგალითად $p \approx 2^{500}$ მნიშვნელობით, ანუ ორობითი ვექტორის n=500 განზომილებით, ხოლო M შეტყობინება წარმოადგენს ბევრად უფრო გრძელ ღია ციფრულ მიმდევრობას, ე.ი. ღია ტექსტს.

ამ ალგორითმში ინფორმაციის დაცვის მიზანი არ არის X სუბიექტის მიერ ტექსტის დაშიფვრა-გასაიდუმლოება. ტექსტი ღიაა და ღიად უნდა დარჩეს, მაგრამ თუ ტექსტში გარეშე Z სუბიექტი შეიტანს ცვლილებას, იგი უნდა გამოაშკარავდეს Y მხარეზე შემოწმების შედეგად.

ალგორითმი ეფუძნება დიფი-ჰელმანის ალგორითმით დაპატენტებულ ცნობილ ცალმხრივ ფუნქციას:

$$g^x \equiv y \pmod{p}$$

ამ შემთხვევაშიც p დიდი მარტივი რიცხვია; g და x - ნატურალური რიცხვები (1<g, x<p). X წარმოადგენს X სუბიექტის საიდუმლო კერძო გასაღებს. p, g, y გაცხადებულია (ღიაა).

X მხარე შეარჩევს ფსევდოშემთხვევით k<p რიცხვს და გამოთვლის

$$R \equiv g^k \pmod{p}$$

რიცხვის მნიშვნელობას; შემდეგ გამოთვლის S სიდიდეს შემდეგი გამოსახულებიდან:

$$M \equiv (xR+kS) \bmod (p-1)$$

რიცხვს და შეადგენს (3.1) შეტყობინებას (სადაც M არის M_0 ღია ტექსტის ჰეშირების შედეგად მიღებული შედეგი |M|<p), ე.ი.

$$M=H(M_0)$$

არის M_0 ღია ტექსტის ცალმხრივი ჰეშ-ფუნქცია; H ფუნქცია გაცხადებულია (ჰეშირების საკითხს ქვემოთ დავუბრუნდებით)

Y მხარე მიიღებს რა (3.1.) შეტყობინებას, შეამოწმებს მას შემდეგი ტოლობის მეშვეობით:

$$g^M \equiv y^R R^S \pmod{p}.$$

(3.6.) გამოსახულებით შესაძლებელია შემოწმდეს მღებული შეტყობინება, რადგან :

$$g^M \equiv g^{xR}.g^{kS} \pmod{p},$$

$$g^M \equiv g^{xR+kS} \pmod{p},$$

$$M \equiv (xR+kS) \bmod (p-1),$$

რაც (3.5.)-ის თანახმად შეესაბამება (3.4.) თანაფარდობას.

ამრიგად, თუ Z მხარე M ღია ტექსტში შეიტანს რაიმე ცვლილებას და მიიღებს ახალ M_{01} ტექსტს, მაშინ მან უნდა გადაწყვიტოს ორი პრობლემიდან ერთ-ერთი:

1) ან M_{01} ტექსტისათვის გაცხადებული H ფუნქციის მიხედვით მიიღოს იგივე $M=H(M_{01})$ მნიშვნელობა ;

2) ან ახალი M_{01} ღია ტექსტისათვის გამოთვალოს ისეთი R_1 და S_1 ხელმოწერა, რომლითაც შეცვლილი

$$|M||R_1||S_1|$$

შეტყობიებისათვის დაკმაყოფილედება შემოწმების (3.6.) პირობა.

არც ერთი ამ პრობლემიდან რეალურ დროში გადაწყვეტადი არ არის, როდესაც p დიდი რიცხვია და Z სუბიექტს x საიდუმლო გასაღები არ გააჩნია (რა თქმა უნდა, თუ არა R_1 და S_1 რიცხვების შერჩევის შემთხვევითი გამართლება, რისი ალბათობაც თითქმის არ არსებობს:$\approx 10^{-30}$).

3.2. ციფრული ხელმოწერის ალტერნატიული ალგორითმი

თავის ცნობილ ნაშრომში ბრიუს შნაიერი შენიშნავს, რომ დამატებითი ვარიანტებისა და განზოგადების შედეგად ციფრული ხალმოწერის სქემების რაოდენობამ შეიძლება შეადგინოს ცამეტ ათასზე მეტი (თუმცა მათგან ყველა ეფექტური არ იქნება).

ციფრული ხელმოწერის ალგორითმების უმრავლესობა ეფუძნება გალუას GF(p) ველებში დისკრეტული ლოგარითმების, ფესვის ამოღების, ფაქტორიზაციის პრობლემას და სხვა.

სადირსეტაციო ნაშრომში გამოკვლეულია ციფრული ხელმოწერის შესაძო ვარიანტები, რომლებიც, აგრეთვე, იყენებს დისკრეტული ლოგარითმების პრობლემას (ანუ $g^x \equiv y \bmod p$ ცალმხრივ ფუნქციას). მათემატიკური საფუძვლების სივიწროვე, ცხადია, ართულებს ალტენატიული კრიპტოგრაფიული ალგორითმების აგებას. ამავე დროს აღსანიშნავია, რომ, როგორც სხვა ცნობილ შემთხვევებში, პროტოტიპად (კვლევის ვარიანტად) გამოყენებულია ერთ-ერთი, კერძოდ, ელგამალის სქემა, რათა გარკვეული

ფუნქციონალური ელემენტის შემოტანის შედეგად მივიღოთ ალგორითმის, როგორც ვარიანტის, ახალი სტრუქტურული თვისობრიობა.

ორიგინალური ალგორითმის აგება

არსებული ალგორითმების სახესხვაობები და ფუნქციონირება ითვალისწინებს გარკვეულ პროტოკოლურ შეზღუდვებსა და პირობითობას. ამის მაგალითია თუნდაც ის, რომ ელგამალის ალგორითმი კრძალავს ერთ-ერთი პარამეტრის სიდიდის განმეორებით გამოყენებას ხელმოწერის სხვადასხვა სეანსში.

ორიგინალური ალგორითმისათვის სინთეზის და შემოწმების ფორმულებს, შესაბამისად, აქვს შემდეგი სახე:

$$S = (x+kRM) \bmod (p-1)$$

და

$$a^s \equiv yR^{RM} \bmod p$$

ინფორმაციული გზავნილისა და ხელმოწერის კონკატაცია ქმნის შემდეგ ჩანაწერს:

$$|M_0||R||S| ,$$

სადაც $M \equiv H(M_0)$, M_0 - გადაცემული ინფორმაციაა, რომელიც პროტოკოლით არის დაცული;

$R \equiv a^k \bmod p$ და S - ხელმოწერის წყვილი; k - ერთჯერადი გამოყენების შემთხვევითი საიდუმლო რიცხვია.

თუ ალგორითმის პარამეტრებს განვიხილავთ, როგორც გალუას GF (p) ველის ციკლური ჯგუფის ქვეჯგუფის ელემენტებს, მაშინ ძირითადი პარამეტრების შერჩევისათვის გვექნება შემდეგი წესი:

p - მაღალი რიგის მარტივი რიცხვია (მაგალითად, 509 და 512 ბიტებს შორის);

(p-1) - ნაკლები p - ზე, მაგრამ მაღალი რიგისაა;

a - ქვეჯგუფის გენერატორია, ნებისმიერი რიცხვია, რომელიც (p - 1) - ზე ნაკლებია და რომლისთვისაც $a^{p-1} \bmod p \equiv 1$;

x - საიდუმლო გასაღებია, $0 < x < (p - 1)$;

y - ღია გასაღებია, რომელიც გამოითვლება x პარამეტრით: $y \equiv a^x \bmod p$.

მაგალითი: ვთქვათ, p=11, M=3, a=2, x=2, k=3. აქედან

$$y=a^x \bmod p=2^2 \bmod 11=4,$$

$$R \equiv a^k \bmod p$$

$$R=2^3 \bmod 11=8 \bmod 11.$$

p, g, y, R, M -ღიაა, x-საიდუმლო გასაღებია, k- ერთჯერადი საიდუმლო გასაღები.

ის ვინც აფორმირებს x და k, ადვილად იპოვის S-ს:

$$S=(x+kRM) \bmod (p-1)$$

$$S=(2+3 * 8 * 3) \bmod 10=74 \bmod 10=4,$$

ე.ი.

$$S=4.$$

კონკატენაციას აქვს სახე:

$$|3||8||4| \quad (|M||R||S|).$$

განვიხილოთ შემოწმება:

$$a^s \equiv yR^{RM} \bmod p,$$

$$2^4 \equiv 4 * 8^{8*3 \bmod 10} \bmod 11,$$

$$16 \equiv 4 * 8^4 \bmod 11,$$

$$16 \equiv 4 * 8^2 * 8^2 \bmod 11,$$

$$16 \equiv 4 * 64 * 64 \bmod 11,$$

$$16 \equiv 4 * 9 * 9 \bmod 11$$

$$16 \equiv 16 \bmod 11,$$

ე.ი. შემოწმება სწორია.

სისწრაფე და სიმარტივე

ელგამალის ალგორითმთან შედარებაში, სწრაფქმედება და სიმარტივე, ორიგინალური ალგორითმისა ჩანს, სინთეზისა და შემოწმების ფორმულების გამოთვლებში. ალგამალის სინთეზის ფორმულიდან გასაგზავნი S გასაღების პოვნა გამოიყურება შემდეგნაირად $S=(xR+k)/ M \bmod (p-1)$

რაც ცალსახად მოითხოვს უფრო მეტი არითმეტიკული ოპერაციის ჩატარებას ვიდრე $S = (x+kRM) \bmod (p-1)$

ელგამალის ალგორითმის სინთეზის ფორმულა:

1 ბიჯი: x*R გამრავლების შესრულება;

2 ბიჯი: (x*R)+k შეკრების შესრულება;

3 ბიჯი: M-ზე გაყოფის შესრულება;

4 ბიჯი: მიღებული შედეგის mod (p-1) გაყოფა.

ორიგინალური ალგორითმის სინთეზის ფორმულა:

1 ბიჯი: k*R*M გამრავლების შესრულება;

2 ბიჯი: (k*R*M)+k შეკრების შესრულება;

3 ბიჯი: მიღებული შედეგის mod (p-1) გაყოფა.

ასევე მარტივი დასანახია შემოწმების ფორმულების შედარებისას ორიგინალური ალგორითმის ფორმულის გამოთვლის სიმარტივე

ელგამალის ალგორითმის შემოწმების ფორმულა:

1 ბიჯი: g^M ხარისხში აყვანა;

2 ბიჯი: მიღებული შედეგის mod (p) გაყოფა;

3 ბიჯი: y^R ხარისხში აყვანა;

4 ბიჯი: მიღებული შედეგის mod (p) გაყოფა;

5 ბიჯი: R^S ხარისხში აყვანა;

6 ბიჯი: მიღებული შედეგის mod (p) გაყოფა;

7 ბიჯი: ტოლობის (სადარობის) შემოწმება.

ორიგინალური ალგორითმის შემოწმების ფორმულა:

1 ბიჯი: a^s ხარისხში აყვანა;

2 ბიჯი: მიღებული შედეგის mod (p) გაყოფა;

3 ბიჯი: y შედეგის mod (p) გაყოფა;

4 ბიჯი: R^{RM} ხარისხში აყვანა;

5 ბიჯი: მიღებული შედეგის mod (p) გაყოფა;

6 ბიჯი: ტოლობის (სადარობის) შემოწმება;

აქედან გამომდინარე ეს ორიგინალური ალგორითმი უფრო სწრაფიცაა და უფრო მარტივიც.

3.3 პროგრამული უზრუნველყოფის შესახებ

ციფრული ხელმოწერისათვის პროგრამული უზრუნველყოფა, აღნიშნულ ნაშრომში განხორციელებულია C# - ის ბაზაზე.

```
//ხელმოწერის  ფუნქცია
//პარამეტრები

 //საჭირო ცვლადების გამოცხადება:

   int p = Convert.ToInt32(Ptxt.Text);
   int k = Convert.ToInt32(Ktxt.Text);
   int x = Convert.ToInt32(Xtxt.Text);
   int a = Convert.ToInt32(Atxt.Text);
    int m = GetRandomeNumber(1, p); // რენდომად რიცხვის მინიჭება

//  ხელმოწერის შემოწმებისათვის მნიშვნელობების დათვლა

double x1 = Math.Pow(a, s);
double rmr = Math.Pow(r, m *r) % p;
double x2 = y * rmr;

//რენდომის ფუნქცია:  M-ს

Random random = new Random();
return random.Next(minimum, maximum);

// ითვლის Y მნიშვნელობას
 private double Y(int a, int x, int p)
        {
            return Math.Pow(a, x) % p;
        }

) // ითვლის R მნიშვნელობას
private double R(int p, int k, int a
        {
            double r = Math.Pow(a, k) % p;
            return r;
        }
// ითვლის S მნიშვნელობას
private double S(int x, int k, int p, int m, double r)
        {
            return (x + k * r * m) % (p - 1);
        }
```

დასკვნა

სამაგისტრო ნაშრომის თემატიკა კრიფტოგრაფიული სისტემების მიმოხილვა და ციფრული ხელმოწერის ალგორითმების კვლევაა. გამოკვლეული და მიღებულია ციფრული ხელმოწერის ახალი ალგორითმი. როგორც სხვა ცნობილი, აღიარებული სქემების შემთხვრვაში, ნაშრომის კვლევის ობიექტს (პროტოტიპს) წარმოადგენს ელგამალის ალგორითმი, რომლისთვისაც პარამეტრების გარკვეული ფუნქციონალური თვისებების გამოყენებით, მიიღება საჭირო სტრუქტურული ალტერნატივა. მიღებული ალგორითმის თვისობრივი უპირატესობა არის მისი სრაფქმედება. ის განკუთვნილია იმ მომხმარებლებისათვის, რომლისთვისაც მთავარი აქცენტი კეთდება სისწრაფეზე და არა გადაცემული ინფორმაციის რაოდენობაზე.

გამოყენებული ლიტერატურა

1. მეგრელიშვილი რ. ინფორმაციის დაცვის სისტემები. // თბილისის უნივერსიტეტის გამომცემლობა 2007

2. მეგრელიშვილი რ., ჭელიძე მ. გნოლიძე თ. ელექტრონული ხელმოწერის ალტერნატიული ალგორითმის სინთეზის ამოცანისთვის. // სოხუმის უნივერსიტეტი, აკადემიური პერსონალის სამეც. კონფერაცია, 2008.

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

4. ElGamal T. A public-key cryptosystem and signature scheme based on discrete logarithms. IEEE Trans. On Inf. Theory, v. IT-31, n.4. pp. 469-472, 1985.

5. ElGamal T. A public-key cryptosystem and signature scheme based on discrete logarithms. Advances in Cryptology: Proceedings of CRYPTO 84, Springer-Verlag, pp. 10-18, 1985.

6. ElGamal. T.A subexponential-time algorithm for computing discrete logarithms over GF(p2) // IEEE Trans. Inform. Theory. 1985. V. 31. P. 473-481.

7. ElGamal T. On computing logarithms over finite fields // Advances in cryptology-CRYPTO 85 (Santa Barbara, Calif., 1985). 1986. (Lect. Notes in Comput. Sci.; V. 218). P. 396-402.

8. Kobiltz N.A course in number theory and cryptography. Springer Verlag, 1987.

9. Kobiltz N. Elliptic curve cryptosystems // Math. Comb. 1987. V. 48. P.203-209.

10. Kobiltz N. Algebraic aspects of cryptography. Springer-verlag, 1998.

11. Robshaw M.J., <<Security Estimates for 512-bit RSA>>, RSA Laboratories, June 29, 1995.

12. Rubin, Honeyman “Nonmonotonic cryptographic protocols”. Proc.Comb. Sec. Found. Workshop, VII, 1994.

13. Williams H.C. A modification of the RSA public-key cryptosystem // IEEE Trans. Inform. Theory. 1980. V.26, No. 6. -.726-729.

14. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. М.: Наука, 1976.

15. Василенко О.Н. В19 Теоретико-числовые алгоритмы в криптографии.-М.: МЦНМО, 2003.-328с.

16. Введение в криптографию / под овщ. В.В. Яшенко. 3-е изд., доп. М.: МЦНМО: «ЧеРо», 2000.

17. ГОСТ Р 34.11 -94. Государственный стандарт Российской Федерации. Криптографическая защита информации. Функция хеширования. М.: Госстандарт Россий. 1994.

18. Росс Андерсон, «Почему не срабатывают криптосхемы: уроки последних лет». http://www.bgs.ru/russian/security04.html

19. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. – М.: Научный мир, 2004.

20. Павел Семьянов, «Почему криптосистемы ненадежны». http://www.hackzone.ru/articles/crypto.html.