მალხაზ ჭელიძე

კრიპტოსისტემისა და ციფრული ხელმოწერის ალგორითმების სინთეზისათვის

წარმოდგენილია დოქტორის აკადემიური ხარისხის მოსაპოვებლად

საქართველოს ტექნიკური უნივერსიტეტი

თბილისი, 0175, საქართველო

2008

საქართველოს ტექნიკური უნივერსიტეტი

ჩვენ, ქვემორე ხელისმომწერნი ვადასტურებთ, რომ გავეცანით ჭელიძე მალხაზის მიერ შესრულებულ სადისერტაციო ნაშრომს დასახელებით: *"კრიპტოსისტემისა და ციფრული ხელმოწერის ალგორითმების სინთეზისათვის"* და ვაძლევთ რეკომენდაციას საქარველოს ტექნიკური უნივერსიტეტის სადისერტაციო საბჭოში მის განხილვას დოქტორის აკადემიური ხარისხის მოსაპოვებლად.

თარიღი

ხელმძღვანელი: რ. მეგრელიშვილი _____

რეცენზენტი: _____

რეცენზენტი: _____

რეცენზენტი: _____

საქართველოს ტექნიკური უნივერსიტეტი

წელი

ავტორი: ჭელიძე მალხაზ

დასახელება: კრიპტოსისტემისა და ციფრული ხელმოწერის ალგორითმების სინთეზისათვის

ფაკულტეტი : ინფორმატიკისა და მართვის სისტემების

ხარისხი: დოქტორი

სხდომა ჩატარდა:

ინდივიდუალური პიროვნებების ან ინსტიტუტების მიერ ზემომოყვანილი დასახელების დისერტაციის გაცნობის მიზნით მოთხოვნის შემთხვევაში მისი არაკომერციული მიზნებით კოპირებისა და გავრცელების უფლება მინიჭებული აქვს საქართველოს ტექნიკურ უნივერსიტეტს.

ავტორის ხელმოწერა

რეზიუმე

ნაშრომი "კრიპტოსისტემისა და ციფრული ხელმოწერის ალგორითმების სინთეზისათვის" წარმოადგენს ორიგინალური კრიპტოსისტემების აგების მცდელობას.

აღნიშნული მიზნის შესაბამისად დამუშავებულია კოდირების ალგებრულ სტრუქტურაზე დაფუძნებული ინფორმაციის დაცვის ორიგინალური მატრიცული მეთოდი, რომელსაც ეფუძნება შემოთავაზებული სიმეტრიული კრიპტოსისტემა.

გამოკვეულია და მიღებულია ციფრული ხელმოწერის ალგორითმების ორი ვარიანტი. როგორც სხვა ცნობილი სქემები, მოცემული ალგორითმებიც წარმოადგენს ელგამალის ალგორითმის, როგორც პროტოტიპის, გარკვეულ მოდიფიკაციას. მთავარი არსი მდგომარეობს მასში, რომ ზოგიერთი პარამეტრის გარკვეული ფუნქციონალური თვისების გამოყენებით მიიღება საჭირო სტრუქტურული ალტერნატივა.

ამრიგად, მიღებულია შემდეგი ძირითადი შედეგები:

- მრავალწევრთა ალგებრასა და გალუას $GF(p^m)$ ველებზე დაყრდნობით მიღებულია პირდაპირ და შებრუნებულ $n \times n$ მატრიცთა (ანუ კრიპტოგრაფიულ გასაღებთა) აგების ორიგინალური მეთოდი, რომელიც კონსტრუქციული და მარტივად რეალიზებადია ნებისმიერი მთელი n რიცხვისათვის $GF(p)$ ველზე;
- მიღებულ მატრიცებზე დაყრდნობით აგებულია შიფრაცია-დეშიფრაციის მარტივი (პირველადი) სიმეტრიული კრიპტოსისტემა, ხოლო მარტივი კრიპტოსისტემისა და ფსევდოშემთხვევითი მიმდევრობის გამოყენებით, რომლის გენერირება შესაძლებელია $GF(p^k)$ ველზე დაფუძნებული პროგრამული თუ წანაცვლების რეგისტრების მეშვეობით, მიღებულია შიფრაცია-დეშიფრაციის კომბინირებული სიმეტრიული კრიპტოსისტემა;
- გამოკვლეული და მიღებულია ციფრული ხელმოწერის ახალი ალგორითმების ვარიანტები;
- განსაზღვრულია არეალი და მახასიათებელი პარამეტრები იმ კატეგორიის მომხმარებლებისა, რომელთათვისაც მიზანშეწონილი და რეკომენდირებულია მიღებული კრიპტომეთოდების გამოყენება.

განვიხილოთ თითოეული შედეგი.

ურთიერთშებრუნებულ მატრიცთა აგება ადვილად ხორციელდება გალუას $GF(p)$ ველზე მრავალწევრთა A_n ალგებრაში $\mathrm{mod}(x^n - 1)$.

ამისათვის განიხილება $GF(p^m)$ ველის პრიმიტიული ელემენტი, მისი ხარისხები და შესაბამისი მინიმალური ფუნქციები, რომელთა ნამრავლით მიიღება $g(x) = x^n - 1/h(x)$ მრავალწევრი, რომელიც ორიგინალური მეთოდით (განიხილება სათანადო თეორემა) აფორმირებს პირდაპირ A_1 მატრიცს, ხოლო $h(x)$ მრავალწევრი- შებრუნებულ A_2 მატრიცს. აქედან გამომდინარე, შიფრაცია-დეშიფრაციის პროცესი მოცემული a შეტყობინებისათვის შეიძლება განისაზღვროს, როგორც: $aA_1 = c$; $cA_2 = a$. გასაღებთა სიმრავლეს ქმნის მატრიცებში შესაბამისი სტრიქონებისა და სვეტების გადანაცვლება, რაც ჯამში $n^2!$-ის ტოლ გასაღებთა სიმრავლეს გვაძლევს.

კომბინირებული სისტემა. მარტივ მატრიცულ კრიპტოსისტემასთან ერთად, როგორც ზემოთ იყო აღნიშნული, განიხილება ცნობილი მეთოდი $GF(p^k)$ ველში ფსევდოშემთხვევითი d მიმდევრობებისა (მათი პერიოდია $2^k - 1$), რომელთა გენერაცია არ არის რთული პროგრამულად ან აპარატურულად წანაცვლების რეგისტრების მეშვეობით. გამოიყენება XOR-ი: $a + d = b$ და შემდეგ შიფრაცია $bA = c$, რაც იწვევს კრიპტოსისტემის მედეგობის მნიშვნელოვან ამაღლებას (დეშიფრაცია შიფრაციის ანალოგიურია: $a = cA_2$).

ციფრული ხელმოწერის ალგორითმები. როგორც სხვა ცნობილ და აღიარებულ შემთხვევებში,- პროტოტიპში ერთი ელემენტის ცვლილებით მიიღება განსხვავებული სტრუქტურა, ჩვენ შემთვევაშიც პარამეტრის გარკვეული ფუნქციური თვისების გამოყენებით (მხედველობაშია პირველი მეთოდი) მიიღება ახალი სტრუქტურა, კერძოდ, გამარტივებული და უფრო სწრაფქმედი. მაგალითად, $S = x + km$ სინთეზის ფორმულაში M ინფორმაციის პარამეტრი ღებულობს მხოლოდ ლუწ მნიშვნელობებს: $2|M$; პირვანდელი სქემა გამარტივებულია და მიიღება საჭირო სტრუქტურა (იხ. აგრეთვე, ქვემოთ).

მიზანშეწონილობა და რეკომენდაციები. სიმეტრიული მატრიცული კრიპტოსისტემის თვისობრივი უპირატესობა არის მისი აგების კონსტრუქციულობა, სიმარტივე და სწრაფქმედება. მაგრამ იგი ნაკლებად მდგრადია. ამიტომ ის განკუთვნილია იმ მომხმარებლებისათვის, რომლისთვისაც მთავარი აქცენტი კეთდება სისწრაფეზე და არა გადაცემული ინფორმაციის რაოდენობაზე, რაც ხორციელდება გასაღებების ცვლილების პერიოდში (მაგალითად, 1-5 ნაბეჭდი გვერდი). მაგრამ, ამ პერიოდებში, თუ გავითვალისწინებთ გასაღების ცვლილების განუხრელ განხორციელებას, მიიღება მედეგი, მაღალი სწრაფქმედების სისტემა.

ციფრული ხელმოწერის პირველი ალგორითმის მახასიათებლები კრიპტოსისტემის ანალოგიურია (მაღალი სწრაფქმედება მედეგობის ნაწილობრივი შემცირების ხარჯზე);

მეორე ალგორითმი- თავისი თვისებებით, ძალიან ახლოსაა ცნობილ სქემებთან (ლიტერატურაში ჩვენთვის არ არის ცნობილი ასეთი სტრუქტურის დაფიქსირების ფაქტი, თუმცა, სამწუხაროდ, მისი არარსებობის ნამდვილობის მტკიცებაც შეუძლებელია). მედეგობის თვალსაზრისით ეს ალგორითმი არ ჩამოუვარდება ცნობილ საუკეთესო ალგორითმებს, ხოლო სწრაფქმედებით უკეთესიცაა; მის მიმართ ჩვენს მიერ გატეხვის განხორციელების მცდელობამ შედეგი არ გამოიღო, რისი ახსნაც მისი სტრუქტურის შედარებითი ანალიზის მეშვეობით სავსებით შესაძლებელია.

Abstract

- The new matrix cryptographic method and system of data encryption-decryption are developed with key transmission via both secret and public channels.

- There are discussed the available variants of construction the algorithms of digital signatures. The algorithms, as many other algorithms, are obtained from the simplification of the algorithm of ElGamal. The main objective is to change the functionality of some parameters, in a result we obtain the necessary structural alternation.

შინაარსი

ნახაზების ნუსხა

მადლიერება

რასაკვირველია, უპირველეს ყოვლისა, მადლიერი ვარ ჩემი სამეცნიერო ხელმძღვანელის, პედაგოგისა და უფროსი მეგობრის ბატონ რიჩარდ მეგრელიშვილის, რომელსაც უდიდესი წვლილი მიუძღვის ჩემი სადისერტაციო ნაშრომის შექმნაში.

შესავალი

როგორ გადავცეთ საჭირო ინფორმაცია საჭირო ადრესატს საიდუმლოდ? როგორია კრიპტოგრაფიის მიზნები და პრობლემები?*

უპირველესად შევნიშნოთ, კრიპტოგრაფიის ამოცანები დაისმის მხოლოდ იმ ინფორმაციისთვის, რომელიც საჭიროებს დაცვას. ასეთ შემთხვევაში ამბობენ, რომ ინფორმაცია შეიცავს საიდუმლოებას ან წარმოადგენს პრივატულს (კერძოს), კონფიდენციალურს, და მოითხოვს დაცვას. ინფორმაციის დასაიდუმლოების ყველაზე ტიპიურ სფეროებს წარმოადგენს: სახელმწიფო, სამხედრო, კომერციული, იურიდიული, სამედიცინო და ა.შ. [10, 21, 42, 47, 60].

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

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

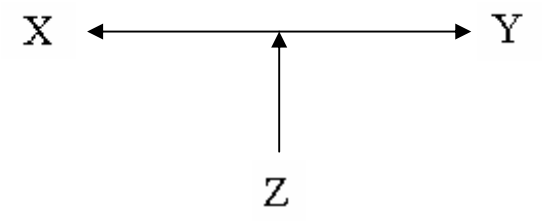
•არის არაკანონიერი მომხმარებელი, რომელიც ცდილობს ხელში ჩაიგდოს საიდუმლო ინფორმაცია, რათა ის გამოიყენოს საკუთარი ინტერესებისათვის კანონიერი მომხმარებლის საზიანოდ.

განვიხილოთ საშიშროება, როდესაც ადგილი აქვს დაცული ინფორმაციის გამჟღავნებას, თუმცა არსებობს დაცული ინფორმაციისთვის სხვა საფრთხეებიც: არაკანონიერი მომხმარებლების 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 კავშირის არხში გადაცემული საიდუმლო ინფორმაცია და გამოიყენოს თავის სასარგებლოდ (სურ.1.). ეს ფორმალური სქემა შეიძლება ჩაითვალოს

* კრიპტო - პირობითი საიდუმლო ნიშნები; გრაფია - წერა.

ტიპიურ სიტუაციად, სადაც გამოიყენება კრიპტოგრაფიული მეთოდები ინფორმაციის დაცვისა.



ნახ.1. . კრიპტოსისტემის ფორმალური სქემა

კრიპტოგრაფია - ეს არის სამეცნიერო-ტექნიკური დარგი, რომელიც უზრუნველყოფს ინფორმაციის დასაიდუმლოებას (უსაფრთხოებას). მისი ძირითადი ამოცანაა გადაწყვიტოს 4 ძირითადი პრობლემა: ინფორმაციის შიფრაცია-დეშიფრაცია, ანუ უსაფრთხოება- კონფიდენციალურობა, აუტენტიფიკაცია, 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 გასაღებისაგან, რომელსაც იყენებს ალგორითმი; გასაღებების განაწილების შესაბამისი სისტემა; ღია (დაუშიფრავი) ტექსტი და დაშიფრული ტექსტი (შიფროტექსტი). გასაღები არის ალგორითმის რეალიზაციის ერთ-ერთი კონკრეტული სახე (აღსანიშნავია, რომ გასაღებთა სიმრავლის მაღალი რიგი წარმოქმნის ალგორითმის მაღალ საიმედოობას, ანუ სისტემის მედეგობას (მდგრადობას)).

შემუშავებული მეთოდოლოგიით თავდაპირველად ღია ტექსტის მიმართ გამოიყენება შიფრაციის ალგორითმის გასაღები, და მიიღება შიფროტექსტი; შემდგომ შიფროტექსტი 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 კრიტოსისტემის 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.

ამავა დროს მნიშვნელოვანია, როგორ დავამყაროთ ინფორმაციის გადაცემის უსაფრთხო კავშირი მონაწილეებს შორის გასაღების გადაცემამდე? ამ პრობლემას წარმოადგენს აუტენტიფიკაცია; 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 უფლებამოსილ პიროვნებას თუ მოიწინააღმდეგეს?

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

სიმეტრიული კრიპტოსისტემის დროს დიდ პრობლემას გასაღებების 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 გასაღების 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 გადაცემის პროცესში და ა.შ.

როგორც ვხედავთ, ერთი კანონიერი მომხმარებლისაგან მეორე კანონიერ მომხმარებელისადმი 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 მომხმარებლებმა ინფორმაციის დაცვის დროს. რაც არ უნდა მდგრადი იყოს ინფორმაციის დაცვის მექანიზმის რომელიღაც რგოლი, ის ვერ დაიცავს სისტემას "გატეხვისაგან", თუ სხვა რომელიმე რგოლი სუსტია.

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

თანამედროვე ტექნიკის განვითარებისას 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 იმდენად 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. ზოგიერთი საიდუმლოება ათეულობით წელს ინახება, ზოგი რამდენიმე საათს. გასათვალისწინებულია, თუ ვინ არის მოწინააღმდეგე, ე.ი. ვისგან გვიწევს საიდუმლო ინფორმაციის დაცვა: ცალკეული პირია ის, თუ მძლავრი ორგანიზაცია (კორპორაცია) ანდა მძლავრი სახელმწიფო სტრუქტურა და ა.შ.

ნაშრომის მიზანი: მცდელობა ორიგინალური კრიპტომეთოდების განხორციელებისა.

აღნიშნული მიზნის შესაბამისად შემოთავაზებულია სიმეტრიული კრიპტოსისტემის აგების მეთოდი, დამუშავებულია კოდირების ალგებრულ სტრუქტურაზე დაფუძნებული ინფორმაციის დაცვის ორიგინალური სისტემა მატრიცული მეთოდი (კრიპტოგრაფიული გასაღების საიდუმლო და ღია არხით გადაცემის შემთხვევაში).

გამოკვეული და მიღებულია ციფრული ხელმოწერის ახალი ალგორითმების ორი ვარიანტი, როგორც სხვა ცნობილი სქემები, მოცემული ალგორითმებიც წარმოადგენს ელგამალის ალგორითმის, როგორც პროტოტიპის, გარკვეულ მოდიფიკაციას. მთავარი არსი მდგომარეობს მასში, რომ ზოგიერთი პარამეტრის გარკვეული ფუნქციონალური თვისების გამოყენებით მიიღება საჭირო სტრუქტურული ალტერნატივა.

ამოცანის აქტუალურობა: შეიძლება ითქვას, რომ საკუთრივ კრიპტოსისტემების თემატიკა აქტუალურია. გამოკვლეულ და მიღებულ სტრუქტურებს აქტუალობას ანიჭებს გარკვეული ელემენტების ორიგინალური ფუნქციური გამოყენებები ციფრული ხელმოწერის ალგორითმების შემთხვევაში, ხოლო სიმეტრიულ სისტემაში ის, რომ ალგებრული აპარატის ორიგინალური გამოყენების შედეგად მიღებული ურთიერთშებრუნებული მატრიცების აგების მეთოდი კონსტრუქციული და მარტივად რეალიზებადია (ამასთან, გასაღებთა სიმრავლე ხასიათდება მატრიცის განზომილების ფაქტორიალით). ამავე დროს მიგვაჩნია, რომ ქვეყანა, საზოგადოდ, გეგმაზომიერად უნდა ავითარებდეს სამამულო კრიპტოსისტემებს, რადგან იმპორტული კრიპტოსისტემები, როგორც წესი,

გამჭირვალეა ამ სისტემების მწარმოებელი ფირმებისა თუ სხვა ქვეყნებისათვის.

კვლევის მეთოდები: მრავალწევრთა ალგებრისა და გალუას სასრული ველების, კოდირების, ალბათობისა და რიცხვთა თეორიის აპარატი.

ნაშრომის სამეცნიერო სიახლე: 1. კრიპტოგრაფიულ სიმეტრიულ სისტემაში გასაღების ფორმირება ორიგინალური მატრიცებისა და ქსორის (ანუ ფსევდოშემთხვევითი მიმდევრობის) კომბინირებული გამოყენებით, რაც ეფუძნება მრავალწევრთა ალგებრასა და გალუას $GF(p^m)$ ველებში არსებულ ოპერაციებს და შეიძლება მარტივად განხორციელდეს პროგრამულად ან წანაცვლების სქემების მეშვეობით;. 2. ციფრული ხელმოწერისათვის მიღებულია ალგორითმის ორიგინალური ვარიანტები.

მოცულობა და სტრუქტურა- ნაშრომი შედგება:

-შესავალისაგან;

-სამი თავისაგან;

-დასკვნისაგან;

გამოყენებული ლიტერატურის ნუსხისაგან.

ნაშრომის მოცულობა შეადგენს 100 გვერდს.

შესავალში წარმოდგენილია და სადისერტაციო ნაშრომის "კრიპტოსისტემისა და ციფრული ხელმოწერის ალგორითმების სინთეზისათვის" აქტუალობა, და მოკლე შინაარსი, ჩამოყალიბებულია ნაშრომის მიზანი, მეცნიერული სიახლე და კვლევის მეთოდები.

I თავში აღწერილია კრიპტოგრაფიის განვითარების ისტორიული და მეთოლოგიური ასპექტები, კერძოდ, კრიპტოგრაფიის წარმოქნისა და განვითარების მეთოდები და, რაც მთავარია, კრიპტოგრაფიის აქტუალობა- მისი გამოყენების აუცილებლობა. მოცემულია ძირითადი კრიპტოგრაფიული მიმართულებანი და მათი გამოყენების არეალი (გამოყენების სფერო). აღწერილია კრიპტოალგორითმები და შესაბამისი სტანდარტები.

II თავში მოცემულია ორიგინალური სიმეტრიული კრიპტოსისტემის აგება მატრიცების მეშვეობით, კერძოდ აღწერილია მეთოდოლოგია, თუ როგორ შეიძლება მატრიცების კრიპტოგასაღებად გამოყენება. განხილულია მეთოდი, თუ როგორ შეიძლება მატრიცული მეთოდით აგებული კრიპტოსისტემის კრიპტომედეგობის გაზრდა n-განზომილებიანი ფსევდო-შემთხვევითი ქსორის დამატებით. განხილულია შეტევა და "გატეხვის" ვარიანტები მატრიცული მეთოდით აგებულ კრიპტოსისტემაზე.

III თავში მოცემულია ელგამალის ციფრული ხელმოწერის ორი ალტერნატიული ალგორითმი. ამ შემთვევაშიც, ელგამალის ალგორითმი არის კვლევის საგანი და პროტოტიპი, როგორც სხვა ცნობილი ციფრული ხელმოწერის ალგორითმებისათვის (მაგალითად, ГОСТ-ი, DSA და ა.შ.). კიდევ ერთხელ შეგვიძლია შევნიშნოთ, რომ ნაშრომში მოცემული ციფრული ხელმოწერის ორივე მეთოდი ორიგინალურია, თუმცა მათი შედარებითი კრიპტოანალიზი საყოველთაოდ ცნობილ ალგორითმებთან გარკვეულწილად არასრულია, მაგრამ შეტევის მეთოდები ძირითადად არის გამოკვლეული და განხილული.

ამგვარად დისერტაციაში წარმოდგენილი მეთოდები და გადაწყვეტილი ამოცანები აქტუალურია, მაგრამ, როგორც სხვა ცნობილ ორიგინალურ შემთვევებში, ახლაც მატრიცული და ციფრული ხელმოწერის ორივე მიდგომის კრიპტომედეგობა მოითხოვს შემდგომ გამოცდას და მტკიცებულებას (რადგან კრიპტოგრაფიული მეთოდის მედეგობას, როგორც ცნობილია, განსაზღვრავს "ცხოვრება"), რაც გარკვეული პროცესია.

თავი I

კრიპტოგრაფიის განვითარების ისტორიული და მეთოდოლოგიური მიმოხილვა

1.1. კრიპტოგრაფიის განვითარების ეტაპები

ინფორმაციის დასაიდუმლოება-დაცვა მისი გარდაქმნის მეშვეობით, რომელიც გამორიცხავდა მის წაკითხვას გარეშე პირის მიერ, აინტერესებდა კაცობრიობას უხსოვარი დროიდან. ინფორმაციის ამ საიდუმლო გარდაქმნას 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 დაშიფრვისათვის. 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, რომელიც ტოლია ანბანში სიმბოლოების რაოდენობისა). ბუნებრივია ტექსტის დაშიფვრის შემდეგი იდეა: მოცემულ ტექსტურ სიტყვებში და მთლიანად წინადადებაში ასო-ნიშნებს შევუცვალოთ ადგილები. პოზიციების ცვლილება, ცხადია, გამოიწვევს ტექსტში ასო-ნიშნების არევას და ტექსტის შინაარსის გაბუნდოვანებას, რაც განსაზღვრების თანახმად არის ტექსტის გარდაქმნა, ანუ დაშიფრვა. ასეთი დაშიფვრის წესია იულიუს ცეზარის ალგორითმი, რომელიც თავის მხრივ წარმოადგენს იმ დროს არსებული ალგორითმების 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 შესაბამის ასო-ნიშნებს, მივიღებთ დაშიფვრის ალგორითმს:

$$A\,B\,C\,D\,E\,F\,G\,H\,I\,J\,K\,L\,M\,N\,O\,P\,Q\,R\,S\,T\,U\,V\,W\,X\,Y\,Z$$
$$D\,E\,F\,G\,H\,I\,J\,K\,L\,M\,N\,O\,P\,Q\,R\,S\,T\,U\,V\,W\,X\,Y\,Z\,A\,B\,C$$

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 გადანაცვლების წესის გართულება, ვთქვათ სპეციალური ცხრილების (მატრიცების) შემოღება და სხვ.

მეორე შიფრი არის პოლიბეანური კვადრატი, რომელიც შექმნა ბერძენმა მწერალმა პოლიბეიმ. 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 მრავალალფავიტური გადანაცვლების მეთოდი. ეს შიფრი ცნობილია აგრეთვე ვიჟინერის სახელით (ბლეს ვიჟინერი – XVI საუკუნის დიპლომატი).

ვიჟენერმა (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-ნიშანი გადაადგილდეს k_1 პოზიციით, მე-2- k_2 პოზიციით და ა.შ. შეიძლება შემოვიღოთ l სიგრძის $k = k_1,...,k_l$ გასაღები, ანუ l სიგრძის გარკვეული სიტყვა ან l სიგრძის მთელი წინადადება.

მეორე მიმართულება გულისხმობს გარკვეული მატრიცის აგებას, რომელიც განახორციელებს დაშიფრვას. ასეთია ვიჟენერის 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 რიგითი 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 l, 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; $m_i \in \{0,\dots,N-1\}$. დავუშვათ, რომ მოცემული M ღია ტექსტური $a_1, a_2, a_3, \dots$ შეტყობინება, C სპეციალური $c_1, c_2, c_3, \dots$ ტექსტით (გასაღებით) დაშიფვრის შემდეგ

ღებულობს B შიფროტექსტის, ანუ $b_1, b_2, b_3, \ldots$ მიმდევრობის სახეს. M ტექსტის a_{v_i} სიმბოლოს შეესაბამება m_{v_i} რიცხვითი მნიშვნელობა, C გასაღების c_{u_i} სიმბოლოს- m_{u_i} მნიშვნელობა, ხოლო B შიფროტექსტის b_{w_i} სიმბოლოს- m_{w_i} მნიშვნელობა, სადაც $v_i, u_i, w_i \in \{0, \ldots, N-1\}$. მაშინ თითოეული სიმბოლოს დაშიფვრა და გაშიფვრა

$$m_{v_i} + m_{u_i} \equiv m_{w_i} \pmod{N},$$

$$m_{w_i} - m_{u_i} \equiv m_{v_i} \pmod{N}$$

შესაბამისობებით განხორციელდება.

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

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

XIX საუკუნეში ჰოლანდიელმა კერხოჰმა ჩამოაყალიბა კრიპტოგრაფიის ძირითადი წესი: შიფრის მედეგობა უნდა განისაზღვრებოდეს მხოლოდ გასაღების საიდუმლოობით. ინფორმაციის გამტაცებელს ან კრიპტოანალიტიკოსს შეუძლია, იცოდეს ყველა მონაცემი, გარდა გასაღებისა. ითვლება, რომ კრიპტოსისტემა გახსნილია, თუ გამტაცებელს დასაშვებზე მეტი ალბათობით შეუძლია შემდეგი ოპერაციების ჩატარება: საიდუმლო გასაღების პოვნა, გარდაქმნის ალგორითმის ეფექტური შესრულება, რომელიც ფუნქციონალურად ექვივალენტურია საწყისი კრიპტოალგორითმისა. იმისათვის, რომ

კრიპტოსისტემა გახსნილად ჩაითვალოს, საჭიროა არა მხოლოდ გასაღების გახსნის (ანუ საიდუმლო გასაღების პარამეტრების მიღების) ალგორითმის ჩვენება, არამედ იმის ჩვენებაც, რომ ეს ალგორითმი შეიძლება შესრულდეს რეალურ დროში. ალგორითმის გახსნის სირთულე ითვლება კრიპტოსქემის ერთ-ერთ მთავარ მახასიათებლად და მას კრიპტომედეგობა ეწოდება.

ფორმალური კრიპტოგრაფიის ბოლო სიტყვა, რომელიც საკმაოდ მაღალი კრიპტომედეგობას იძლეოდა როტორული კრიპტოგრაფია იყო (ავტომატიზირების მარტივი მეთოდები). პირველი შესაბამისი სისტემა გამოიგონა 1790 წელს მომავალმა ამერიკის პრეზიდენტმა თომას ჯეფერსონმა.

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

მაგალითად, ვთქვათ ღია ტექსტია:

“თუ ტექსტს არ დაშიფრავ მოწინააღმდეგე დაგამარცხებს”;

მაშინ სათანადო ანაკრები დისკოებზე არის:

თუტექსტსარ

დაშიფრავმო

წინააღმდეგ

ედაგამარცხ

ებს.

ხოლო დაშიფრული ტექსტია:

“თდწეეუაიდბტშნასეიაგქფაასრღმტამასვდრამეცროგხ”.

აქ გამოყენებული გადანაცვლება ადვილად შეიძლება გაიშიფროს, თუ პირველი “თ” ასოს შემდეგ წავიკითხავთ მეექვსე “უ” ასოს, შემდეგ მე-11 “ტ”-

ს, მე-16 “ე”-ს და ა.შ., ე.ი. ასო-ნიშნები შეიძლება ამოვიკითხოთ შიფროტექსტის იმ პოზიციებზე, რომლებიც ერთმანეთისაგან დაშორებულია გარკვეული ინტერვალებით. ამიტომ როტორულ მანქანებში ითვალისწინებენ, აგრეთვე, ღია ტექსტის ასო-ნიშნების სხვა ასო-ნიშნებით ჩანაცვლებას. მაგალითად, ვთქვათ, პირველ როტორზე “ა” ჩაიწერება როგორც “კ”, “ბ̃” როგორც “ლ” და ა.შ.; მეორე როტორზე იგივე “ა” ჩაიწერება როგორც “თ”, “ბ̃” როგორც “ტ” და ა.შ. ამრიგად, ტექსტის ასო-ნიშნები გადანაცვლებასთან ერთად აღმოჩნდება ჩანაცვლებული სხვა ასო-ნიშნებით და განსხვავებული წესით.

ყველაზე ცნობილი როტორული მანქანა იყო “ენიგმა”, რომელიც შეიქმნა ევროპაში 1917 წელს და მისი გაუმჯობესებული ვარიანტი გამოიყენეს გერმანელებმა მეორე მსოფლიო ომში (გარდა გერმანული ვარიანტისა იმჟამად არსებობდა ამერიკული *Sigama*, ინგლისური *Typex*, იაპონური Re*d*, *Orange* და *Purple*). პირველად “ენიგმა” გატეხეს პოლონელმა კრიპტოგრაფებმა და აცნობეს ინგლისელ კრიპტოანალიტიკოსებს, რომლებმაც განაგრძეს ახალი ვერსიების კრიპტოანალიზი [1, 9, 10, 15, 20, 42].

მეცნიერული კრიპტოგრაფიის (1930 წ.- 60-იანი წლები) ძირითადი განმასხვავებელია კრიპტოსისტემა მკაცრი მათემატიკური საფუძველით და კრიპტომედეგობით. 30-იანი წლებისათვის საბოლოოდ ჩამოყალიბდა მათემატიკური მიმართულებანი, რომლებიც წარმოადგენენ მეცნიერულ საფუძველს კრიპტოლოგიისა: ალბათობის თეორია და მათემატიკური სტატისტიკა, ზოგადი ალგებრა, რიცხვთა თეორია, აქტიურად დაიწყო განვითარება ალგორითმების თეორიისა, ინფორმაციის თეორიისა და კიბერნეტიკის. თავისებური წყალგამყოფი გახდა კლოდ შენონის ნაშრომი “კავშირგაბმულობის თეორია საიდუმლო სისტემებში” (1949 წ) [8, 6].

მეოცე საუკუნის 60-იან წლებში მოწინავე კრიპტოგრაფიულმა სკოლებმა შექმნეს ბლოკური შიფრი, რომელიც უფრო მედეგია როტორულ

კრიპტოსისტემებთან შედარებით, თუმცა მისი რეალიზაციისათვის საჭიროა ციფრული ელექტრონული მოწყობილობანი.

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 საშუალებების 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" (1976 წ.). ამ ნაშრომში პირველად იყო ფორმულირებული დაშიფრული ინფორმაციის გაცვლის პრინციპები საიდუმლო გასაღების გარეშე [1,2,3,42].

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). დასაიდუმლოების მიზნით ღია ტექსტის გარდაქმნას ეწოდება **დაშიფვრა (შიფრაცია)**, ხოლო დაშიფრული ტექსტიდან ღია ტექსტის აღდგენას- **გაშიფვრა (დეშიფრაცია)**. შიფრაციისა და დეშიფრაციის მეთოდებისა და ალგორითმების კვლევას

კრიპტოანალიზი ეწოდება, ხოლო მათემატიკის დარგს, რომელიც სწავლობს კრიპტოგრაფიასა და კრიპტოანალიზს - **კრიპტოლოგია**.

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

კლასიკურ კრიპტოგრაფიაში არ არის მიღებული საკუთრივ ალგორითმის (შიფრის) დამალვა-დასაიდუმლოება, თუმცა, ასეთი მიდგომის მართებულობა კერძო შემთხვევებში არ არის გამორიცხული.

ალგორითმის დასაიდუმლოება გაუმართლებელია იმის გამო, რომ მისი გამჟღავნება გამოიწვევს დაშიფრული ტექსტის, ანუ, როგორც 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 ალგორითმის სინთეზის დროს, კრიპტოგრაფი ქმნის ალგორითმის (შიფრის) ალტერნატიული განხორციელების უამრავ ვარიანტს (გასაღებების სიმრავლეს) და მოცემული სამოქმედო პერიოდისათვის შეირჩევს ერთ-ერთ მათგანს. ალტერნატიული ვარიანტის შერჩევა დაკავშირებულია **გასაღების** შერჩევაზე.

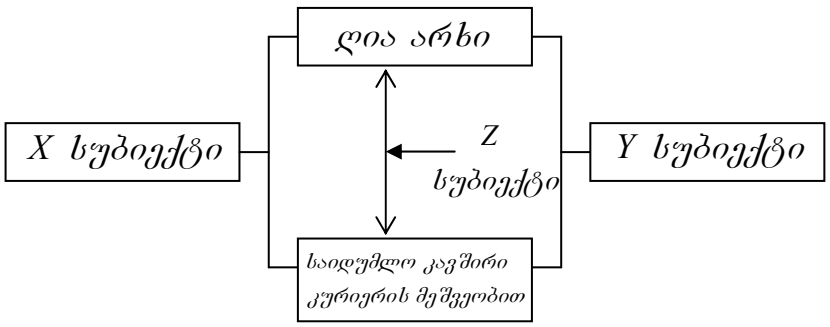
ზემოაღნიშნული შეიძლება განვიხილოთ სეიფის მაგალითზე. სეიფის დაცვის მოცემული წესი წარმოადგენს გარკვეული ალგორითმის განხორციელებას, ე.ი. ალგორითმის განხორციელებაა სეიფზე განთავსებული ელემენტები (შესაძლოა რამდენიმე დისკოს სახის) და მათზე გამოსახული ციფრთა ანაკრები (გარკვეული კომბინაცია), რიცხვი (გასაღები), 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. თანამედროვე 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 შეიძლება მიიღოს ციფრების ნებისმიერი მნიშვნელობა.

1.2. კრიპტოგრაფიული მეთოდები და სისტემები

განვიხილოთ ინფორმაციის გაცვლის უმარტივესი მოდელი. ინფორმაციის გადამცემი და მიმღები მხარეები პირობით აღვნიშნოთ 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 სუბიექტს შორის ინფორმაციის კრიპტოგრაფიული გაცვლის პრინციპული სქემა. Z სუბიექტი განიხილება, როგორც X და Y სუბიექტების მოწინააღმდეგე მხარე.



ნახ1.2. 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 დაშიფრული 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 მიზანია ინფორმაციის გარდაქმნა და X სუბიექტისაგან Y სუბიექტისათვის ისე გადაცემა, რომ იგი გაუგებარი და გამოუყენებელი იყოს ნებისმიერი Z სუბიექტისათვის. ეს არის ინფორმაციის საკუთრივ დასაიდუმლოების (დაშიფვრის) პრობლემა. მაგრამ ამ ძირითადი ამოცანის გარდა კრიპტოგრაფიას აქვს სპეციალური ამოცანები, რომელთა შორისაა:

ნამდვილობა (**აუტენტიფიკაცია**). 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 არაუარყოფითობა. გამგზავნს არ უნდა შეეძლოს უარყოს შეტყობინების 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 ოპერაციებში 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, რადგან X და Y სუბიექტებს შორის კავშირი ხორციელდება პრინციპულად ერთისა და იმავე გასაღების გამოყენებით. მეორე კლასის მეთოდებს უწოდებენ **ასიმეტრიულს**, რადგან X და Y სუბიექტებს შორის კავშირი ხორციელდება განსხვავებული გასაღებებით 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 საიმედობაა, 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 შიფრაციისა და დეშიფრაციის სისტემა DES; უ.დიფის და მ.ჰელმანის ღია არხით გასაღების გაცვლის პირველი

ასიმეტრიული მეთოდი, აგრეთვე, შიფრაციის და ნამდვილობის დამადასტურებელი სისტემა *RSA* და ტ.ელგამალის ციფრული ხელმოწერის ასიმეტრიული ალგორითმი.

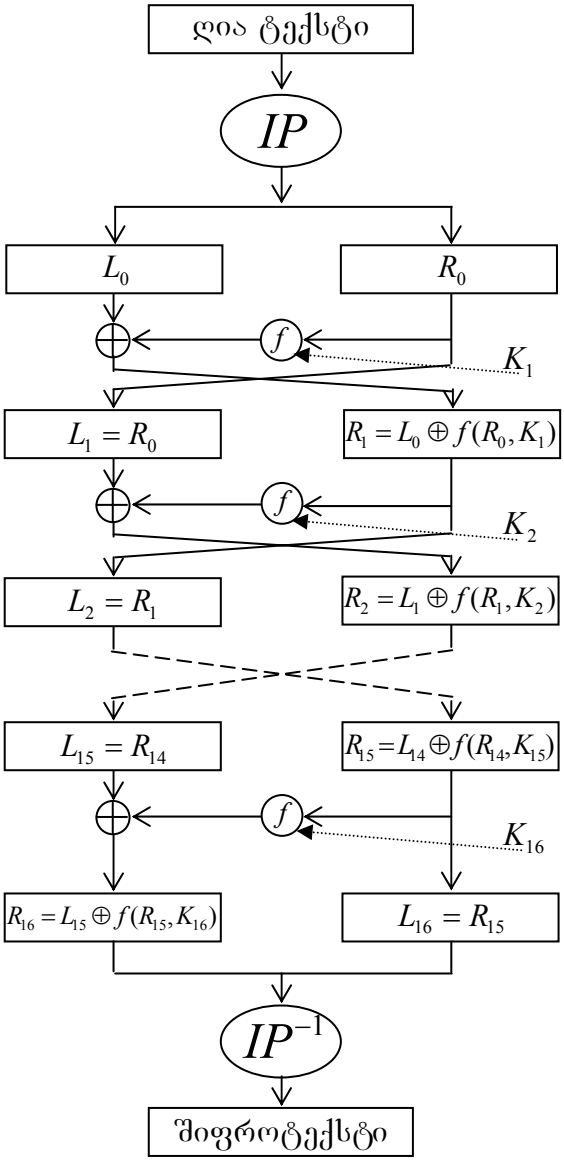
1.2.1. კრიპტოგრაფიული სისტემა *DES*

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

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

სიმეტრიული სისტემებიდან დღეისათვის ყველაზე წარმატებულია ამერიკული სისტემა *DES*-ი.

DES-ი (*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 Standarrt* Institute) სტანდარტს.



ნახ.1.3. *DES* სისტემის გამარტივებული სქემა

ალგორითმი DEA პირველად გამოკვლეული და დამუშავებულია ცნობილი IBM-ის ფირმის მიერ 1970 წელს (შემდგომ უმჯობესდებოდა.) ალგორითმი ამუშავებს 64-ბიტიანი განზომილების ღია ტექსტურ ბლოკებს და იყენებს 56-ბიტიან გასაღებებს. ალგორითმის განვითარებასა და სრულყოფაში დიდი წვლილი მიუძღვის, აგრეთვე, უშიშროების ეროვნულ სააგენტოს (*National* Institute *of S* tan *dards and Techno* log *y* - *NIST* ,

a division of the U.S. Deoartment of Commerce; ყოფილი: NBS- National Bureau of Standards).

ალგორითმის ძირითადი ოპერაციებია: ჩანაცვლება, გადანაცვლება, მოდულით 2 და ქვებლოკებად დაყოფის ლოგიკური ოპერაციები და სხვ. ალგორითმი მუშაობს ღია ტექსტის 64-ბიტიან ბლოკებზე, რის შედეგად გამოსასვლელზე მიიღება 64-ბიტიანი შიფროტექსტი. ტექსტის დაშიფვრა ხდება 16 ეტაპის განმავლობაში, რომლებშიც ოპერაციები მსგავსია. ოპერაციის განსხვავებულობა 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 შემოწმებისათვის გამოიყენება. ამიტომ ძირითად ფუნქციას გასაღების 56 ბიტი ახორციელებს (ამასთან, შიფრაციის ეტაპზე გასაღებიც განიცდის გარკვეულ გადანაცვლებას).

მიუხედავად ოპერაციათა სიმარტივისა, *DES*-ი ქმნის მაღალ კრიპტომედეგობას. კრიპტომედეგობის ანალიზი მკაცრ გამოთვლებს არ ექვემდებარება. ამიტომ იმის მოლოდინი, რომ ალგორითმი შეიძლება გატყდეს, არსებობდა გარკვეული პერიოდის განმავლობაში და შეიძლება მომავალშიც არსებობდეს. მაგრამ გაუმჯობესებული ვარიანტი რეალურად ამართლებს სტანდარტისადმი წაყენებულ საყოველთაოდ ცნობილ მოთხოვნებს.

დეშიფრაცია თითქმის არ განსხვავდება შიფრაციისაგან. დამახასიათებულია ძირითადად ის, რომ დეშიფრაციის დროს k_i გასაღებები გამოიყენება საწინააღმდეგო თანამიმდევრობით.

DES სისტემას 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 უფრო გასაგები გახდეს შემდეგი მარტივი მაგალითის განხილვის შედეგად. ვთქვათ, ორ პიროვნებას გიორგის და ირაკლის მიზნად აქვს დასახული, რომ საუბრის დროს ერთმანეთს შეატყობინოს საიდუმლო ინფორმაცია. მათთან ერთად 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 მეთოდი შემდეგში მდგომარეობს:

სურ.1.2.-ზე მოცემული სქემის შესაბამისად X და Y ორი სუბიექტი (Z სუბიექტის არსებობის პირობებში) ღია არხით კურიერის გარეშე

ამყარებს შემდეგ ინფორმაციულ კავშირს. დავუშვათ, რომ p მარტივი და a ნატურალური რიცხვები გაცხადებულია, ანუ ღიაა (p მაღალი რიგის, $\approx 2^{500}$ სიდიდის მარტივი რიცხვია; $1 < a < p$). ინფორმაციის გაცვლას X და Y მხარეებს შორის აქვს შემდეგი სახე:

X მხარე საიდუმლო (კერძო) გასაღებად შეირჩევს x ნატურალურ რიცხვს ($1 < x < p$); გამოთვლის

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

რიცხვს და ღია არხით გადააგზავნის Y მხარეზე.

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

$$c_1^{\ y} \equiv a^{xy} \equiv k_1 \bmod p$$

რიცხვს. k_1 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

$$c_2^{\ x} \equiv a^{yx} \equiv k_2 \bmod p$$

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):

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

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

მაგრამ, პირიქით, x ელემენტის გამოთვლა c ელემენტის მიხედვით გაცილებით რთულია და მოითხოვს დაახლოებით $p^{1/2}$ 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 გალოგარითმებას უკეთეს შემთხვევაში- $2^{p/2}$ ოპერაცია.

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

დიფი-ჰელმანის ალგორითმი გამოიყენება როგორც გასაღებების გაცვლის, დაშიფვრის, აგრეთვე, აუტენტიფიკაციის მიზნით კრიპტოგრაფიული პროტოკოლების ამოცანებში და სხვ.

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

$$c_1 = 2^2 \equiv 4 (\mathrm{mod} 11),$$
$$c_2 = 2^4 \equiv 5 (\mathrm{mod} 11),$$
$$K_1 = 4^4 \equiv 5 \cdot 5 \equiv 3 (\mathrm{mod} 11),$$
$$K_2 = 5^2 \equiv 3 (\mathrm{mod} 11),$$

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, რაც, ცხადია, ცნობილია Y მხარესათვისაც. 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 $K = 3$ გასაღებით:

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

მიღებულ C შიფროტექტს 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. ეიდლმენმა დაამუშავეს შიფრაციისა და ნამდვილობის (აუტენტიფიკაციის) ახალი მეთოდი. RSA დაპატენტებულია შეერთებულ შტატებში, ლიცენზირებულია სხვა ქვეყნებში და წარმოადგენს ფაქტიურ სტანდარტს მსოფლიოს მრავალ ქვეყანაში [1, 2, 3, 14, 38, 41].

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:

$$\varphi(N) = (p-1)(q-1)$$

და $\varphi(N)$ რიცხვს დაასაიდუმლოებს.

შემდეგ 2-დან $(\varphi(N)-1)$-დე ინტერვალში შეირჩევს e რიცხვს (როგორც შემთხვევით რიცხვს; თუ $(e,\varphi(N)) \neq 1$, მაშინ შეირჩევს 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

$$ed \equiv 1 \bmod k\varphi(N), \tag{1.1}$$

შედარებიდან, აგრეთვე

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

შესაბამისომიდანაც.

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

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

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

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

Z მხარე d რიცხვის მნიშვნელობას ვერ გამოთვლის, რადგან ამისათვის მან უნდა გადაწყვიტოს ერთ-ერთი ამოცანა: ან გამოთვალოს $\varphi(N)$ ფუნქციის მნიშვნელობა ან იპოვოს N რიცხვის ერთ-ერთი მარტივი მამრავლი (ფაქტორიზაციის ამოცანა), რაც დროის რეალურ მასშტაბში თანამედროვე კომპიუტერული სიმძლავრეებით შეუძლებელია.

მაგალითი. დავუშვათ, რომ $p = 3$, $q = 5$, $M = 3$, მაშინ

$$N = pq = 15; \quad \varphi(N) = (p-1)(q-1) = 8.$$

(1.1) თანაფარდობიდან

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

ანუ

$$e = 3, \quad d = 3.$$

Y მხარე გაშიფრავს მას:

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

1.2.4. ელგამალის კრიპტოსისტემა

მოცემული სისტემა წარმოადგენს RSA-ს ალტერნატივას და მისგან განსხვავებით ეყრდნობა დისკრეტული ლოგარითმის პრობლემას. ამით იგი წააგავს დიფფი-ჰელმანის 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 გასაღებს $y = g^x \bmod p$. თუ Y მხარეს სურს გაუგზავნოს X მხარეს m ტექსტი, ის ირჩევს შემთხვევით k რიცხვს ($k < p$) და გამოთვლის

$$y_1 = g^k \bmod p$$

და

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

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

X მხარე მიღებულ დაშიფრულ შეტყობინებას აღადგენს:

$$m = (y_1^{\ x} \bmod p) \oplus y_2 .$$

1.2.5. ელიფსური ფუნქციების გამოყენება კრიპტოგრაფიაში

ელიფსური წირები (ფუნქციები)- მათემატიკური ობიექტია, რომელიც შეიძლება განსაზღვრულ იქნეს ნებისმიერ ველზე (სასრულ, ნამდვილ, რაციონალურ და კომპლესურ ველზე). კრიპტოგრაფიაში ძირითადად გამოიყენება სასრული ველები. ელიფსური წირი არის (x, y) წერტილთა სიმრავლე, რომელიც აკმაყოფილებს შემდეგ განტოლებას [56]:

$$y^2 = x^3 + ax + b,$$

და ამასთან უსასრულოდ დაშორებული წერტილი. საკმაოდ ადვილია წირზე წერტილების შეკრება, რომელიც იგივე როლს თამაშობს რაც გამრავლების ოპერაცია RSA-სა და ელგამალის კრიპტოსისტემებში.

რეალურ კრიპტოსისტემებში ელიფსური ფუნქციების დროს გამოიყენება შემდეგი განტოლება:

$$y^2 = x^3 + ax + b \bmod p,$$

სადაც p მარტივი რიცხვია.

1.3. ელექტრონული (ციფრული) ხელმოწერის ალგორითმები

1.3.1 ციფრული ხელმოწერის დანიშნულება

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

რაში მდგომარეობს მონაცემთა აუტენტიფიკაცია?

ყოველი ტექსტს ან დოკუმენტს ბოლოს თან ერთვის, ხელმოწერა (სპეციალური ჩანაწერი), რომლითაც მიიღწევა ორი შედეგი; ა). მიმღები მხარე დარწმუნდება წერილის (შეტყობინების) ნამდვილობაში, შეამოწმებს

რა ხელმოწერას სათანადო ფორმულის (შემოწმების ფორმულის) მეშვეობით; და ბ). ხელმოწერა წარმოადგენს იურიდიულ გარანტიას დოკუმენტის ავტორობისა, რომ დოკუმენტი ეკუთვნის მოცემულ ავტორს და არა ვინმე სხვას. ეს ასპექტი ძალიან მნიშვნელოვანია სხვადასხვა კომერციული ხელშეკრულების დადების დროს, მინდობილობის შედგენისა და სხვა.

თანამედროვე მსოფლიოში ძალიან გავრცელებულია დოკუმენტების ელექტრონული (ციფრული) ფორმა (მათ შორის, კონფიდიციალურიც) და მათი დამუშავების ხერხები. ამასთან აქტუალურია ციფრული დოკუმენტაციის ნამდვილობისა და ავტორობის პრობლემა.

ქაღალდზე ადამიანის ხელმოწერის გაყალბება საკმაოდ რთულია (რასაკვირველია, თანამედროვე კრიმინალისტიკით ამის გარკვევა საკმაოდ ადვილია), ხოლო ციფრული ხელმოწერის გაყალბება, დოკუმენტის შეცვლა, ავტორობის უფლებების დარღვევა და ა.შ. საკმაოდ ადვილია, თუ არ არის დაცული ციფრული ხელმოწერისათვის საჭირო გარკვეული პროტოკოლებით. ამიტომ აუტენტიფიკაციის დროს აუცილებელია შესაბამისი კრიპტოალგორითმები.

ვთქვათ, გვაქვს ორი მომხმარებელი: ამირანი და ბადრი. რა დარღვევებისაგან უნდა დაგვიცვას აუტენფიკაციის სისტემამ?

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 ამირანისაგან მიღებულ შეტყობინებას (ტექსტს) გადააკეთებს და ამტკიცებს რომ, გადაკეთებული შეტყობინება მიიღო ამირანისაგან.

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

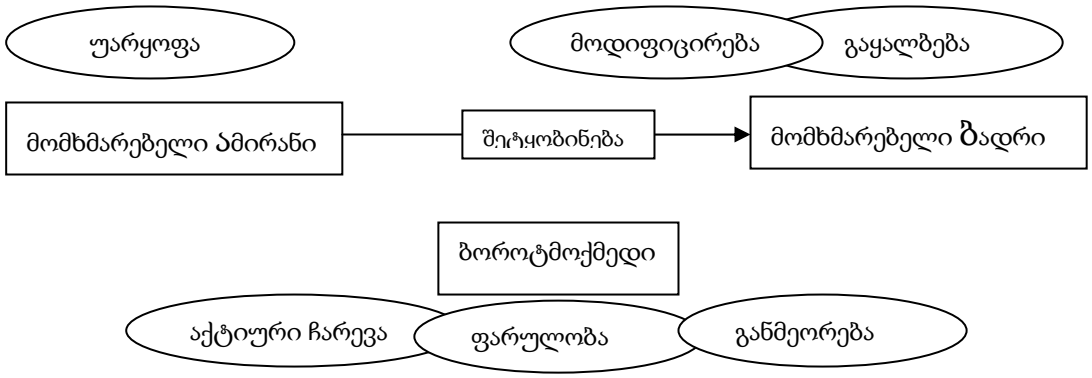
აქტიური ჩარევა. ლადო ხელთ იგდებს შეტყობინებას, რომელსაც ამირანი უგზავნის ბადრის და ფარულად ცდილობს შეცვალოს შეტყობინება თავის სასარგებლოდ.

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

ამ შემთხვევაშიც დაცვის მიზნით გამოიყენება ელექტრონული (ციფრული) ხელმოწერა.

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

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



ნახ.1.4. შესაძლო დარღვევები შეტყობინების დაცვისა, რომელსაც მომხმარებელი ამირანი უგზავნის მოხმარებელ ბადრის.

1.3.2. 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 გასაღებებია, ხოლო $e, n = pq$ - კი ღია; p, q - მარტივი რიცხვებია.

შენიშვნა.

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

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

დავუშვათ ამირანი გადასცემს ბადრის შემდეგ შეტყობინებას: DATA.

ამირანი ხელს აწერს შეტყობინება DATA-ს გადაცემის დროს ბადრისათვის:

$$Ee_ბ, n_ბ \{Ed_ა, n_ა \{DATA\}\}.$$

ამასთან იგი იყენებს:

ა) ამირანის საიდუმლო გასაღებს $Ed_ა, n_ა$,

ბ) ბადრის ღია გასაღებს $Ee_ბ, n_ბ$.

ბადრის შეუძლია წაიკითხოს ხელმოწერილი შეტყობინება თავდაპირველად ბადრის საიდუმლო გასაღებით $Ed_ბ, n_ბ$:

$$Ed_ა, n_ა \{DATA\} = Ed_ბ, n_ბ \{Ee_ბ, n_ბ \{Ed_ა, n_ა \{DATA\}\}\}$$

და შემდეგ ამირანის ღია გასაღებით ($Ee_ა, n_ა$) მიიღოს:

$$DATA = Ee_ა, n_ა \{Ed_ა, n_ა \{DATA\}\}.$$

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 ლადო) საიდუმლო გასაღების გარეშე ვერ შეძლებს ცვლილებების შეტანას ტექსტში (შეტყობინებაში) რომელიც გადაეცემა.

მოცემული სქემა საშუალებას იძლევა შუამავლების გარეშე გადაწყვიტოს სხვადასხვა კონფლიქტური სიტუაცია.

1.3.3. ელგამალის ციფრული ხელმოწერის ალგორითმი

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

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

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

იმისათვის, რომ M შეტყობინებას თან დაერთოს ხელმოწერა, ამისათვის ვირჩევთ შემთხვევით k რიცხვს, რომელიც ერთიერთმარტივია ($p-1$)-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 ინახება საიდუმლოდ. შემოწმებისათვის იყენებენ შემდეგ შესაბამისობას:

$$y^R g^S \bmod p \equiv g^M \bmod p.$$

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

1.3.4. ციფრული ხელმოწერის ალგორითმი *DSA*

1999 წლის აგვისტოში აშშ სტანდარტებისა და ტექნიკის ნაციონალურმა ინსტიტუტმა (National Institute of Standards and Technology, NIST) თავისი ციფრული ხელმოწერის სტანდარტისათვის (Digital Signature Standard, DSS) შემოიღო ციფრული ხელმოწერის სტანდარტი (Digital Signature Algorithm, DSA) [15, 41].

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

DSA ციფრული ხელმოწერის ალგორითმი იყენებს შემდეგ პარამეტრებს:

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

q - 160-ბიტიანი მარტივი რიცხვი, $q|p-1$.

$g \equiv h^{(p-1)/q} \bmod p$, სადაც h ნებისმიერი 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 ნებისმიერი მომხმარებლისათვის ხელმისაწვდომი. დაფარული (საიდულო) გასაღებია x, ხოლო ღია- y.

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

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

(2) ამირანი აგენერირებს

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

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

ამირანი ციფრული ხელმოწერის r და s პარამეტრებს, m შეტყობინებასთან ერთად უგზავნის ბადრის.

(3) ბადრი ამოწმებს ამირანის ხელმოწერას, გამოთვლის რა:

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

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

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

$$v \equiv ((g^{u_1} * y^{u_2}) \bmod p) \bmod q.$$

თუ $v = r$, ციფრული ხელმოწერა სწორია.

1.3.5. ციფრული ხელმოწერის ალგორითმი ГОСТ

ამ რუსულ სტანდარტს ციფრული ხელმოწერისა, ოფიციალურად ჰქვია ГОСТ Р 34.10-94 [15, 17, 18, 41] .

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

q - მარტივი რიცხვია, $q \mid p-1$, რომლის სიგრძეა 254-დან 256 ბიტამდე;

g - ნებისმიერი რიცხვია, $a < p-1$ და $g^q \bmod p = 1$;

x - რიცხვი, $x < q$;

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

ეს ალგორითმიც იყენებს ცალმხრივ ჰეშ-ფუნქციას: $H(m)$.

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 რიცხვს, სადაც $k < q$,

(2) ამირანი აგენერირებს:

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

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

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 შეამოწმებს 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

$$y \equiv g^x \equiv 2^4 \equiv 5 \ (\bmod 11).$$

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

$$R \equiv g^k \equiv 2^6 \equiv 9 \ (\bmod 11).$$

ვთქვათ, $M' = H(M) = 5$.

ხელმოწერის მეორე პარამეტრი არის:

$$S \equiv xR + kM' \equiv 4 \cdot 9 + 6 \cdot 5 \equiv 6 \ (\bmod 10).$$

Y მხარეზე შემოწმების შედეგია:

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

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

$$3 \equiv 3 \cdot 1 \pmod{11}.$$

მაშასადამე, შემოწმების პირობა სრულდება და მიღებული ინფორმაცია სანდოა.

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

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

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

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

მაშასადამე, ღია ტექსტში შეტანილი ცვლილება შემოწმების შედეგად გამოვლენილია.

თავი I I

სიმეტრიული კრიპტოსისტემის აგება მატრიცული მეთოდის გამოყენებით

2.1. ზოგადი მიდგომა მატრიცული გასაღების მისაღებად

მატრიცული მეთოდის ძირითადი განსხვავება ვიჟინერის მეთოდისგან არის ის, რომ ვიჟინერის მეთოდში ბლოკებად დაყოფილი დასაშიფრი a ტექსტი (ორობითი სიტყვა) მრავლდება ვექტორზე (განიხილება ვექტორული ნამრავლი ვექტორულ ალგებრაში, ანუ ქსორირება), ხოლო მატრიცულ მეთოდში ტექსტი მრავლდება გარკვეული მეთოდით გენერირებულ მატრიცზე. ე.ი. შიფრაცია ხდება შემდეგნაირად: ბლოკი, როგორც x ვექტორი, გამრავლდება შესაბამისი განზომილების მატრიცზე. დეშიფრაციის დროს კი მიღებული ვექტორი უნდა გავამრავლოთ შებრუნებულ მატრიცზე, რაც აღადგენს საწყის ვექტორს:

$$x \cdot A = x^{\#}; \qquad x^{\#} \cdot A^{-1} = x. \tag{2.1}$$

ასეთი მიდგომის დროს, როგორც ნებისმიერი სიმეტრიული სისტემის დროს, ძირითად პრობლემას წარმოადგენს: ა) გასაღებთა სიმრავლის ფორმირება-ანუ მატრიცთა სიმრავლისა (რასაკვირველია, ის არ უნდა ექვემდებარებოდეს გადარჩევას რეალურ დროში, რაც არის მისი ძირითადი კრიპტომედეგობა); ბ) ამასთან- შიფრაცია- დეშიფრაციის სიჩქარე და სხვა.

ძირითადი მიზანი ზემოთ ხსენებული მეთოდისა წარმოადგენს სპეციალიზირებული არაგადაგვარებული მატრიცების კლასების ფორმირებას, რომელიც დააკმაყოფილებს საყოველთაოდ მიღებულ კრიპტომედეგობის სტანდარტებს.

A მატრიცს მოეთხოვება, რომ იყოს გადაუგვარებული (ე.ი. დეტერმინანტი 0-ის ტოლი არ უნდა იყოს), რათა გააჩნდეს შებრუნებული, ე.ი. პრობლება გადაუგვარებული მატრიცების სინთეზისა და მათი შებრუნებულის პოვნაში მდგომარეობს. როდესაც საქმე გვაქვს დიდი განზომილების მქონე მატრიცებთან, მათი შებრუნებულის გამოთვლა ცნობილი მეთოდებით დიდ დროს მოითხოვს. ამიტომ საჭიროა, შეიქმნას რეგულარული მეთოდები, რომლებიც მარტივი ალგორითმებით მოგვცემს მატრიცის შებრუნებულს, ე.ი. გამოიყოს ისეთი კლასი მატრიცებისა, რომელთა შებრუნებულის პოვნა რეალიზდება რთული ალგორითმული გამოთვლების გარეშე.

განვიხილოთ ჯერ ცნობილი მეთოდები მატრიცის შებრუნებულის პოვნისა. ცნობილია არაერთი მეთოდი,- მაგალითად, $A = (a_{ij})^n$ მატრიცის შებრუნებულის პოვნა (არასინგულარულის) შემდეგი სახით:

$$A^{-1} = \begin{bmatrix} \frac{A_{11}}{|A|} & \frac{A_{21}}{|A|} & \cdots & \frac{A_{n1}}{|A|} \\ \frac{A_{12}}{|A|} & \frac{A_{21}}{|A|} & \cdots & \frac{A_{n21}}{|A|} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{A_{1n}}{|A|} & \frac{A_{2n}}{|A|} & \cdots & \frac{A_{nn1}}{|A|} \end{bmatrix}, \qquad (2.2)$$

სადაც A_{ij} არის A მატრიცის a_{ij} ელემენტების ალგებრული დამატება.

როგორც ნათლად ჩანს, მიუხედავად იმისა, რომ ორობით $GF(2)$ ველზე (2.2) ოპერაციების ჩატარება დღევანდელი მეთოდოლოგიებით ადვილია, მაგრამ საჭირო გამოთვლები, ცხადია, დროს მოითხოვს და, რაც მთავარია, მისი მეშვეობით ძნელია გარკვეული კლასის ფორმირება, რომლისთვისაც (2.2) მატრიცები მიიღება ტრივიალური გზით.

დასახული მიზნის მიღწევა არც შემდეგი მატრიცული ნამრავლის მეშვეობითაა შესაძლებელი:

$$E_k E_{k-1} \ldots E_1 \, A = 1 \,,$$

და

$$E_k E_{k-1} \dots E_1 = A^{-1},$$

სადაც A^{-1} არის A მატრიცის მარცხენა შებრუნებული მატრიცი; $E_k E_{k-1} \dots E_1$ წარმოადგენენ ელემენტარულ მატრიცებს, რომელთა მეშვეობით A მატრიცი შესაძლებელია დავიყვანოთ კანონიკურ და, მაშასადამე, ერთეულოვან სახემდე.

განსხვავებულ მეთოდს წარმოადგენს A^{-1} მატრიცის i-ური სვეტის $x_1, x_2, \dots, x_n$ ელემენტების მისაღებად (გამომდინარე $A \cdot A^{-1} = 1$ ტოლობიდან) განტოლებათა შემდეგი სისტემის ამოხსნა:

$$a_{i1}x_1 + a_{i2}x_2 + \dots + a_{kn}x_n = \begin{cases} 0, & \text{თუ } k \neq i; \\ 1, & \text{თუ } k = i, \end{cases} \tag{2.3}$$

სადაც $k = 1, 2, \dots, n$. რადგან $|A| \neq 0$, ამიტომ (2.3) სისტემას აქვს ერთადერთი ამონახსნი, რის შედეგადაც, საზოგადოდ, A^{-1} შებრუნებული მატრიცი მიიღება.

კოდირების ალგებრული თეორიიდან ცნობილია, რომ მრავალწევრთა ალგებრაში $GF(q)$ ველზე მოდულით $f(x)$ მიიღება კლასები მატრიცებისა, რომლებიც წარმოქმნიან

$$G = \begin{bmatrix} g_{11} & g_{12} & \dots & g_{1n} \\ g_{21} & g_{22} & \dots & g_{2n} \\ \dots & \dots & \dots & \dots \\ g_{k1} & g_{k2} & \dots & g_{kn} \end{bmatrix} \tag{2.4}$$

და

$$H = \begin{bmatrix} h_{11} & h_{12} & \dots & h_{1n} \\ h_{21} & h_{22} & \dots & h_{2n} \\ \dots & \dots & \dots & \dots \\ h_{r1} & h_{r2} & \dots & h_{rn} \end{bmatrix} \tag{2.5}$$

სახის მაწარმოებელ და შემმოწმებელ ბაზისურ მატრიცებს, რომლებიც აკმაყოფილებს

$$GH^T = 0 \tag{2.6}$$

პირობას (H^T რის H მატრიცის ტრანსპონირებული მატრიცი, $n = k + r$). შესაბამისი მატრიცების სტრიქონთა სივრცე რამოადგენს მრავალწევრთა იდეალებს. ასეთი მატრიცებისათვის დამახასიათებელია $g(x)$ და $h(x)$ მაწარმოებელი მრავალწევრები ($g(x) \cdot h(x) = f(x)$), რომლებიც G (2.4) და H (2.5) ბაზისურ მატრიცების სტრიქონებს აფორმირებს [7, 8, 16, 23, 27, 30, 31, 32, 33, 35, 36, 40, 57, 71, 75].

გარკვეული ანალოგიით, მაგრამ აღნიშნულისგან განსხვავებით ავაგოთ n რიგის კვადრატული მატრიცები და მათი შებრუნებულები შემდეგი სახით:

$$A = \begin{bmatrix} a_1 & a_2 & a_3 & \dots & a_{n-1} & a_n \\ 0 & a_1 & a_2 & \dots & a_{n-2} & a_{n-1} \\ 0 & 0 & a_1 & \dots & a_{n-3} & a_{n-2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_1 & a_2 \\ 0 & 0 & 0 & \dots & 0 & a_1 \end{bmatrix}, \tag{2.7}$$

სადაც (2.7) მატრიცის სტრიქონებს მრავალწევრთა იდეალების ბაზისური მატრიცების მსგავსად შეადგენენ $GF(2)$ ველზე განსაზღვრული $a \in V_n$ გარკვეული (კონკრეტული) ვექტორის კომპონენტები (ანუ A მატრიცს აწარმოებს $g = (a_1, \dots, a_n)$ ვექტორი, ხოლო A^{-1} იწარმოება გარკვეული განსხვავებული $h = (a_1, \dots, a_n)$ ვექტორის კომპონენტებით).

ფიქსირებული g ვექტორისათვის შესაძლებელია შებრუნებულის პოვნის ერთ-ერთი მეთოდით (2.3) სისტემის მეშვეობით) განისაზღვროს h ვექტორის სახე ნებისმიერი მთელი დადებითი n-ისათვის. მაგალითად, (2.3)-ში მათემატიკური ინდუქციის გამოყენებით შეიძლება ვაჩვენოთ, რომ n რიგის

$$A=\begin{bmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{bmatrix}, \tag{2.8}$$

მატრიცისათვის, რომლის მაწარმოებელი ვექტორი არის $g=(a_1,\dots,a_n)$ ($a_i=1$, თუ $i\le 2$ და $a_i=0$, თუ $i>2$), შებრუნებულ მატრიცს აქვს სახე:

$$A^{-1}=\begin{bmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 0 & 1 & 1 & \dots & 1 & 1 \\ 0 & 0 & 1 & \dots & 1 & 1 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{bmatrix}, \tag{2.9}$$

სადაც $h=(a_1,\dots,a_n)$, $a_i=1$ $(1\le i\le n)$.

ანალოგიურად, $g=(a_1,\dots,a_n)$ ($a_i=1$, თუ $i\le 3$ და $a_i=0$, თუ $i>3$) და $h=(a_1,\dots,a_n)$ ($a_i=1,\ i=3k+1,\ i=3k+2;\ a_i=0,\ i=3k$) მაწარმოებელი ვექტორებისათვის შესაბამისად მიიღება:

$$A=\begin{bmatrix} 1 & 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & 1 & \dots & 0 & 0 \\ 0 & 0 & 1 & 1 & \dots & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \end{bmatrix}, \tag{2.10}$$

$$A^{-1} = \begin{bmatrix} 1 & 1 & 0 & \dots & 1 & 1 & 0 \\ 0 & 1 & 1 & \dots & 0 & 1 & 1 \\ 0 & 0 & 1 & \dots & 1 & 0 & 1 \\ 0 & 0 & 0 & \dots & 1 & 1 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 0 & 1 \end{bmatrix}. \qquad (2.10')$$

ე.ი. ((2.10) და (2.10')) მატრიცებს აწარმოებენ შესაბამისად g და h ვექტორები იმ პირობით, რომ მატრიცებში ყოველი i-ური სტრიქონი წარმოადგენს $(i-1)$-ე სტრიქონის კომპონენტების წანაცვლებას ერთი პოზიციით და რომ ((2.10) და (2.10')) მატრიცის $(i+1)$-ე სტრიქონის პირველი i კომპონენტი ნულის ტოლია.

მოცემული (2.8)-(2.10') სახის მატრიცების სინთეზის მიზანი მდგომარეობს იმაში, რომ არ განვახორციელოთ მატრიცის შებრუნებულის გამოთვლა, არამედ გარკვეული მარტივი შესაბამისობით შეგვეძლოს შებრუნებულის პოვნა.

იმისათვის, რომ გასაღებს გააჩნდეს მაღალი მედეგობა, საჭიროა, სიმრავლეში იყოს საკმაოდ დიდი რაოდენობის გასაღები. ავიღოთ n-განზომილებიანი ერთ-ერთი განხილული მატრიცი და მისი შებრუნებული. თუ საწყის მატრიცში გადავაადგილებთ სტრიქონებს, მიღებული მატრიცის შებრუნებულის საპოვნელად საჭიროა საწყისი მატრიცის შებრუნებულში გადავაადგილოთ შესაბამისი სვეტები, ე.ი. ერთი მატრიციდან შეგვიძლია მივიღოთ $n!$ რაოდენობის მატრიცი. ასევე, შესაბამისი სვეტებისა და სტრიქონების გადანაცვლებით მიიღება ისეთივე რაოდენობის მატრიცი და მთლიანობაში $(n!)^2$ სიმრავლე ფიქსირებული g და h ვექტორებისათვის.

მატრიცული გასაღებების მეთოდით საჭირო გასაღებების სინთეზი შესრულდება შემდეგი თანმიმდევრობით: შეირჩევა შესაბამისი g და h ვექტორები, მოხდება A და A^{-1} მატრიცების გენერაცია და შემდეგ

შემთხვევითი (ფსევდოშემთხვევითი) რიცხვის შესაბამისად მატრიცებში განხორციელდება სათანადო გადანაცვლებები.

რა უპირატესობა გააჩნია მატრიცულ მეთოდს ვიჟინერის მეთოდთან შედარებით, სადაც ტექსტი ასევე ბლოკებად იყოფა? ვიჟინერის მეთოდში რომ "გატყდეს" ერთ-ერთი შიფროტექსტის ბლოკის ნაწილი, ცნობილი გახდება თვითონ გასაღების ნაწილი და, შესაბამისად, ეს ნაწილი "გატყდება" ყოველ ინფორმაციულ ბლოკში: ხოლო მატრიცული გასაღების დროს ერთ n-განზომილებიან ბლოკში ინფორმაციის გახსნით (იგულისხმება ღია ტექსტით თავდასხმა) შეუძლებელია მატრიცის პარამეტრების მიღება და მთლიანად ან ნაწილობრივ მატრიცული გასაღების "გატეხვა". მატრიცის გატეხვისათვის საჭიროა n განზომილებიანი მიმდევრობით აღებული n ბლოკი, რათა მივიღოთ შესაბამის n^2 უცნობთა და განტოლებათა შესატყვისობა.

ნაშრომში მატრიცული გასაღების მეთოდი გამიზნულია კომბინირებული კრიპტოსისტემების შესაქმნელად, რომელშიც ერთად იქმნება გამოყენებული ღია არხით სარგებლობის ცნობილი მეთოდები და მატრიცული მეთოდი, თუმცა გარკვეული მომხმარებლისათვის მისი არც ცალკე (სხვა მეთოდებისაგან დამოუკიდებლად) გამოყენებაა მიუღებელი.

2.2. ორიგინალური მატრიცული გასაღების სინთეზი მრავალწევრთა ალგებრაში და სიმეტრიული კრიპტოსისტემა

განხილული ამოცანის გადაწყვეტა უფრო მიზანდასახული იქნება, თუ გამოვიყენებთ კოდირების ალგებრულ სტრუქტურებს, კერძოდ, $GF(q)$ ველზე (სიმარტივისათვის განვიხილავთ $GF(2)$ ველს) მოდულით $f(x)$ მრავალწევრთა ალგებრაში იდეალების თვისებებს. ცნობილია, რომ n-განზომილებიან მრავალწევრთა ნაშთთა კლასები მოდულით $f(x)$ $GF(2)$ ველზე წარმოქმნიან მრავალწევრთა A_n ალგებრას და, მაშასადამე,

ვექტორულ V_n სივრცეს (ვგულისხმობთ, რომ $a=(a_1,...,a_n)\in V_n$ და $a(x)=\sum_{i=1}^{n}a_i x^i \in A_n$ წარმოადგენენ ექვივალენტურ ელემენტებს).

ცნობილია, ასევე, რომ A_n ალგებრაში ნებისმიერი I იდეალისათვის არსებობს ერთადერთი ნორმირებული $g(x)$ მრავალწევრი მინიმალური ხარისხისა ისეთი,* რომ $\{g(x)\}$ ნაშთთა კლასი ეკუთვნის I იდეალს და პირიქით, თითოეული ნორმირებული $g(x)$ მრავალწევრი, გამყოფი $f(x)$-ისა, აწარმოებს გარკვეულ I იდეალს, რომელშიც $g(x)$ არის მინიმალური ხარისხის მრავლწევრი ისეთი, რომ $g(x)$ ნაშთთა კლასი ეკუთვნის I იდეალს.

სამართლიანია შემდეგი

თეორემა 2.1. ვთქვათ, $f(x)=g(x)h(x)$, სადაც $f(x)$ არის n ხარისხის მრავალწევრი, ხოლო $h(x)$- k ხარისხისა. მაშინ $\{g(x)\}$ ნაშთთა კლასით ნაწარმოები იდეალი მოდულით $f(x)$ მრავალწევრთა ალგებრაში არის k განზომილებისა.

ეს ნიშნავს, რომ $g(x)$ მრავალწევრის ხარისხი არის

$$n-k=r. \qquad (2.11)$$

სამართლიანია აგრეთვე

თეორემა 2.2. დავუშვათ, $f(x)$, $g(x)$ და $h(x)$ ნორმირებული მრავალწევრებია და $f(x)=g(x)h(x)$, მაშინ $\{a(x)\}$ ნაშთთა კლასი ეკუთვნის $h(x)$-ით ნაწარმოებ იდეალის ნულოვან სივრცეს მაშინ და მხოლოს მაშინ, როდესაც ის ეკუთვნის $\{g(x)\}$-ით ნაწარმოებ იდეალს.

ზემოთქმულიდან გამომდინარეობს შემდეგი

---

* განვიხილოთ x უცნობის მიმართ n-ური ხარისხის: $f(x)=f_0+f_1x+...+f_nx^n$ მრავალწევრები F ველზე. მრავალწევრს ეწოდება **ნორმირებული**, თუ უმაღლესი ხარისხის x^n უცნობის f_n კოეფიციენტი უდრის 1-ს.

შედეგი 2.1. ვთქვათ, $f(x) = g(x)h(x)$, სადაც $f(x)$ - n ხარისხის და $g(x)$ - r ხარისხის მრავალწევრებია. მაშინ $GH^T = 0$, სადაც G და H მატრიცებს შესაბამისად $g(x)$ და $h(x)$ მრავალწევრები აწარმოებენ.

$g = (g_0, ..., g_{n-1})$ ვექტორის კომპონენტების ციკლური გადანაცვლება i პოზიციით წარმოადგენს $g = (g_i, ..., g_{n+i-1})$ ვექტორს; ანუ $g(x) = 1 + x + ... + x^r$ მრავალწევრის i-ური გადანაცვლება გვაძლევს $g(x^{(i)}) \equiv x^i g(x) \bmod(x^n - 1)$ მრავალწევრს.

ვთქვათ, $g(x)h(x) = x^n - 1$, $g(x)$ და $h(x)$ აწარმოებენ შესაბამისად I და $I^{'}$ იდეალებს. მაშინ

$$G = \begin{bmatrix} g_0 & g_1 & \dots & g_r & 0 & \dots & 0 & \dots & 0 \\ 0 & g_0 & \dots & g_{r-1} & g_r & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & g_0 & \dots & g_r \end{bmatrix}, \tag{2.12}$$

$$H = \begin{bmatrix} h_0^* & h_1^* & \dots & h_k^* & 0 & \dots & 0 & \dots & 0 \\ 0 & h_0^* & \dots & h_{k-1}^* & h_k^* & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & h_0^* & \dots & h_k^* \end{bmatrix}, \tag{2.13}$$

რაც ნიშნავს, რომ ნებისმიერი $g(x^{(i)})$ და $h(x^{(j)})$ მრავალწევრებისათვის სამართლიანია ტოლობა:

$$g(x^{(i)})h(x^{(j)}) \equiv 0 \bmod(x^n - 1), \tag{2.14}$$

სადაც $i, j \in \{1, ..., n\}$. თუ გავითვალისწინებთ, რომ $GF(2)$ ველზე მრავალწევრთა და ვექტორთა ნამრავლი არ ემთხვევა ერთმანეთს, მაშინ ნებისმიერი $g \in I$ ვექტორისათვის

$$gH^{*T} = 0, \tag{2.15}$$

სადაც H^* მატრიცი ნაწარმოებია h^* ვექტორით, რომელიც შეიცავს h ვექტორის კომპონენტებს, ჩაწერილს საწინააღმდეგო თანმიმდევრობით (ე.ი. h^* წარმოადგენს h ვექტორის სარკისებურ შებრუნებულს).

მაშასადამე, (2.14) და (2.15) ექვივალენტური ტოლობები (რაც ჩვენთვის მნიშვნელოვანია) სამართლიანია, რადგან I და I^* იდეალები წარმოადგენენ ჩაკეტილ სიმრავლეებს ვექტორთა ნებისმიერი ციკლური წანაცვლების მიმართ.

განვიხილოთ (2.7) მატრიცის შესაბამისი n რიგის კვადრატული მატრიცები, ნაწარმოები $g(x)$ და $h(x)$ მრავალწევრებით (რომელთა კოეფიციენტების მეშვეობით მიღებულია (2.12) და (2.13) მატრიცების სტრიქონები):

$$A_1 = \begin{bmatrix} g_0 & g_1 & \dots & g_r & 0 & \dots & 0 & \dots & 0 \\ 0 & g_0 & \dots & g_{r-1} & g_r & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 & \dots & g_0 \end{bmatrix}, \qquad (2.16)$$

$$A_2 = \begin{bmatrix} h_0 & h_1 & \dots & h_k & 0 & \dots & 0 & \dots & 0 \\ 0 & h_0 & \dots & h_{k-1} & h_k & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 & \dots & h_0 \end{bmatrix}, \qquad (2.17)$$

სადაც A_2 მატრიცის ყოველი j-ური სვეტი წარმოადგენს $h'(j)$ ვექტორს მოდულით $x^n - 1$ ალგებრაში, რომლის i-ური კომპონენტები იგივეა, რაც $h^*(x)\, x^{r+j-1}$ ვექტორის კომპონენტები, თუ $i \le j$ და $h'_i = 0$, თუ $i > j$.

ყოველივე ზემოთქმულიდან ((2.11) და (2.15) პირობების გათვალისწინებით) გამომდინარეობს, რომ

$$g(i)\, h'(j)^T = \begin{cases} 0, & \text{თუ } i \neq j; \\ 1, & \text{თუ } i = j, \end{cases} \qquad (2.18)$$

სადც h'^T ვექტორი (2.18) ტოლობაში წარმოადგენს ვექტორ-სვეტს (ანუ h' ვექტორის ტრანსპონირებულ ვექტორს).

მაშასადამე, სამართლიანია

თეორემა 2.3. ვთქვათ, $g(x)$ და $h(x)$, შესაბამისად r და k ხარისხის მრავალწევრებია $GF(2)$ ველზე მოდულით $(x^n - 1)$ ალგებრაში ისეთი, რომ

$g(x)h(x) = x^n - 1$, ხოლო A_1 და A_2 ((2.16) და (2.17)) n რიგის $g(x)$ და $h(x)$ მრავალწევრებით ნაწარმოები მატრიცებია. მაშინ A_1 და A_2 ურთიერთშებრუნებულია, ე.ი.

$$A_1 A_2 = \mathrm{I}, \quad A_2 A_1 = \mathrm{I},$$

სადაც I ერთეულოვანი მატრიცია.

არსებობს კონსტრუქციული მეთოდი $x^n - 1$ მოდულით ალგებრაში $g(x)$ და $h(x)$ მრავალწევრების მიღებისა, რომელთათვისაც $g(x)h(x) = x^n - 1$, რაც 2.3 თეორემით მიღებული მეთოდის კონსტრუქციული განხორციელებისათვის საჭირო წინაპირობებს უზრუნველყოფს. ცნობილია $g(x)$ და $h(x)$ მრავალწევრების აგების შესაძლებლობა მინიმალური მრავალწევრების საშუალებით.*

მინიმალური მრავალწევრის თვისებებს გალუას სასრულ ველზე წარმოადგენს შემდეგი თეორემები.

თეორემა 2.4. ვთქვათ, $f(x)$ არის მრავალწევრი $GF(q)$ ველის კოეფიციენტებით, ხოლო β $f(x)$ მრავალწევრის ფესვია $GF(q)$ ველის გაფართოებაში, მაშინ β^q არის $f(x)$ მრავალწევრის ფესვი.

თეორემა 2.5. ვთქვათ, $p(x)$ არის $GF(q)$ ველის კოეფიციენტებიანი m ხარისხის მრავალწევრი, რომელიც დაუყვანადია ამავე ველში და ვთქვათ, β არის $p(x)$ მრავალწევრის ფესვი $GF(q)$ ველის გაფართოებაში, მაშინ $\beta, \beta^p, .., .., \beta^{p^{m-1}}$ ყველა ელემენტი $p(x)$ მრავალწევრის ფესვია.

თეორემა 2.6. თუ $f(x)$ მრავალწევრია $GF(q)$ ძირითად ველზე, მაშინ $f(\beta) = 0$ მაშინ და მხოლოდ მაშინ, როდესაც $f(x)$ იყოფა β ელემენტის $m(x)$ მინიმალურ მრავალწევრზე.

---

* დავუშვათ, რომ β არის $F(\alpha)$ გაფართოების ელემენტი. მინიმალური ხარისხის ნორმირებულ მრავალწევრს ძირითადი F ველის კოეფიციენტებით ეწოდება β ელემენტის **მინიმალური ფუნქცია**, ანუ **მინიმალური მრავალწევრი**, თუ $m(\beta) = 0$.

მაგალითი. ვიპოვოთ $\alpha \in GF(2^4)$ ელემენტის $m(x)$ მინიმალური ფუნქცია.

I ხერხი. აღვნიშნოთ α ელემენტის შესაბამისი მინიმალური ფუნქცია $m_1(x)$-ით. 2.5 თეორემის თანახმად $m_1(x)$ მინიმალური ფუნქციის ფესვებია, აგრეთვე, $\alpha^2, \alpha^4, \alpha^8$, ე.ი. $m_1(x) = m_2(x) = m_4(x) = m_8(x)$ და საძიებელი ფუნქცია მეოთხე ხარისხისაა. მაშასადამე, $m_1(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$. მამრავლების გადამრავლების შედეგად ვღებულობთ:

$$\begin{aligned} m_1(x) &= (x^4 - \alpha^2 x^2 - \alpha x^3 + \alpha^3 x^2 - \alpha^4 x^3 + \alpha^6 x^2 + \alpha^5 x^2 - \alpha^7 x - \\ &- \alpha^2 x^3 + \alpha^{10} x^2 + \alpha^9 x^2 - \alpha^{11} x + \alpha^{12} x^2 - \alpha^{14} x - \alpha^{13} x + \alpha^{15}) = \\ &= x^4 - (\alpha + \alpha^2 + \alpha^4 + \alpha^8) x^3 + (\alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12} + \alpha^5 + \alpha^{10}) x^2 - \\ &- (\alpha^7 + \alpha^{14} + \alpha^{13} + \alpha^{11}) x + 1 \end{aligned}$$

(რადგან $\alpha^{15} = 1$ $GF(2^4)$ ველში). თუ გავითვალისწინებთ, რომ ოროზით ველში ნიშანს არა აქვს მნიშვნელობა და α^i ველის ელემენტების შეკრებას განვახორციელებთ მოცემული ველის ელემენტების გამოყენებით (მაგალითად, $\alpha + \alpha^2 + \alpha^4 + \alpha^8 = \alpha + \alpha^2 + (1 + \alpha^3) + (\alpha + \alpha^2 + \alpha^3) = 1$), შედეგად მივიღებთ:

$$m_1(x) = 1 + x^3 + x^4.$$

ბუნებრივია, რომ მიღებული მინიმალური ფუნქცია ემთხვევა $p(x) = 1 + x^3 + x^4$ მრავალწევრს, რადგან α ელემენტი არის მოცემული $GF(2^4)$ ველის $p(x)$ მოდულის ფესვი. მკითხველს შეუძლია ანალოგიური გზით იპოვოს α^3 ელემენტის შესაბამისი მინიმალური $m_3(x)$ ფუნქცია, რომელიც წარმოადგენს $\alpha^6, \alpha^{12}, \alpha^{24} = \alpha^9$, ელემენტების შესაბამის $m_6(x) = m_9(x) = m_{12}(x)$ მინიმალურ მრავალწევრებს და, აგრეთვე, სხვა ელემენტების მინიმალურ ფუნქციებს.

II ხერხი. როგორც აღვნიშნეთ, $m_1(x)$ მრავალწევრი მეოთხე ხარისხისაა. ვთქვათ

$$m_1(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + x^4 \; ; \qquad (2.19)$$

($a_4 = 1,$ რადგან $m(x)$ ნორმირებული მრავალწევრია).

$$\begin{array}{lllll}
\alpha^0 & = 1 & & & (1000) \\
\alpha & = & \alpha & & (0100) \\
\alpha^2 & = & & \alpha^2 & (0010) \\
\alpha^3 & = & & \alpha^3 & (0001) \\
\alpha^4 & = 1 & & + \alpha^3 & (1001) \\
\alpha^5 & = 1 + \alpha & & + \alpha^3 & (1101) \\
\alpha^6 & = 1 + \alpha + \alpha^2 + \alpha^3 & & & (1111) \\
\alpha^7 & = 1 + \alpha + \alpha^2 & & & (1110) \\
\alpha^8 & = & \alpha + \alpha^2 + \alpha^3 & & (0111) \\
\alpha^9 & = 1 & + \alpha^2 & & (1010) \\
\alpha^{10} & = & \alpha & + \alpha^3 & (0101) \\
\alpha^{11} & = 1 & + \alpha^2 + \alpha^3 & & (1011) \\
\alpha^{12} & = 1 + \alpha & & & (1100) \\
\alpha^{13} & = & \alpha + \alpha^2 & & (0110) \\
\alpha^{14} & = & + \alpha^2 + \alpha^3 & & (0011) \\
\hline
\alpha^{15} & = 1 & & & (1000)
\end{array}$$

ნახ. 2.1. $GF(2^4)$ ველის მულტიპლიკაციური ჯგუფის მაგალითი

$\{x\}$ ნაშთთა კლასი აღვნიშნოთ $\alpha \in GF(2^4)$ ელემენტით (სურ.2.1). მაშინ (2.19) გამოსახულებაში x^0 ჩაიწერება, როგორც $\alpha^0 = (1000)$, $x - \alpha = (0100)$, $x^2 - \alpha = (0010)$, $x^3 - \alpha^3 = (0001)$, $x^4 - \alpha^4 = (1001)$; მივიღებთ განტოლებათა სისტემას:

$$a_0 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + a_1 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + a_2 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + a_3 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = 0$$

ანუ

$$
\begin{aligned}
a_0 \qquad\qquad &+1=0;\\
a_1 \qquad\qquad &=0;\\
a_2 \qquad\qquad &=0;\\
a_3 &+1=0;
\end{aligned}
$$

საიდანაც $a_0 = a_3 = 1$, $a_1 = a_2 = 0$, ე.ი. $m_1(x) = 1 + x^3 + x^4$.

შემოწმებით შეიძლება დავრწმუნდეთ, რომ $\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$ ელემენტების მინიმალური ფუნქცია არის $m_3(x) = 1 + x + x^2 + x^3 + x^4$; α^5, α^{10} ელემენტების მინიმალური ფუნქცია არის $m_5(x) = 1 + x + x^2$; $\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$ ელემენტების მინიმალური ფუნქცია- $m_7(x) = 1 + x + x^4$; $\alpha^0 = 1$ ელემენტის მინიმალური ფუნქცია- $m_0(x) = 1 + x$. ამრიგად,

$$x^{15} - 1 = (1 + x)(1 + x^3 + x^4)(1 + x + x^2 + x^4) \times (1 + x + x^2)(1 + x + x^4),$$

ე.ი. $x^{15} - 1$ ორწევრის ყველა 15 ფესვი $GF(2^4)$ ველის ყველა არანულოვანი ელემენტია.

მაგალითი. მრავალწევრთა A_7 ალგებრაში მოდულით $x^7 - 1$ $GF(2)$ ველზე $g(x) = 1 + x + x^3$ და $h(x) = 1 + x + x^2 + x^4$ მრავლწევრებისათვის $g(x)\,h(x) = x^7 - 1$. მიიღება

$$
A_1 = \begin{bmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 0\\
0 & 1 & 1 & 0 & 1 & 0 & 0\\
0 & 0 & 1 & 1 & 0 & 1 & 0\\
0 & 0 & 0 & 1 & 1 & 0 & 1\\
0 & 0 & 0 & 0 & 1 & 1 & 0\\
0 & 0 & 0 & 0 & 0 & 1 & 1\\
0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}, \qquad (2.20)
$$

$$A_2 = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \qquad (2.20')$$

ურთიერთშებრუნებული მატრიცები.

მაგალითი. განვიხილოთ შემთხვევა როდესაც p ტოლია არა 2-ის, არამედ 3-სა. ე.ი. ავაგოთ $GF(3)$ ველზე $g(x)$ და $h(x)$ პოლინომები მრავალწევრთა $A_{n=8}$ ალგებრაში $x^8 - 1$ მოდულით. $p(x) = x^2 + 2x + 2$ არის პრიმიტიული მრავალწევრი $GF(3)$ ველზე. დავაგენერიროდ მულტიპლიკატიური ჯგუფი $GF(3^2)$ ველში მოდულით $p(x)$, სადაც α პრიმიტიული ელემენტია ($p(\alpha) = 0$):

$$\begin{aligned} \alpha^0 &= 1 \\ \alpha^1 &= \alpha \\ \alpha^2 &= 1 + \alpha \\ \alpha^3 &= 1 + 2\alpha \\ \alpha^4 &= 2 \\ \alpha^5 &= 2\alpha \\ \alpha^6 &= 2 + 2\alpha \\ \alpha^7 &= 2 + \alpha \\ &- - - - - - - \\ \alpha^8 &= 1 \end{aligned}$$

α და α^3 ელემენტების მინიმალური ფუნქცია არის $m_1 = x^2 + 2x + 2$; ხოლო α^2 და α^6 ელემენტების მინიმალური ფუნქცია კი- $m_2(x) = x^2 + 1$. როგორც ზემოთ აღვნიშნეთ, მინიმალური ფუნქციების

ნამრავლი გვაძლევს $g(x)$; ანუ $g(x) = m_1(x)m_2(x) = x^4 + 2x^3 + 2x + 2$; აქედან მომდინარეობს, რომ $h(x) = (x^8 - 1)/g(x) = x^4 + x^3 + x^2 + 2x + 1$.

(2.16) და (2.17) გათვალისწინებით ვღებულობთ:

$$A_1 = \begin{bmatrix} 1 & 2 & 0 & 2 & 2 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 2 & 2 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} 1 & 1 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

2.3. მატრიცული მეთოდის გატეხვის შესაძლებლობა

განვიხილოთ შემთხვევა, თუ როგორ ხდება ინფორმაციის დაშიფვრა და როგორ შეიძლება შემოთავაზებული მატრიცული მეთოდის "გატეხვა" (ვიგულისხმოთ, რომ "გატეხვა" არის ჰაკერის (ანალიტიკოსის) მიერ გასაღების, ჩვენს შემთხვევაში მატრიცის, ხელში ჩაგდება, ანუ მისი უცნობი პარამეტრების განსაზღვრა).

დავუშვათ, ჰაკერმა (ანალიტიკოსმა) მოიპოვა ღია ტექსტი. თუ ღია ტექსტის ზომა გაუტოლდება n^2 სიდიდეს (აქ n არის მატრიცის (გასაღების) ზომა), მაშინ შეიძლება ვაჩვენოთ, რომ ჰაკერი (ანალიტიკოსი) ხელში ჩაიგდებს გასაღებს, ანუ მატრიცს (იხ. საკითხის განხილვა ქვემოთ).

როგორც ზემოთ იყო აღნიშნული, შიფრაცია-დეშიფრაციის მატრიცული მეთოდის გამარტივებული სახეა:

$$a \cdot A = b; \qquad b \cdot A^{-1} = a,$$

სადაც a არის ღია ტექსტი, ხოლო b შიფროტექსტი. აქ a ღია ტექსტი უნდა დაიყოს n მონაკვეთებად (ვექტორებად) და ცალკეული n ზომის ვექტორი უნდა გამრავლდეს A მატრიცზე და ამით მიიღება შესაბამისი განზომილების შიფროტექსტი:

$$a^{(1)} \cdot A = (a_{11}, a_{12}, ..., a_{1n}) \cdot A = b^{(1)} = (b_{11}, b_{12}, ..., b_{1n}),$$

$$a^{(2)} \cdot A = (a_{21}, a_{22}, ..., a_{2n}) \cdot A = b^{(2)} = (b_{21}, b_{22}, ..., b_{2n}), \qquad (2.21)$$

. . . . . .

$$a^{(n)} \cdot A = (a_{n1}, a_{n2}, ..., a_{nn}) \cdot A = b^{(n)} = (b_{n1}, b_{n2}, ..., b_{nn}).$$

ჰაკერის (ანალიტიკოსის) ერთ-ერთი უმთავრესი მიზანია გასაღების (მატრიცის) მიღება, ე.ი. მატრიცის n^2 უცნობის პოვნა. თუ ის შეძლებს n^2 წრფივად დამოუკიდებელ განტოლებათა შედგენას, მაშინ ის ააგებს განტოლებათა სისტემას და "გატეხავს" გასაღებს, ე.ი. (2.16) (და (2.17)) მატრიცული გასაღების j-ური სვეტის ელემენტების გამოსათვლელად n განტოლებათა შესაბამის სისტემას აქვს შემდეგი სახე:

$$a_{11}x_{1j} + a_{12}x_{2j} + \ldots + a_{1n}x_{nj} = b_{1j},$$

$$a_{21}x_{1j} + a_{22}x_{2j} + \ldots + a_{2n}x_{nj} = b_{2j}, \qquad (2.21')$$

. . . . . .,

$$a_{n1}x_{1j} + a_{n2}x_{2j} + \ldots + a_{nn}x_{nj} = b_{nj}.$$

იმისათვის, რომ "გატყდეს" მატრიცული გასაღები საჭიროა n^2 რაოდენობის (2.21) სახის განტოლება, ანუ განტოლებათა $(2.21')$ სისტემა $j=1,...,n$ მნიშვნელობებისათვის.

მართალია, დიდი ზომის მატრიცების დროს $GF(p)$ ველზე ეს პრობლემატურია, მაგრამ არც მატრიცის ზომის ძალიან გაზრდაა რეკომენდირებული, რაც იწვევს, რასაკვირველია, დიდ აპარატულ დატვირთვას და შიფრაციის სიჩქარის შემცირებას. განვიხილოთ მაგალითი:

დავუშვათ, ზემოთ ხსენებული მეთოდის შესაბამისად დავაგენერირეთ 3-განზომილებიანი A მატრიცი:

$$A=\begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{pmatrix}.$$

განვიხილოთ ღია (დასაშიფრი) ტექსტი $a=(a_{11}\,a_{12}\,a_{13}\,a_{21}\,a_{22}\,a_{23}\,...)$. დავყოთ ღია ტექსტი a 3-განზომილებიან მონაკვეთებათ (ვექტორებად):

$$a^{(1)}=(a_{11}\,a_{12}\,a_{13}),\quad a^{(2)}=(a_{21}\,a_{22}\,a_{23}),\quad a^{(3)}=(a_{31}\,a_{32}\,a_{33}),\ ,\ \ldots.$$

შესაბამისი ღია ტექსტის შიფროტექსტებს ექნება შემგეგი სახე:

$$b^{(1)}=a^{(1)}A=(a_{11}\,a_{12}\,a_{13})\begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{pmatrix}=(b_{11},b_{12},b_{13}),$$

$$b^{(2)}=a^{(2)}A=(a_{21}\,a_{22}\,a_{23})\begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{pmatrix}=(b_{21},b_{22},b_{23}),$$

$$b^{(3)}=a^{(3)}A=(a_{31}\,a_{32}\,a_{33})\begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{pmatrix}=(b_{31},b_{32},b_{33})\ ,$$

. . . . . .

გასაგებია, რომ, თუ ანალიტიკოსი (ჰაკერი) ამ შემთხვევაში ხელში ჩაიგდებს ღია ტექსტის 3 მონაკვეთს (ვექტორს) და ექნება შესაბამისი შიფროტექსტის მონაკვეთები, მაშინ ის შეძლებს ($2.21'$)-ის შესაბამისად) 9 განტოლების აგებას 9 უცნობით და მატრიცის (გასაღების) ყველა ელემენტის პოვნას (რეალურად მატრიცის განზომილება უნდა იყოს 100 ან მეტი, ე.ი. 100 მიმდევრობით 100-განზომილებიანი შიფროტექსტის დროს ანალიტიკოსს ხელთ უნდა ჰქონდეს 100 შესატყვისი n-განზომილებიანი მონაკვეთი ღია ტექსტისა).

2.4. ფსევდოშემთხვევითი მიმდევრობის გენერირება $GF(p^m)$ ველში და მისი გამოყენება შიფროტექსტის ქსორირებისათვის

იმისათვის, რომ, Z ანალიტიკოსს გავურთულოთ ღია ტექსტით თავდასხმა მოვემულ კრიპტოსისტემაზე, შიეძლება გამოვიყენოთ შიფრაციის წინ ღია ტექსტის ქსორირება (XOR); ე.ი. n ზომის ღია ტექსტებს დაედება ქსორი, ანუ გარკვეული მონაკვეთები $N = 2^k - 1$ განზომილების ფსევდოშემთხვევითი მიმდევრობისა:

$$c = a + d,$$

ვიგულისხმოთ, რომ $d = (d_{11}d_{12}\ldots d_{1n}, d_{21}, \ldots, d_{nn}, \ldots)$.

მაშინ შიფროტექსტს ექნება შემდეგი სახე:

$$b = cA = (a + d)A.$$

განვიხილოთ ერთი მონაკვეთის (რასაკვირველია n სიდიდის) დაშიფვრა:

$$c^{(1)} \cdot A = (c_{11}, c_{12}, \ldots, c_{1n}) \cdot A = b^{(1)} = (b_{11}, b_{12}, \ldots, b_{1n}).$$

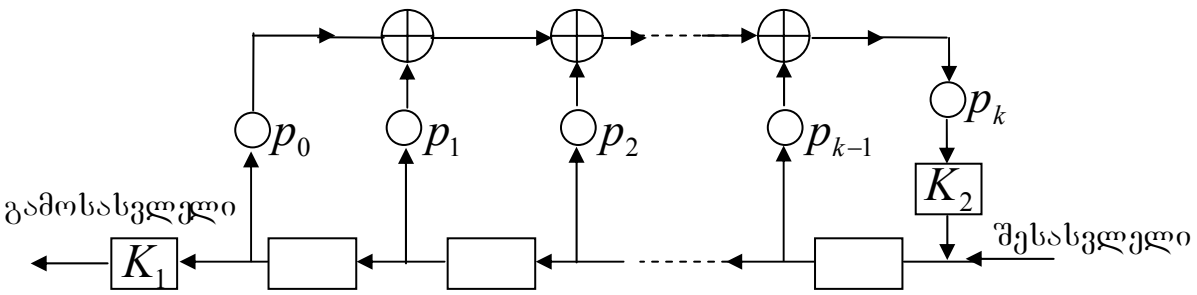
მაშინ გასაღების "გატეხვის" ($2.21'$) სისტემა მიიღებს შემდეგ სახეს:

$$
\begin{aligned}
&c_{11}x_{1j} + c_{12}x_{2j} + \ldots + c_{1n}x_{nj} = b_{11},\\
&c_{21}x_{1j} + c_{22}x_{2j} + \ldots + c_{2n}x_{nj} = b_{21},\\
&\ldots\ldots\ldots\ldots\ldots\\
&c_{n1}x_{1j} + c_{n2}x_{2j} + \ldots + c_{nn}x_{nj} = b_{n1},
\end{aligned}
\qquad (2.22)
$$

სადაც Z სუბიექტისათვის გვაქვს $n(n+1)$ უცნობი და n განტოლება. ამ შემთხვევაში Z სუბიექტმა მატრიცული გასაღების "გასატეხად", $(2.21')$-ის შესაბამისად, ხელში უნდა ჩაიგდოს არა მარტო შიფროტექსტის შესატყვისი ღია ტექსტი, არამედ, მასთან ერთად, შესაბამისი მონაკვეთები ფსევდოშემთხვევითი მიმდევრობისა; მხოლოდ ასე შეძლებს Z ანალიტიკოსი კრიპტოსისტემის "გატეხვას".

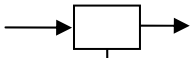
N ფსევდოშემთხვევითი მაქსიმალური სიგრძის მიმდევრობა გენერირდება წანაცვლების რეგისტრებით, რომელთა ფუნქციონირება ქვემოთ არის განხილული.

წანაცვლების რეგისტრები (როგორც ზემოთ არის ნაჩვენები) ახორციელებენ გამრავლების და გაყოფის ოპერაციებს. ჩვენთვის საინტერესოა რეგისტრები, ასევე, რომლებიც ასრულებენ ველის ელემენტების გამოთვლებს და წარმოქმნიან მაქსიმალური სიგრძის ფსევდოშემთხვევით n-მიმდევრობებს. მაქსიმალური სიგრძის n-მიმდევრობების გენერაციის ზოგადი სქემა მოცემულია 2.2 ნახ-ზე [7].

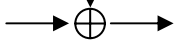


ნახ.2.2. $GF(2^m)$ ველში გამოთვლების განხორციელების ზოგადი სქემა.

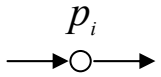
სქემა შედგება სამი სახის ელემენტებისაგან:



ორმდგომარეობიანი მეხსიერების ელემენტი;



გალუას ველში შეკრების ელემენტი (სუმატორი);



კავშირის ელემენტი.

სქემაში p_i ელექტრონული კავშირის არსებობა დამოკიდებულია $p(x) = p_0 + p_1 x + ... + p_m x^m$ პრიმიტიული მრავალწევრის p_i კოეფიციენტებზე ($p_i \in GF(2)$). თუ $p(x)$ მრავალწევრის კოეფიციენტი $p_i = 1$, მაშინ სქემაში შესაბამისი ელექტრული კავშირი არსებობს, თუ $p_i = 0$, მაშინ კავშირი არ გვაქვს (წრედი გათიშულია).

K_1 და K_2 სარქველი ჩაკეტილია რეგისტრში ინფორმაციის ჩაწერის პერიოდში და ღიაა გამოთვლების პერიოდში.

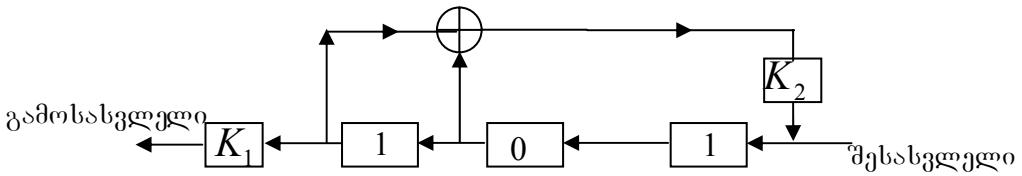
მაქსიმალური სიგრძის n-მიმდევრობა მიიღება მაშინ, როდესაც $p(x)$ მრავალწევრი წარმოადგენს დაუყვანადს და პრიმიტიულს $GF(2)$ ველში.

მაგალითი. $p(x) = 1 + x + x^3$ მრავალწევრი პრიმიტიულია და რეგისტრის გამოსასვლელზე მიიღება ფსევდოშემთხვევითი $n = 7$ სიგრძის ($n = 2^m - 1$, $m = \deg p(x)$, $n = 2^3 - 1$) ორობითი სიმბოლოების მიმდევრობა. $p(x) = 1 + x + x^3$ მრავალწევრის შესაბამისი რეგისტრი მოცემულია ნახ. 2.3-ზე.

n-მიმდევრობის მისაღებად საჭიროა რეგისტრში ჩაიწეროს m განზომილების გარკვეული ორობითი რიცხვი, ანუ $a = (a_1, ..., a_m)$ ($a_i \in GF(2)$) ვექტორი. მოცემული მაგალითისათვის რეგისტრში ჩავწერთ $c = (101)$ ვექტორს, მაშინ გამოსასვლელზე მივიღებთ $n = 7$ სიგრძის $a = 1011100$ მიმდევრობას, რომელიც პერიოდული მიმდევრობაა (რადგან

სატაქტო ოპერაციების გაგრძელების შემთხვევაში მოცემული მიმდევრობა გამეორდება).

პირველი ეტაპი ითვალისწინებს $a = (101)$ ინფორმაციის რეგისტრში ჩაწერას, რასაც დასჭირდება $m = 3$ ტაქტი. მოცემული ცხრილის მიხედვით (ნახ. 2.3, ცხრ.1) შემდგომი $n = 7$ ტაქტის განმავლობაში წანაცვლების რეგისტრი წარმოქმნის $a = 1011100$ მიმდევრობას.



ნახ. 2.3. $GF(2^m)$ ველში გამოთვლების განხორციელება კერძო მაგალითზე.

ტაქტის №	გამოსასვლელი a_i	რეგისტრის მდგომარეობა a ინფორმაციის ჩაწერის შემდეგ		
0		1	0	1
		რეგისტრის მდგომარეობა i-ური ტაქტის შემდეგ		
1	1	0	1	1
2	0	1	1	1
3	1	1	1	0
4	1	1	0	0
5	1	0	0	1
6	0	0	1	0
7	0	1	0	1

ცხრ.1. $GF(2^m)$ ველში გამოთვლების განხორციელება კერძო მაგალითზე

როგორც ვხედავთ, მე-7 ტაქტის შემდეგ რეგისტრის მდგომარეობა უბრუნდება საწყისს. ამიტომ, თუ სატაქტო ოპერაციებს გავაგრძელებთ, გამოსავალზე მივიღებთ იგივე 1011100 მიმდევრობას.

წანაცვლების რეგისტრით გენერირებული n-მიმდევრობა შეიძლება ჩაიწეროს რეკურენტული თანაფარდობის, ანუ სხვაობიანი განტოლებების მეშვეობით:

$$\sum_{j=0}^{m} p_j a_{i+j} = 0,$$

ანუ

$$a_{i+m} = -\sum_{j=0}^{m-1} p_j a_{i+j},$$

სადაც $p_0 = 1$, $p_m = 1$ და ნებისმიერი $p_j \in GF(2)$.

მაგალითი. $p(x) = 1 + x + x^3$ მრავალწევრისათვის $p_2 = 0$, $p_0 = p_1 = p_3 = 1$. დავუშვათ, რომ $a(x) = 1 + x^2$, $a = (101)$, მაშინ $a_0 = 1$, $a_1 = 0$, $a_2 = 1$ წარმოადგენენ საძიებელი მიმდევრობის პირველ სამ კომპონენტს. დანარჩენი კომპონენტები მიიღება შემდეგი განტოლებების მეშვეობით:

$$a_{0+3} = p_0 a_0 + p_1 a_1 + p_2 a_2$$
$$a_{1+3} = p_0 a_1 + p_1 a_2 + p_2 a_3$$
$$- - - - - - - - - - -$$

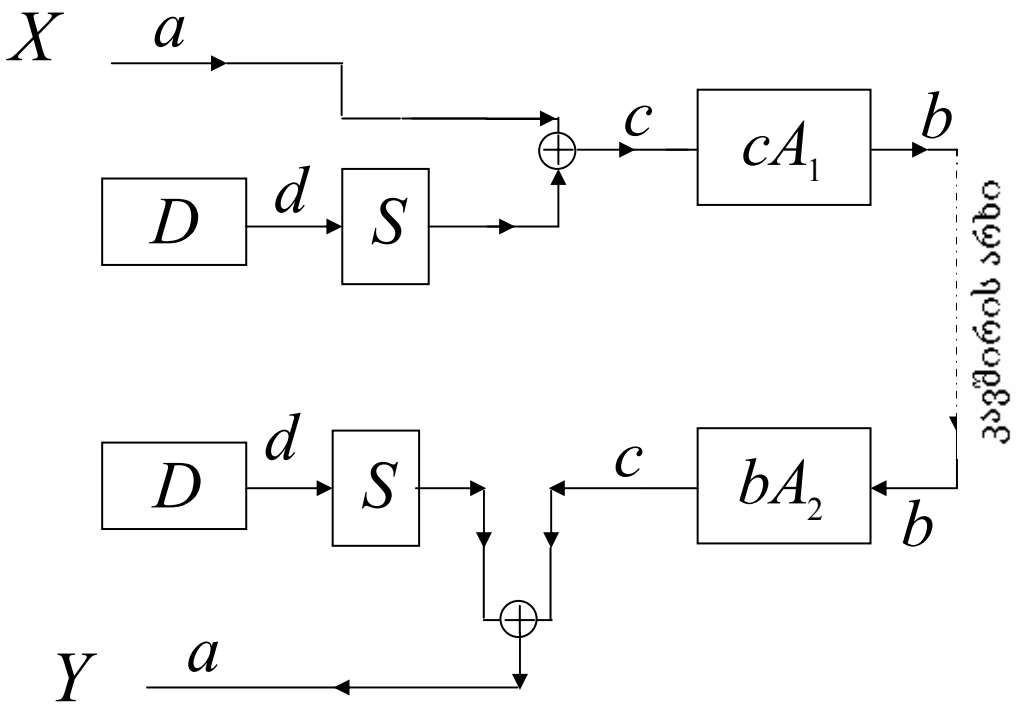
მოცემული პარამეტრებისათვის მიიღება შემდეგი მიმდევრობა:

$$a_0 = 1$$
$$a_1 = 0$$
$$a_2 = 1$$
$$a_3 = 1 \cdot 1 + 1 \cdot 0 + 0 \cdot 1 = 1$$
$$a_4 = 1 \cdot 0 + 1 \cdot 1 + 0 \cdot 1 = 1$$
$$a_5 = 1 \cdot 1 + 1 \cdot 1 + 0 \cdot 1 = 0$$
$$a_6 = 1 \cdot 1 + 1 \cdot 1 + 0 \cdot 0 = 0$$
$$a_7 = a_0 = 1 \cdot 1 + 1 \cdot 0 + 0 \cdot 0 = 1$$
$$a_8 = a_1 = 1 \cdot 0 + 1 \cdot 0 + 0 \cdot 1 = 0$$
$$a_9 = a_2 = 1 \cdot 0 + 1 \cdot 1 + 0 \cdot 0 = 1$$

$$a_{10} = a_3 = 1 \cdot 1 + 1 \cdot 0 + 0 \cdot 1 = 1$$
$$a_{11} = a_4 = 1 \cdot 0 + 1 \cdot 1 + 0 \cdot 1 = 1$$
$$a_{12} = a_5 = 1 \cdot 1 + 1 \cdot 1 + 0 \cdot 1 = 0$$
$$a_{13} = a_6 = 1 \cdot 1 + 1 \cdot 1 + 0 \cdot 0 = 0$$
$$----------$$

ე.ი. მიიღება მიმდევრობა $a = 1011100$, რომელიც $n = 7$ პერიოდით მეორდება და ემთხვევა წანაცვლების რეგისტრის მეშვეობით მიღებულ მიმდევრობას.

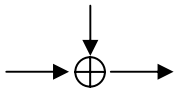
2.5. კომბინირებული სიმეტრიული კრიპტოსისტემა

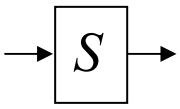


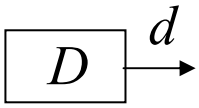
ნახ. 2.4. მატრიცული შიფრაცია-დეშიფრაციის კომბინირებული პროცესის სქემა

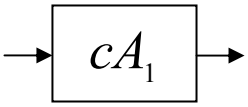
სქემა შედგება შემდეგი ელემენტებისაგან:

X, Y კანონიერი მომხმარებლებიი;

 გალუას ველში შეკრების ელემენტი (სუმატორი);

 სინქრონიზაციის ბლოკი;

 ფსევდოშემთხვევითი მიმდევრობების გენერატორი;

 ვექტორის ნამრავლი მატრიცზე.

განვიხილოთ ნახ. 2.4-ის შინაარსი.

X მომხმარებელი შეტყობინების a ვექტორს ქსორირებით დაუმატებს ფსევდოშემთხვევითი d მიმდევრობის (რომლის განზომილებაა $2^k - 1$) იმ მონაკვეთს, რომელიც შეთანხმებულია სინქრონიზატორში და მივიღებთ c ვექტორს. შემდეგ ეტაპზე ხდება c ვექტორის გამრავლება სპეციალურ A_1 მატრიცზე ($GF(p)$ ველზე მრავალწევრთა A_n ალგებრაში $\mathrm{mod}(x^n - 1)$ პრიმიტიული ელემენტით ნაწარმოები $g(x)$ მრავალწევრით აგებული A_1 მატრიცი), ე.ი. მოხდება შიფრაცია და მივიღებთ b შიფროტექსტს (ვექტორს). დაშიფრული b ტექსტი კავშირის არხით გადაეცემა Y მომხმარებელს.

Y მხარე b შიფროტექსტს გაამრავლებს A_2 მატრიცზე ($h(x) = (x^n - 1)/g(x)$ მრავალწევრით აგებულ მატრიცზე და $A_1 A_2 = 1$), ე.ი. ხდება დეშიფრაციის პირველი ეტაპი და ვღებულობთ c ვექტორს. შემდეგ c ვექტორს ემატება ფსევდოშემთხვევითი d მიმდევრობის ის მონაკვეთი, რომელიც წარმოქმნილი იყო გენერატორში და შეთანხმებული სინქრონიზატორში. დეშიფრაციის ამ მეორე ეტაპის შედეგად Y მხარე ღებულობს a შეტყობინებას (ღია ტექსტს).

აქ მნიშვნელოვანი არის ის, რომ ორივე მხარეს: X და Y-ს ერთიდაიგივე ფსევდოშემთხვევითი მიმდევრობის გენერატორი გააჩნიათ და, ამასთან, ორივე მხარეზე ხდება იმ მონაკვეთის სინქრონიზაცია*, რომელიც გამოიყენება XOR-სთვის. ე.ი. შესაძლებელია X მხარემ (ანუ გადაცემმა) მართოს ფსევდოშემთხვევითი გენერატორები და სინქრონიზატორები ორივე მხარეს.

უფრო დეტალურად ვაჩვენოთ, თუ როგორ მუშაობს ზემოთმოცემული კრიპტოსისტემა.

X მხარე აგენერირებს $g(x)$ მრავალწევრით A_1 მატრიცას, შესაბამისად Y მხარე კი- $h(x)$ მრავალწევრით A_2 მატრიცას ($A_1A_2=1$). X მხარე უგზავნის Y-ს მატრიცების აღრევის გასაღებს. ასევე უგზავნის ფსევდოშემთხვევითი მიმდევრობის შესახებ კოდურ ინფორმაციას, თუ რომელი მონაკვეთი გამოიყენება XOR-თვის.

ამ კრიპტომეთოდში გაცხადებულია (ღიაა):

- $g(x)$ და $h(x)$ მრავალწევრები, შესაბამისად ამ მრავალწევრებით აგებული A_1 და A_2 მატრიცები;
- ფსევდოშემთხვევითი მიმდევრობის გენერატორი და შესაბამისად, ფსევდოშემთხვევითი მიმდევრობის მაწარმოებელი $p(x)$ მრავალწევრი.

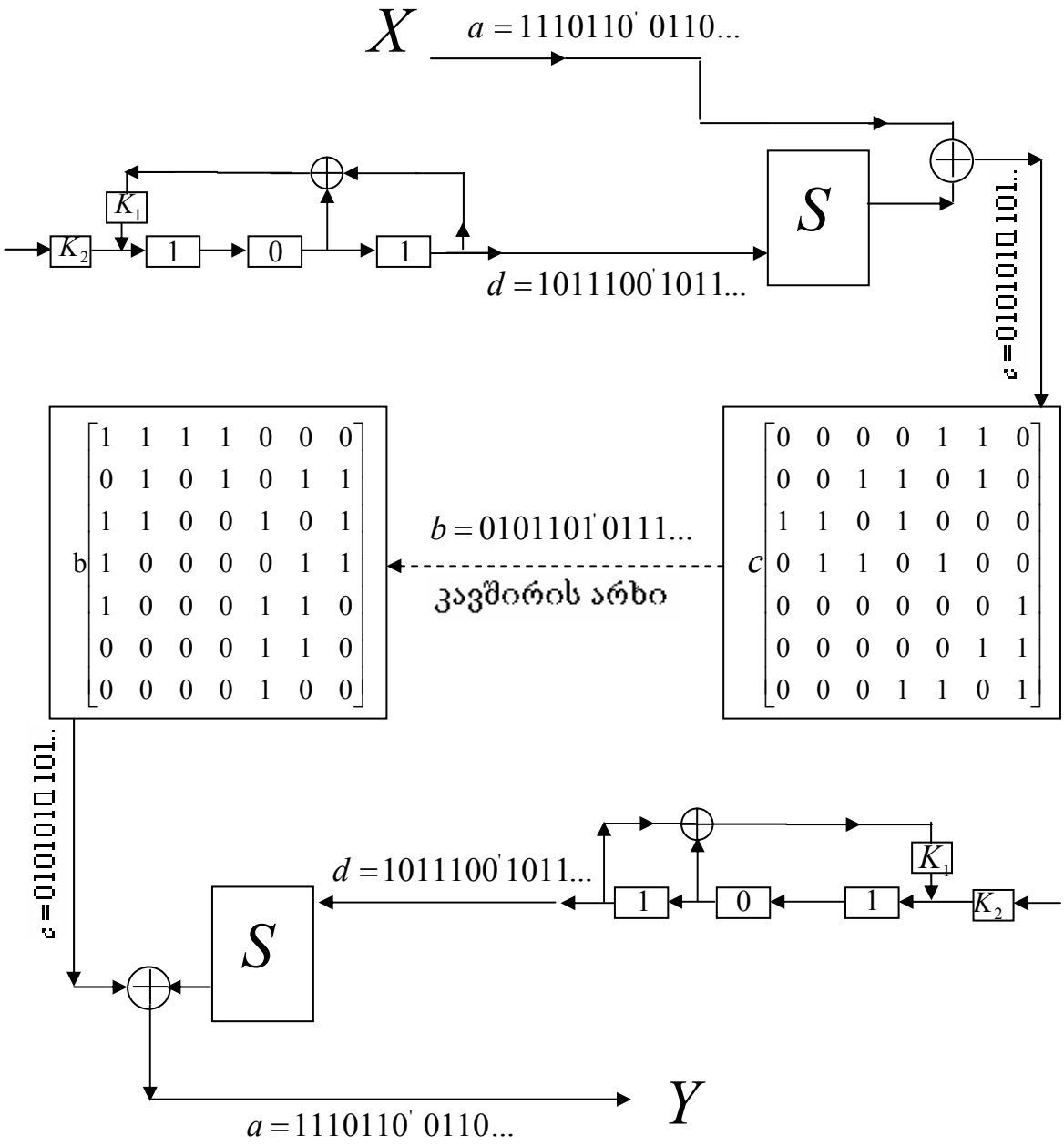
საიდუმლოა:

- მატრიცების აღრევის წესი, შესაბამისად A_1 მატრიცში- სტრიქონები (სვეტები), ხოლო A_2 მატრიცში- სვეტები (სტრიქონები) გასაღები);
- ფსევდოშემთხვევითი მიმდევრობების გენერატორის (რეგისტრის) საპროცედურო ინფორმაცია (გასაღები) ;
- ფსევდოშემთხვევითი მიმდევრობის ის მონაკვეთი, რომელიც გამოიყენება XOR-თვის (კოდური ინფორმაცია, ანუ- გასაღები).

მაგალითი. ნახ. 2.5-ზე განხილულია კერძო შემთვევა. თქვათ, X მხარე უგზავნის $a=1110110'0110...$ შეტყობინებას Y-ს.

* სინრონიზაციაში იგულისხმება ორივე გენერატორის შეთანხმება, მაგალითად იმპულსების ერთნაირი სიხშირე და იმპულსების ტაქტური პერიოდების თანხვედრა.

ფსევდოშემთხვევით გენერატორში დაგენერირდება მიმდევრობა $d = 10111001011...$, რომლის სიგრძეა $2^k - 1$, ანუ ამ კერძო შემთხვევაში $k = 3$.



ნახ.2.5. მატრიცული შიფრაცია-დეშიფრაციის კომბინირებული პროცესის კერძო შემთხვევა

X მხარე ირჩევს, თუ d მიმდევრობის რომელი მონაკვეთი გამოიყენოს XOR-თვის. ამ კერძო შემთხვევაში მიმდევრობის პირველი

ელემენტიდან იწყება ათვლა. შემდეგ ეტაპზე ხდება a და d შეკრება, ვღებულობთ $c = 01010101101...$ ვექტორს. c ვექტორი მრავლდება A_1^* მატრიცზე (ამ კეძო შემთხვევაში A_1^* და A_2^* აღრევის შედეგად მიღებული მატრიცებია) და ვღებულობთ შიფროტექსტს $b = 01011010111....$ შიფროტექსტი b გადაეცემა Y მხარეს კავშირის არხის მეშვეობით.

Y მხარე b შიფროტექსტს გაამრავლებს A_2^* მატრიცზე და მიიღებს c ვექტორს. c ვექტორს ემატება ფსევდოშემთხვევითი d მიმდევრობის ის მონაკვეთი რომელიც შეთანხმებულია წინასწარ (X წინასწარ უთანხმდება Y მხარეს გასაღებს). შეკრების შედეგად Y მხარე ღებულობს $a = 1110110'0110...$ შეტყობინებას (ღია ტექსტს).

შევნიშნოთ, რომ განხილულ შემთხვევაშიც, ისე როგორც საზოგადოდ, გამოიყენება სამი ტიპის გასაღები:

- მატრიცების აღრევის;
- ფსევდოშემთხვევითი მიმდევრობების გენერატორის საპროცედურო ინფორმაციის;
- ფსევდოშემთხვევითი მიმდევრობის მონაკვეთის შერჩევის.

განვიხილოთ ცალკეული მათგანი.

მატრიცების აღრევის გასაღები. როგორც ნახ. 2.5-დან ჩანს, A_1 და A_2 მატრიცებში განხორციელებული გარდაქმნა- სტრიქონების (სვეტების) გადანაცვლება ღებულობს შემდეგი ჩასმის სახეს:

$$t = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 0 & 5 & 4 \end{pmatrix}.$$

სიმარტივისათვის შეიძლება შევთანხმდეთ, რომ გასაღების მეშვეობით მივუთითოთ შესაბამისი გადანაცვლება, ანუ სტრიქონების (სვეტების) გადანაცვლების შედეგის ნომრები (ათობით სისტემაში): 2, 3, 1, 6, 0, 5, 4 ანუ, ორობითი ჩანაწერით, $011'100'010'111'001'110'101$. როგორ შეიძლება გასაღების ამ ინფორმაციის X მხარედან Y მხარეზე გადაცემა არა კურიერის მეშვეობით, არამედ ღია არხით, მაგალითად, დიფი-ჰელმანის

ალგორითმის გამოყენებით? ამისათვის წარმოვიდგინოთ, რომ დიფი-ჰელმანის ალგორითმით ფორმირებულია შემდეგი (გარკვეული) გასაღები: $K = 011'010'010'110'111'110'101'$. ეს ფსევდოშემთვევითი სიდიდე შეიძლება გამოვიყენოთ ჩვენი მიზნებისათვის და X და Y მხარეზე დავაფორმიროთ ერთიდაიგივე გასაღები. ამისათვის ვისარგებლოთ, ვთქვათ, შემდეგი ღია წესით (მაგრამ, ცხადია, არ უნდა დაგვავიწყდეს, რომ K გასაღები საიდუმლოა). გარდავქმნათ K გასაღები ყოველი ქვებლოკისათვის ერთის ტოლი რიცხვის დამატებით (ჩვენ შემთხვევაში $\mathrm{mod}\,7$ გათვალისწინებით) მხოლოდ იმ შემთხვევაში, თუ ადგილი აქვს ქვებლოკის რიცხვითი მნიშვნელობის გამეორებას და დავტოვოთ ყოველი მათგანი უცვლელად, როდესაც აღნიშნულის საჭიროება არ არის. მოცემული K გასაღებისათვის პირველი ორი ქვებლოკი დარჩება უცვლელი; ცვლილება შეეხება მესამე ქვებლოკს და ა.შ. შედეგად გასაღებს ექნება შემდეგი სახე: $K^* = 011'010'100'110'000'001'101'$, რაც შეესაბამება შემდეგ ჩასმას:

$$t^* = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 6 & 0 & 1 & 5 \end{pmatrix},$$

ანუ ათობით სისტემაში

$$K^* = 3,2,4,6,0,1,5$$

გასაღებს.

ფსევდოშემთხვევითი მიმდევრობების გენერატორის საპროცედურო ინფორმაციის გასაღები. ჩვენ კერძო შემთხვევაში ეს სიდიდე არის 101 რიცხვი. ამიტომ შეიძლება ითქვას, რომ ამ შემთხვევაში საკითხი გაცილებით მარტივია. K_2^* გასაღების მიღება სავსებით შესაძლებელია იმავე მეთოდოლოგიით, რომელიც ზემოთ იყო განხილული საჭირო გარდაქმნების გარეშე.

ფსევდოშემთხვევითი მიმდევრობის მონაკვეთის შერჩევის გასაღები. განხილულიი მაგალითი სიმარტივისათვის შერჩეულ იყო შემთხვევა,

როდესაც ფსევდოშემთხვევითი მიმდევრობა გამოყენებულია პირველი სიმბოლოდან. საზოგადოდ, შეიძლება ითქვას, რომ სატელეკომუნიკაციო სისტემებში ეს საკითხი კარგად არის შესწავლილი და აპრობირებული და სათანადო ბრძანების (ანუ სიგნალის) განხორციელება პრობლემას არ წარმოადგენს (ამიტომ აქ არ განიხილება).

2.6. ბლოკური სიმეტრიული კრიპტოსისტემების შედარებითი ანალიზი

მოვახდინოთ, დისერტაციაში მოცემული მატრიცული მეთოდის (რომელიც მიიღება ფსევდოშემთხვევითი მიმდევრობისა და ქსორირების პროცედურის ერთობლივად განხილვის შედეგად) სხვა ცნობილ კრიპტოსისტემებთან შედარება, მაგალითად, ისეთ ბრენდთან, როგორიცაა *DES* სტანდარტის *DEA* ალგორითმი.

DEA ალგორითმი ასიმეტრიულ ალგორითმთან შედარებით არის ბევრად უფრო სწრაფი, როგორც ზემოთაა აღნიშნული მიახლოებით 100-1000 ჯერ. მაგრამ არსებობს სიტუაცია, და შესაბამისად მომხმარებელი, რომელიც დაინტერესებულია უფრო სწრაფმქმედი შიფრაციის ალგორითმით, თუნდაც ამით ალგორითმის მედეგობა შედარებით ნაკლები იყოს იგივე *DES* სტანდარტის *DEA* ალგორითმზე. *DEA* ალგორითმით, როგორც აღვნიშნეთ, შიფრაცია ხდება 16 ეტაპად, რაც მოითხოვს გარკვეულ დროს (რასაკვირველია, დამოკიდებულია შეტყობინების სიდიდეზეც). დისერტაციაში მოცემული მატრიცული მეთოდი და ფსევდოშემთხვევითი მიმდევრობის ქსორირება მოითხოვს სულ ხუთ ეტაპს (რასაკვირველია როდესაც შეთანხმებულია მატრიცის სტრუქტურა და ფსევდოშემთვევითი მიმდევრობის გენერატორი):

I. ფსევდოშემთხვევითი მიმდევრობის გენერატორის გასაღების შერჩევა-შეთანხმება;

II. ფსევდოშემთხვევითი მიმდევრობის იმ მონაკვეთის შეთანხმება, რომელიც გამოიყენება ქსორირებისათვის;

III. შეთანხმებული ქსორის დამატება ღია ტექსტზე;

IV. შეთანხმებული მატრიცის აღრევა;

V. ქსორირებული შეტყობინების გამრავლება აღრეულ მატრიცზე.

ხუთივე ეს ეტაპი თანამედროვე ტექნოლოგიების გათვალისწინებით ძალიან სწრაფად რეალიზირდება. რასაკვირველია, შიფრაციის ყოველი სეანსის დროს, ხუთივე ეტაპი არ გამოიყენება. გასაღებების გაცვლა შესაძლებელია ან კურიერის მეშვეობით, ან (როგორც დისერტაციაში არის ნაჩვენები მათი გარკვეული მიზანშეწონილობა) ასიმეტრიული კრიპტოსისტემების გამოყენებით. მითუმეტეს, რომ გასაღებების ზომა უმნიშვნელოა (ეს არის მოკლე მონაკვეთი-შეტყობინება, ანუ ვექტორი); მისი გადაცემა და მიღება (ანუ გაცვლა) ხდება ძალიან სწრაფად თანამედროვე ტექნოლოგიური საშუალებების გათვალისწინებით.

დისერტაციაში მოცემული სიმეტრიული მეთოდით (მატრიცული მეთოდი პლიუს ფსევდოშემთხვევითი მიმდევრობით ქსორირება) შეიძლება დაინტერესებული იყოს ისეთი მომხმარებელი, რომელსაც ესაჭიროება მოკლე შეტყობინების ოპერაციების, - შიფრაცია-დეშიფრაციის, - ძალიან სწრაფად რეალიზება, ხოლო მედეგობა დროის მოკლე შუალედის მიხედვით, ვთქვათ, რამოდენიმე წუთიდან რამოდენიმე საათამდე. მაგალითისათვის შეგვიძლია მოვიყვანოთ ომის დროს საარტელერიო კორექტორის მიერ გადაცემული სამიზნეების კოორდინატები, რომლის საიდუმლოება მოკლე დროის შემდეგ კარგავს აქტუალურობას. ასევე, მაგალითად შეგვიძლია მოვიყვანოთ რეაგირებები საფონდო ბირჟაზე ბროკერების მიერ გადაცემულ ინფორმაციებზე, რომლის ფასი დროის მოკლე მონაკვეთში ხდება ნულის ტოლი და ა.შ.

მოკლედ, გამოვდივართ მომხმარებლის ინტერესებიდან ანუ სისტემა მისაღებია მათთვის, ვინც დაინტერესებულია მაღალი სისწრაფით და ამავე დროს იყენებს შედარებით მოკლე შეტყობინებებს, რაც, დავუშვათ, არ

აღემატება A4 ფორმატის ერთ გვერდს, რომელიც შეიცავს დაახლოებით 2000 ნაბეჭდ სიმბოლოს. იმ შემთხვევაში თუ გამოყენებულია ფსევდოშემთხვევითი მიმდევრობებით ქსორირება, მაშინ, ცხადია, მედეგობა (ანუ ნაბეჭდ სიმბოლოთა დასაშვები რაოდენობა) მნიშვნელოვნად გაიზრდება; ე.ი. მატრიცისათვის, რომლის ზომაა 100x100, თუ შეტყობინების განზომილება გადააჭარბებს ერთ გვერდს, მაშინ მოხდება შესაბამისი გასაღებების ცვლილებები (როგორიცაა მატრიცის აღრევის, ფსევდოშემთხვევითი მიმდევრობის ახალი მონაკვეთის შეთანხმებისა და ა.შ.).

თავი III

ციფრული ხელმოწერის ალტერნატიული ალგორითმების სინთეზი

3.1. ელგამალის ალგორითმი, როგორც ერთ-ერთი ძირითადი პროტოტიპი ცნობილი ალგორითმების მისაღებად; ამერიკული 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 [1, 4-6, 14, 38-39,42, 54, 60]. X მხარეზე მიიღება ე.წ. კონკატენაცია

$$|M||R||S| \tag{3.1}$$

სადაც R და S ორობითი სიტყვების 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-დასაიდუმლოება. ტექსტი ღიაა და ღიად უნდა დარჩეს, მაგრამ თუ ტექსტში გარეშე Z სუბიექტი შეიტანს ცვლილებას, იგი უნდა გამოაშკარავდეს Y მხარეზე შემოწმების შედეგად.

ალგორითმი ეფუძვნება დიფი-ჰელმანის ალგორითმით დაპატენტებულ ცნობილ ცალმხრივ ფუნქციას:

$$g^x \equiv y \pmod{p} \tag{3.2}$$

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

$$R \equiv g^K \pmod{p} \tag{3.3}$$

რიცხვის მნიშვნელობას; შემდეგ გამოთვლის S სიდიდეს შემდეგი გამოსახულებიდან:

$$M \equiv (xR + kS) \bmod (p-1) \tag{3.4}$$

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

$$M = H(M_0) \tag{3.5}$$

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:

$$g^M \equiv y^R R^S \pmod{p}. \tag{3.6}$$

(3.6) გამოსახულებით შესაძლებელია შემოწმდეს მიღებული შეტყობინება, რადგან:

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

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

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

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

$$\left|M_{01}\right|\left|R_1\right|\left|S_1\right|$$

შეტყობინებისთვის დაკმაყოფილდება 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: $\approx 10^{-30}$).

1991 წელს სტანდარტებისა და ტექნიკის ინსტიტუტის (NIST) მიერ შემუშავებულ იქნა ციფრული ხელმოწერის სტანდარტი - DSS (Digital Signature Standard). იგი შეიქმნა ციფრული ხელმოწერის ალგორითმის - DSA (Digital Signature Algorithm) მიხედვით, რომელიც არის ელგამალის ალგორითმის ბაზაზე დამუშავებული ალგორითმი.

DSA ალგორითმის სინთეზის ფორმულას აქვს შემდეგი სახე:

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

სადაც

$$r \equiv (g^k \bmod p) \bmod q.$$

შემოწმება ხორციელდება შემდეგი მიმდევრობით:

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

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

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

$$v \equiv ((g^{u_1} * y^{u_2}) \bmod p) \bmod q.$$

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 ციფრული ხელმოწერის ალგორითმი და შესაბამისი სტანდარტი.

3.2. ციფრული ხელმოწერის ალტერნატიული ალგორითმები

თავის ცნობილ ნაშრომში ბრიუს შნაიერი შენიშნავს, რომ დამატებითი ვარიანტებისა და განზოგადების შედეგად ციფრული ხელმოწერის სქემების რაოდენობამ შეიძლება შეადგინოს ცამეტ ათასზე მეტი (თუმცა მათგან ყველა ეფექტური არ იქნება) [1].

ციფრული ხელმოწერის ალგორითმების უმრავლესობა ეფუძნება გალუას $GF(p)$ ველებში დისკრეტული ლოგარითმების, ფესვის ამოღების, ფაქტორიზაციის პრობლემას და სხვა [3, 5, 6, 9, 14, 17].

სადისერტაციო ნაშრომში გამოკვლეულია ციფრული ხელმოწერის შესაძლო ვარიანტები, რომლებიც, აგრეთვე, იყენებს დისკრეტული ლოგარითმების პრობლემას (ანუ $g^x \equiv y \bmod p$ ცალმხრივ ფუნქციას). მათემატიკური საფუძვლების სივიწროვე, ცხადია, ართულებს ალტერნატიული 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 თვისებრიობა [4, 5, 6, 14, 38, 41, 52].

3.2.1. პირველი 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. 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:

$$M_1 \equiv (xR_1 + k_1 S_1) \bmod (p-1), \tag{3.7}$$

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 შემთვევითი 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:

$$M_2 \equiv (xR_1 + k_1 S_2) \bmod (p-1). \tag{3.8}$$

(3.7) და (3.8)-დან მიიღება:

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

საიდანაც განისაზღვრება

$$k_1 \equiv \frac{M_1 - M_2}{S_1 - S_2} \bmod (p-1) \tag{3.9}$$

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

განვიხილოთ სინთეზის (3.7) ფორმულის განსხვავებული, გამარტივებული ვარიანტი:

$$S \equiv (x + kM) \bmod (p-1). \tag{3.10}$$

შემოწმების ფორმულა შესაბამისად არის:

$$g^S \equiv yR^M \bmod p, \tag{3.11}$$

სადაც $y \equiv g^x \bmod p$ - ღია გასაღები, ხოლო $M = H(M_0)$ სიდიდისათვის საჭიროა დამატებითი პირობის შემოტანა, რომ ის ჰეშირების შემდეგ საჭიროების შემთხვევაში გარდაიქმნას ისე, რომ დაკმაყოფილდეს პირობა: $2|M$ (M სიდიდის ლუწობის პირობა, რაც მარტივად განხორციელდება). M სიდიდის ლუწობის პირობის შემოტანა დაიცავს ალგორითმს გატეხვისაგან. განვიხილოთ შემოწმების (3.11) ფორმულა. დავუშვათ, რომ მოცემული $M_\# = H(M_{0\#})$ ინფორმაციისათვის S პარამეტრი შევარჩიეთ, როგორც გარკვეული $S_\#$ სიდიდე და შევეცადოთ განვსაზღვროთ $R_\#$:

$$g^{S_\#} \equiv yR_\#^{M_\#} \bmod p. \tag{3.12}$$

(3.12) გამოსახულებაში $R_\#$ სიდიდის გარდა ყველა პარამეტრი ცნობილია. თუ $(M_\#, p-1) = 1$, რაც შესაძლებელია, მაშინ:

$$R_\# \equiv (y^{-1} g^{S_\#})^{M_\#^{-1}} \bmod p, \tag{3.13}$$

სადაც $M_\# M_\#^{-1} \equiv 1 \bmod (p-1)$. მაგრამ, თუ $M_\#$ ლუწი სიდიდეა, მაშინ $(M_\#, p-1) \neq 1$, $R_\#$ სიდიდის განსაზღვრა (3.12)-ე ფორმულიდან შეუძლებელია, რაც იმას ნიშნავს, რომ ალგორითმი ამ მეთოდით არ გატყდება და პროტოკოლით დაუშვებელი $|M_\| R_\| S_\#|$ კონკატენაციის ყალბი გზავნილი არ შედგება.

ჰეშირების შემდეგ M სიდიდისათვის ლუწობის პირობის შესრულება არ წარმოადგენს რთულ ოპერაციას, მაგრამ შესაძლებელია სინთეზის და შემოწმების ფორმულისათვის განხილული ალგორითმის შემდეგი ვარიანტიც:

$$S \equiv (x + 2km) \bmod (p-1), \tag{3.14}$$

$$g^S \equiv yR^{2M} \bmod p. \qquad (3.15)$$

განვიხილოთ ეს ვარიანტი. გატეხვის მცდელობამ სინთეზის (3.14) ფორმულის მიმართ შედეგი არ გამოიღო. რაც შეეხება შემოწმების (3.15) ფორმულას, (3.12) და (3.13) ფორმულების განხილვამ აჩვენა, რომ განხილული მეთოდით გატეხვის მცდელობა უშედეგო უნდა იყოს, რადგან $2M$ სიდიდე უპირობოდ ლუწია.

მაგალითი. ვთქვათ, $p=11$, $M=4$, $g=2$, $x=2$, $k=3$. აქედან

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

$$R = g^k \bmod p = 2^3 \bmod 11 = 8.$$

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

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

$S = (x + km) \bmod (p-1) = (2 + 3 \cdot 4) \bmod 10 = 14 \bmod 10 = 4$, ე.ი. $S = 4$.

კონკატენაციას აქვს სახე

$$\left|4\right\|8\left\|5\right| \quad (\left|M\right\|R\left\|S\right|).$$

განვიხილოთ შემოწმება:

$$g^S = g^{x+kM} \bmod p,$$

$$g^s = y \cdot R^M \bmod p,$$

$$2^4 = 4 \cdot 8^4 \bmod 11,$$

$$16 = 16384 \bmod 11,$$

$$5 = 5 \bmod 11,$$

ე.ი. შემოწმება სწორია.

3.2.2. მეორე ალგორითმის აგება

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

$$S = (x + kRM) \bmod q \qquad (3.16)$$

და

$$g^S \equiv yR^{RM} \bmod p. \tag{3.17}$$

ინფორმაციული გზავნილისა და ხელმოწერის კონკატენაცია ქმნის შემდეგ ჩანაწერს:

$$\left|M_0\right\|R\|S|, \tag{3.18}$$

სადაც $M \equiv H(M_0)$, M_0- გადაცემული ინფორმაციაა, რომელიც პროტოკოლით არის დაცული; $R \equiv g^k \bmod q$ და S- ხელმოწერების 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);

q - მარტივი რიცხვია, $p-1$ რიცვის მამრავლი, შედარებით ნაკლები, მაგრამ გარკვეული რიგისა;

g - ქვეჯგუფის გენერატორია, ნებისმიერი რიცხვია, რომელიც ($p-1$)- ზე ნაკლებია და რომლისათვისაც $g^q \bmod p \equiv 1$;

x - საიდუმლო გასაღებია, $0 < x < q$;

k_1 - ერთჯერადი შემთხვევითი საიდუმლო სიდიდე;

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

დასკვნა

სადისერტაციო ნაშრომის თემატიკა კრიპტოგრაფიული სისტემებია. ნაშრომში შეიძლება გამოვყოთ შემდეგი ძირითადი შედეგები:

1. მრავალწევრთა ალგებრასა და გალუას $GF(p^m)$ ველებზე დაყრდნობით მიღებულია პირდაპირ და შებრუნებულ $n \times n$ მატრიცათა გენერაციის ორიგინალური მეთოდი, რომელიც მარტივად რეალიზებადია ნებისმიერი მთელი n რიცხვისათვის $GF(p)$ ველზე.
2. მიღებულია მატრიცებისა და ფსევდოშემთხვევითი მიმდევრობის კომბინირებული გამოყენებით, რომელთა გენერირება შესაძლებელია $GF(p^m)$ ველს დაფუძნებული პროგრამული თუ წანაცვლების სქემებით მეშვეობით, მიღებულია შიფრაცია-დეშიფრაციის სიმეტრიული კრიპტოსისტემა.
3. გამოკვლეულია და მიღებულია ციფრული ხელმოწერის ახალი ალგორითმების ორი ვარიანტი. როგორც სხვა ცნობილი, აღიარებული სქემების შემთხვევაში, სადისერტაციო ნაშრომისთვისაც კვლევის ობიექტს (პროტოტიპს) წარმოადგენს ელგამალის ალგორითმი, რომლისთვისაც პარამეტრების გარკვეული ფუნქციონალური თვისებების გამოყენებით, მიიღება საჭირო სტრუქტურული ალტერნატივა.

ნაშრომი აპრობირებულია კონფერენციებზე [107,110] და გამოვეყნებულია სტატიებში [108-109, 111].

გამოყენებული ლიტერატურა

1. Shneier B. Applied cryptography. John Wiley and Sons. Inc. New York. 1996.

2. 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.

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

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 a signature scheme based on discrete logarithms. Advances in Cryptology: Proceedings of CRYPTO 84, Springer-Verlag, pp. 10-18, 1985.

6. Menezes A., Van Oorschot P. and Vanstone S. Handbook of applied cryptography. CRS Press, 1996. © 1997.

7. Peterson W.W. Encoding and error-correction procedures for the Bose-Choudhuri codes. IRE Trans. IT-6, 459-470, 1960 (თარგმ.: Питерсон У.У. Кодирование и справление ошибок для кодов Боуза-Чоудхури. Кибернетический сборник, вып. 6, М, ИЛ, 25-54, 1963.

8. Shannon C.E. A mathematical theory of communication. Bell System Tech. J., 27, n. 3, pp. 379-428; 27, n.4. pp. 623-656, 1948 (თარგმ.: Шеннон К. Работы по теории информации и кибернетике. М.: ИЛ, сс. 243-333, 1963).

9. Баричев С. В. Криптография без секретов. –М.: Наука, 1998.

10. Криптология – наука о тайнописи // Компьютерное обозрение. –1999. -№3. – С. 10 – 17.

11. Ростовцев А. Г., Михайлова Н. В. Методы криптоанализа классических шифров. –М.: Наука, 1995. –208 с.

12. Ростовцев А. Г. Решеточный криптоанализ // Безопасность информационных технологий, 1997. Вып. 2. С. 53–55.

13. Ростовцев А. Г. Метод обращения итерированной хэш-функции // Тезисы докладов конференции “Методы и технические средства обеспечения безопасности информации”. — СПб: Изд-во СПбГТУ, 2001.

14. Ростовцев А. Г., Маховенко Е. Б. Введение в криптографию с открытым ключом. — СПб.: Мир и Семья, 2001.

15. Ростовцев А. Г., Маховенко Е. Б. Практическое криптография. М., 2006.

16. Лидл Р., Нидеррайтср Г. Конечные ноля: Пер с англ. М.: Мир, 1988. Т. 1, 425 с., т. 2, 390 с.

17. ГОСТ Р 34.10-94. Государственный стандарт Российской Федерации. Криптографическая зашита информации. Процелуры выработки ипроверки электронной цифровой подписина базе асимметричного криптографического алгоритма. М.: Госстандарт СССР, 1989.

18. ГОСТ Р 34.11 -94. Государственный стандаре Российской Федерации. Криптографическая защита информации. Функция хеширования. М.: Госстандарт Россий, 1994.

19. RSA Laboratories. PKCS ffl: RSA Encryption Standard, version 2.0, Oct 1998.

20. Месси Дж. Введение в современную криптологию / ТИИЭР, т.76, №5.

21. Matsui M. Linear cryptanalysis method for DES cipher // Advances in Cryptology — EUROCRYPT ′93, LNCS, v. 765, 1994.

22. Coppersmith D., Odlyzko A. M., and Schroeppel R., "Discrete logarithms in GF(p)," Algorithmica, vol.1, pp. 1-16, 1986.

23. Andrew M. Odlyzko, «The future of integer factorization», AT&T Bell Laboratories, July 11, 1995.

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

25. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2002. 2-е изд.

26. Ван дер Варден Б.Л. Алгебра. М.: Наука, 1976.

27. Василенко *О.Н.* Некоторые алгоритмы построения больших простых чисел // Вестн. Моск. ун-та. Сер. 1. Матем. Механ. 1997. №5. С. 62—64.

28. Василенко О.Н. Современные способы проверки простоты чисел // Кибер. сборник, 1988. е. 25. с. 162-188.

29. Василенко О.Н. О дискретном логарифмировании в некоторых группах // Вестн. Моск. ун-та. Сер. 1. Матем. Механ. 2000. №5. С. 53—55.

30. Виноградов И.М. Основы теории чисел. М.: Наука, 1972.

31. Бухштаб А.А. Теория чисел. 2-е изд. М.: Просвещение, 1966.

32. Гантмахер Ф. Р. Теория матриц. М., 1954.

33. Галочкин А.И., Нестеренко Ю.В. Введение в теорию чисел. М.: Изд-во МГУ, 1995.

34. Григорьев Д.Ю. Разложение многочленов над конечным полем и решение систем алгебраических уравнений // Зап. науч. семин. ЛОМИ АН СССР. 1984. №137. С. 20–79.

35. Кострикин А.И. Введение в алгебру. М.: Наука, 1977.

36. Ленг С. Эллиптические функции. М.: Наука, 1984.

37. Прахар К. Распределение простых чисел. М.: Мир, 1967.

38. Саломаа А. Криптография с открытым ключом. М.: Мир, 1996.

39. Сидельников В.М., О системе шифрования, постпоенной на основе кодов Рида-Соломона, Дискретная математика, т. 4, вып. 3, стр. 57-63, 1992.

40. Сидельников В.М., Откпытое шифрование на основе двоичных кодов Рида-Соломона, Дискретная математика, т. 6, вып. 3, стр. 3-20, 1994.

41. Смарт Н. Криптография. М:Техносфера, 2005. 528 с.

42. Насыпный В.В. Одноразовое шифрование с открытым распределением ключей // Открытые системы, 2004, № 1, с.66-69.

43. Насыпный В.В. Защищенные стохастические системы // Открытые системы 2004, Я2 8, с. 60-61.

44. Нечаев В.И. Сложность дискретного логарифма // Научные труды МГПУ. 1994. С. 46–49.

45. Нечаев В.И. К вопросу о сложности детерминированного алгоритма для дискретного логарифма //Мат. заметки. 1994. Т. 55 (2).С. 91—101.

46. Чмора А.Л. Современная прикладная криптография. 2-е изд., стер. – М.: Гелиос АРВ, 2002.

47. Adleman L. The function field sieve // Proceedings of ANTS-I.1994. (Lect. Notes in Comput. Sci.; V. 877). P. 108—121.

48. Cohen H. A course in computational algebraic number theory.Springer-Verlag, 1993.

49. Coppersmith D. Fast evaluation of discrete logarithms in fields of characteristic two. IEEE Trans // Inform. Theory. 1984. V. 30 (4). P. 587—594.

50. Coppersmith D. Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm // Math. Comp. 1994. V. 62 (205).P. 333—350.

51. Coppersmith D., Winograd S. On the asymptotic complexity of matrix multiplication // SIAM J. Comput. 1982. V. 11. P. 472—492.

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

53. ElGamal T. On computing logarithm over finite fields // Advances in cryptology—CRYPTO’85 (Santa Barbara, Calif., 1985). 1986. (Lect. Notes in Comput. Sci.; V. 218). P. 396—402.

54. Koblitz N. A course in number theory and cryptography. Springer Verlag, 1987.

55. Koblitz N. Elliptic curve cryptosystems //Math. Comp. 1987. V. 48. P. 203—209.

56. Koblitz N. Algebraic aspects of cryptography. Springer-Verlag, 1998.

57. Трост Э. Простые числа. М.: ГИФМЛ, 1959.

58. Хассе Г. Простие числа. М.: ИЛ, 1953.

59. Введение в криптографию / Под общ. В.В. Ященко. 3-е изд., доп. М.: МЦНМО: "ЧеРо", 2000.

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

61. Ленстра Х. У. Алгоритмы проверки на простоту // Алгебра и теория чисел (с приложениями)Ж Сб. статей. М.: Мир, 1987. Вып.43.

62. Чистов А.Л. Алгоритм полиномиальной сложности для раз ложения многочленов и нахождения компонент многообразия в субэкспоненциальное время // Зап. науч. семин. ЛОМИ АН СССР. 1984. №137. С. 124—188.

63. Чебышев П.Л. Полное собрание сочинений. Т. 1. Теория чисел. Изд-во АН СССР, 1946.

64. Нечаев В.И. Элементы криптографии. М.: Высшая школа, 1999.

65. Чебышев П.Л. Полное собрание сочинений. Т. 1. Теория чисел. Изд-во АН СССР, 1946.

66. Лидл Р., Нидеррайтер Г. Конечные поля. Т. 1, 2. М.:Мир, 1988.

67. Гашков С. Б. Упрощенное обоснование вероятностного теста Миллера-Рабина для проверки простоты чисел // Дискретная математика. 1998. Т. 10 (4). С. 35—38.

68. Василенко О.Н. Применение круговых полей в криптосистемах RSA // IV Международная конференция «Современные проблемы теории чисел и ее приложения». Тула ,10-15 сентября, 2001 / Тезисы докладов. С 36—37.

69. Акритас А. Основы компьютерной алгебры с приложениями. М.: Мир, 1994.

70. Алексеев В. Б. Сложность умножения матриц. Обзор // Кибернетич. сборн. 1988. Вып. 25. С. 189—236.

71. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. М.: МИФИ, 1997.

72. Березин И.С., Жидков Н.П. Методы вычислений. Т. 1. М.: Наука, 1966.

73. Боревич З .И., Шафаревич И . Р. Теория чисел. М.: Наука, 1985.

74. Берлекэмп Э. Алгебраическая теория кодирования. М.: Мир, 1971.

75. Карацуба А.А., Офман Ю.П. Умножение многозначных чисел на автоматах // ДАН СССР. 1961. Т. 145 (2). С. 293—294.

76. Курош А.Г. Теория групп. М.: Наука, 1967.

77. Ленг С. Алгебра. М.: Мир, 1968.

78. Шор П. Полиномильные по времени алгоритмы разложения числа на простые множители и нахождения дискретного логарифма для квантового компьютера // Квантовый компьютер и квантовые вычислениюю Ижевск: ижевская республиканская типография, 1999. Т. 2. с. 200-247.

79. Verheul E.L., van Tilborg H.C.A. Cryptanalysis of “less-short” RSA secret exponents // AAECC, 1997.

80. Писсанецки С. Технология разреженных матриц. М.: Мир, 1988.

81. Buchman J., Williams H.C. A key-exchange system based on imaginary guadratic fields // Journal of Cryptology. 1988. Vol. 1. P. 107-118.

82. Gordon D. Discrete logarithms in $GF(p)$ using the number field sieve // SIAM Journal on Discrete Mathematics. 1993. Vol. 6. P. 124-138.

83. Fiat A., Shamir A. How to prove yourself: Practical solutions to identification and signature problems // Advances in Crytology- CRYPTO ’86 Lecture Notes in Coputer Science. Springer-Velag. 1987. Vol. 263. P. 186-194.

84. Rubin, Honeyman “Nonmonotonic cryptographic protocols”. Proc.Comp. Sec. Found. Workshop, VII, 1994.

85. Burrows, Abadi, Needham “A logic of authentication”. Report 39, Digital Systems Research Center, California, 1989.

86. Kessler, Wedel “ AUTLOG - An advanced logic of authentication” Proc.Comp.Sec.Found. Workshop, VII, 1994.

87. Жельников В.А. Криптография от папируса до компьютера. М., BF, 1997.

88. Романец Ю.Ф., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М., Радио и связь, 1999 г.

89. Ростовцев А. Г. Алгебраические основы криптографии. — Мир и Семья, СПб, 2000.

90. Баранов А. П., Борисенко Н. П., Зегжда П. Д., Корт С. С., Ростовцев А. Г. Математические методы защиты информации. — Военный институт правительственной связи. Орел, 1997.

91. Kelsey J., Schneier B., Wagner D. Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES // Advances in Cryptology — CRYPTO ′96, LNCS, v. 1109, Springer-Verlag, 1996, pp. 237–251.

92. Берлекэмп Э.П. Алгебраическая теория кодирования. М.: – Мир, 1971.

93. Блейхут Р. Теория и практика кодов, исправляющих ошибки. – М.: Мир, 1982.

94. Мак-Вильямс Ф.Дж., Слоэн Н.Дж. Теория кодов, испра-вляющих ошибки. – М.: Связь, 1979.

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

96. И.Л. Ерош, В.В. Скуратов. Адресная передача сообщений с использованием матриц над полем GF(2) / Проблемы информационной безопасности. Компьютерные системы. 2004, №1, с. 72-78.

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

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

99. Нечаев В.И. Сложность дискретного логарифма // Научные тру ды МГПУ. 1994. С. 46–49.

100. Сидельников В. М., Черепнев М. А., Ященко В. В., Системы открытого распределения ключей на основе некоммутативных полугрупп, Доклады РАН, 1993, т. 332, № 5.

101. Сидельников В. М. "Частные Ферма и логарифмирование в конечном простом поле", Международные научные чтения по аналитической теории чисел и приложениям, МГУ им. М. В. Ломоносова, 1997.

102. Березин Б. В., Дорошкевич П. В., "Цифровая подпись на основе традиционной криптографии", "Защита информации". - Москва, 1992, №2, с.148-167.

103. Shmuely Z., "Composite Diffie-Hellman public-key generating systems are hard to break," Computer Science Departmant, Technion, Haifa, Israel, Technical Rep. 356, Feb. 1985.

104. Davida G. I., "Chosen signature cryptanalysis of the RSA (MIT) public key cryptosystem," Tech. Rep. TR-82-2, Dept. of Electrical Engineering and Computer Science, Univ. of Wisconsin, Milwaukee, WI, Oct. 1982.

105. Pohlig S. C. and Hellman M.E., "An improved algorithm for computing logarithms in GF(p) and its cryptographic significance," IEEE Trans. Informat. Theory, vol. IT-24, pp.106-110, Jan. 1978.

106. Robshaw M.J., «Security Estimates for 512-bit RSA», RSA Laboratories, June 29, 1995.

107. მეგრელიშვილი რ., მეგრელიშვილი ე., მოსიძე თ., ჭელიძე მ. ახალი მატრიცული კრიპტოგრაფიული მეთოდი და მონაცემთა შიფრაციისა და დეშიფრაციის სისტემა. - საქ. მეცნ. აკადემია. ა. ელიაშვილის სახ. მართვის სისტ. ინსტიტუტი, კონფერ. მოხსენებათა კრებ. ”მართვისა ენერგეტიკის პრობლემები”, თბილისი, 2004, ტ. №8, გ. 181-184.

108. Megrelishvili R.P., Khutsishvili G.K. and Chelidze M.A. One method of construction of mutually inverse matrices over the Galois field and a new Cryptisystem.// Georgian Engineering news, Tbilisi, №2, 2006, p. 40-43.

109. Megrelishvili R.P., Chelidze M.A., Khutsishvili G.K., Megrelishvili E.R. Generalized Vandermonde Deteminants over Galois field $GF(q)$ and Classes of Optimal and Effective Error-Correcting Codes.// Bulletin of the Georgian national academy of sciences, 173, №3, 2006, p. 476-479.

110. მეგრელიშვილი რ., ჭელიძე მ., გნოლიძე თ. ელექტრონული ხელმოწერის ალტერნატიული ალგორითმის სინთეზის ამოცანისათვის. //სოხუმის უნივერსიტეტი, აკადემიური პერსონალის სამეც. კონფერენცია, 2008.

111. Мегрелишвили Р.П., Челидзе М.А., Гнолидзе Т. К задаче построение алтернативных алгоритмов цифровой подписи. // საქართველოს საინჟინრო სიახლენი, №3, 2008.