ივანე ჯავახიშვილის სახელობის თბილისის
სახელმწიფო უნივერსიტეტი

ლევანი ბუზალაძე

ახალი მატრიცული ცალმხრივი ფუნქციისა და ღია არხით გასაღების გაცვლის ალგორითმის ანალიზი და მისი ინოვაციური განხორციელება

საინფორმაციო სისტემები

სამაგისტრო ნაშრომი შესრულებულია საინფორმაციო სისტემების
მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

ხელმძღვანელი: რიჩარდ მეგრელიშვილი
ტექ. მეცნიერებათა დოქტორი, პროფესორი,
ზუსტ და საბუმებისმეტყველო მეცნიერებათა ფაკულტეტის
პროფესორი ემერიტუსი

თბილისი
2015

ანოტაცია

კრიპტოგრაფია ფართოდ გავრცელებული სამეცნიერი დარგია . მისი გამოყენების არეალი მოიცავს : სამხედრო , საბანკო , სახელმწიფო , ინტერნეტს და სხვა მრავალს ისეთ სფეროს , რომელთა გარეშეც წარმოუდგენელია დღევანდელი ადამიანის ცხოვრება . ინტერნეტის ფართო გავრცელებამ განავითარა ახალი სერვისები (ინტერნეტ ბანკი , ინტერნეტ მაღაზია , სოციალური ქსელები და სხვა), ამ ყველაფრის ფონზე მონაცემების დაცვა გახდა მნიშვნელოვანი არა მარტო სახელმწიფო , როგორც ეს იყო ადრინდელ წლებში, არამედ თითოული ადამიანის უსაფრთხოების დონეზე.

ინფორმაციის დაცვას უდიდესი ყურადღება ექცევა მსოფლიოში. ყველა წამყვან სახელმწიფოში ფუნქციონირებს სპეციალური სამსახურები, რომელთა ძირითადი მიმართულება კიბერდანაშაულთან ბრძოლა და კიბერშეტევისგან თავდაცვაა. ასევე მიმდიონარებს კვლევები ახალი თავდაცვითი მეთოდების შესახებ. ტარდება კონფერენციები , იბეჭდება სტატიები და ამ ყველაფერს ერთი მთავარი დანიშნულება აქვს : მოახდინოს ადამიანის უსაფრთხოების უზრუნველყოფა .

ცხადია ყველაფერი ზემოთაღნიშნული წარმოუდგენელია კრიპტოგრაფიის გარეშე. ამის ერთ-ერთ მაგალთად ციფრული ხელმოწერა შეგვიძლი მივიჩნიოთ, რომელიც უზრუნველყოფს ინფორმაციის გამგზავნის ზუსტ აუტენტიფიკაციას. თუმცა კრიპტოგრაფია მხოლოდ ციფრული ხელმოწერა არაა, ის აერთიანებს უამრავ მეთოდს , რომლებიც უზრუნველყოფენ ინფორმაციის უსაფრთხოებას.

თანამედროვეობამდე კრიპტოგრაფიამ დიდი გზა გაიარა , მოხდა უამრავი ალგორითმის აღმოჩენა , გამოკვლევა და პრაქტიკაში გამოყენება. თუმცა დრომ კრიპტოსისტემები ორ ძირითად ჯგუფში გააერთიანა , ესენია : სიმეტრიული და ასიმეტრიული კრიპტოსისტემები. მათ შორის ძირითადი განსხვავება გასაღებების გადაცემის მეთოდოლოგიაშია . სიმეტრიული კრიპტოსისტემა გასაღების გადასაცემად იყენებს დახურულ არხს, ხოლო ასიმეტრიული კი ღია არხით ახოციელებს იგივეს . ასევე აღსანიშნავია , რომ ასიმეტრიული კრიპტოსისტემები ,

მიუხედავად მათი საიმედოობისა , მოიხმარენ უფრო მეტ დროს , ვიდრე სიმეტრიული სისტემები. ეს არის სწორედ თანამედოვე კრიპტოგრაფიის ამჯამინდელი გამოწვევა , შექმნას ისეთი ალგორითმი , რომლებიც შესრულებისას მოიხმარს მაქსიმალურად მცირე დროს , რათა მან საიმედოობასთან ერთად , დროის თვალსაზრისითაც გაუწიოს კონკურენცია სიმეტრიულ კრიპტოსისტემებს.

წინამდებარე ნაშრომი სწორედ აღნიშნული პრობლემის გადაჭრისკენ წინ გადადგმულ ნაბიჯს წარმოადგენს , გვთავაზობს რა ახალი , მატრიცული , სწრაფქმედი ცალმხრივი ფუნქციისა და ღია არხით გასაღებების გაცვლის ალგორითმის კვლევას, რომელიც პირველად მიღებული და გამოკვლეული იყო ნაშრომის ხელმძღვანელის ტექნ. მექნიერებათა დოქტორის, პროფესორ ემერიტუსის რ. მეგრელიშვილის მიერ 2006 წელს.

უნდა აღინიშნოს , რომ ზოგადად ასიმეტრიული კრიპტოსისტემების ძირითადი საფუძველი არის ცალმხრივი ფუნქცია და არც აღნიშნული ალგორითმია გამონაკლისი. ცალმხრივი ფუნქცია ეწოდება ისეთ ფუნქციას , რომლის დროსაც მისი მნიშვნელობის გამოთვლა ძალიან ადვილია, თუ ვიცით არგუმენტის მნიშვნელობა , თუმცა ფუნქციის მნიშვნელობიდან არგუმენტის გამოთვლა რეალურ დროში შეუძლებელია.

ერთერთი ყველაზე ცნობილი ასიმეტრიული სისტემა არის დიფი - ჰელმანის ალგორითმით აგებული კრიპტოგრაფიული სისტემა. დიფმა და ჰელმანმაც , თავიანთი ალგორითმის შესაქმნელად ცალმხრივი ფუნქცია გამოიყენეს , რომელსაც შემდეგი სახე ჰქონდა :

$$c = a^x (\mathrm{mod}\ p)$$

ბატონი რიჩარდ მეგრელიშვილის მიერ აღმოჩენილი ცალმხრივი ფუნქცია კი ეფუძნება ვექტორის მატრიცზე ნამრავლს :

$$u = v * A$$

სადაც v არის ვექტორი , ხოლო A წარმოადგენს მატრიცს.

ნაშრომში განხილული და გამოკვლეულია სწორედ აღნიშნულ მატრიცულ ფუნქციაზე დაფუძნებული ღია არხით გასაღებების გაცვლის ალგორითმი , რომელიც

გარკვეულწილად დიფი-ჰელმანის ალგორითმის ანალოგიურია. აღნიშნული ალგორითმით გასაღებების გამოთვლა შემდეგნაირად ხდება :

I პიროვნება ირჩევს კერძო გასაღებს A_1 - ს , ამრავლებს მასზე v ვექტორს და უგზავნის II პიროვნებას:

$$I \rightarrow II : \quad u_1 = v^*A_1$$

II პიროვნება მიღებული ინფორმაციისა და თავისი კერძო გასაღების საფუძველზე გამოთვლის k_1 - ს:

$$II : \quad k_1 = u_1^*A_2 = v^*A_1^*A_2$$

II პიროვნება ირჩევს კერძო გასაღებს A_2 - ს , ამრავლებს მასზე v ვექტორს და უგზავნის I პიროვნებას:

$$II \rightarrow I : \quad u_2 = v^*A_1$$

I პიროვნება მიღებული ინფორმაციისა და თავისი კერძო გასაღების საფუძველზე გამოთვლის k_2 - ს:

$$I : \quad k_2 = u_2^*A_1 = v^*A_2^*A_1$$

საბოლოოდ k_1 და k_2 უნდა იყვნენ ტოლები , თუმცა

$k_1 = v^*A_1^*A_2$

$k_2 = v^*A_2^*A_1$

გასაღებების ტოლობისთვის საჭიროა, რომ I და II პიროვნებების მიერ არჩეული კერძო გასაღებები (მატრიცები) იყვნენ კომუტაციურები. აღნიშნული პრობლემა გადაწყვეტილია როგორც უკრაინელი მეცნიერის ბელიცკის და ქართველი დოქტორანტს სოფო შენგელიას ასევე აწ უკვე მაგისტრის ლიანა კლოიანის მიერ , მათ ააგეს კომუტატიურ მატრიცთა კლასი , რომლიდანაც ვიღებთ კიდეც ჩვენთვის საჭირო მატრიცებს. აღსანიშნავია , რომ მათი მეთოდები არის განსხვავებული.

კვლევის ძირითად მიზანს პირველ რიგში წარმოადგენს ახალი , ცალმხრივი მატრიცული ფუნქციის წარმოდგენა , მისი გამოყენება კრიპტოგრაფიულ ალგორითმში და ამ ალგორითმის საფუძველზე პირველი , ინოვაციური პროდუქტის შექმნა . ასევე ჩვენი მიზანია მივაკვლიოთ იმ მეთოდებს , რომლებიც საშუალებას მოგვცემს მაქსიმალურად გავაუმჯობესოთ ახალი ალგორითმის მიერ გასაღებების გამოთვლისთვის საჭირო დრო .

Abstract

Cryptography is widely spread scientific field in the world. It is used in many different areas: military, monetary, governmental, internet services and many different fields. Nowadays without cryptography we can barely imagine human life. Along with development of internet it opened doors to plenty of new services (internet banking, internet shopping, social networks and etc.), to take into the consideration above stated, protection of data became one of the most important not only on governmental level, but as individual humanity level as well.

Protection of the information is one of the essential subject in the universe. There are many specific services whose main objectives are fight against cybercrimes and protection against cyber-attack. At the same time recent surveys are going on regarding the new methodologies of cyber-protection. Plethora of scientific conferences holds, many of newspaper and online articles are published out that aims to improve level of human protection.

It is obvious that all of this is unimaginable without the cryptography. One of the good examples is Digital Signature, which provides exact Authenticity of sender's information. Besides digital signature cryptography unifies myriads of methods, which provides protection of information.

Modern cryptography took long way till today, lots of algorithms were found out, researched and used in practice. During this period cryptosystems were divided into two major groups: symmetrical and asymmetrical cryptosystems. The difference between those two groups is in methodology of exchange of keys. Symmetrical cryptosystems in order to exchange key uses protected channel, while asymmetrical cryptosystems uses public channel for exchange of keys. It is worth to mention that the asymmetrical cryptosystems, despite of its reliability, they consume much more time rather than symmetrical cryptosystems. It appears that main challenge of the modern cryptography is to create such an algorithms which will consume as short period of time as possible to compete with symmetrical cryptosystems.

Our scientific research is step up in the way of the solving this problem, which offers us a new qucick, one-way matrix function and research of algorithm with public key exchange. This algorithm first was discovered and researched by mentor of the paper: Doctor of Technical Sciences, Professor Emeritus Richard Megrelishvili in 2006.

Generally one-way functions are major basis of asymmetrical cryptosystems and above mentioned algorithm as well, as it is part of the asymmetrical cryptosystems. One-way function is a function where we can easily calculate its outcome but if we know only outcome, it is impossible to calculate its argument in the real time.

One of the most famous asymmetrical system in the work is Diffie-Hellman algorithm. Diffie and Hellman used one-way function for creating their own algorithm, this function looked like:

$c = a^x \pmod p$

One of the one-way functions was discovered and researched by professor Megrelisvhili which looked like:

$u=v * A$

Where v is a vector and A is matrix.

In the research we reviewed and examined the public key exchange algorithm which is based on matrix one-way function. That algorithms is somehow analogical to Diffie-Hellman algorithm. Calculate of public keys by above mentioned algorithm will be in this way:

I person will chose his private key (A_1), multiplies it to vector (v) and sends result to II person:

$I \rightarrow II : \quad u_1 = v^*A_1$

II person with received result and his own private key (A_2) calculates first public key (K_1):

$II : \quad K_1 = u_1^*A_2 = v^*A_1^*A_2$

II person will chose his private key (A_2), multiplies it to vector (v) and sends result to I person:

$II \rightarrow I : \quad u_2 = v^*A_1$

I person with received result and his own private key (A_1) calculates first public key (K_2):

$I : \quad K_2 = u_2^*A_1 = v^*A_2^*A_1$

Finally both public keys must be equal, nevertheless:

$$K_1 = v^*A_1^*A_2$$

$$K_2 = v^*A_2^*A_1$$

In order to achieve equalities of both public keys, matrixes which are chosen as private key by Person I and Person II must be commutative. This problem was already solved out by Ukrainian scientist Belitsky, Georgian PHD candidate Sofo Shengelia and also by MA Liana Kloian. They built commutative matrix class, from which we gain useful matrixes for us. Must be mentioned that their methodologies are different.

Main goal of our research is to represent new one-way matrix function, its role in cryptographic algorithm and create first, innovative product on bases of this algorithm. In addition our objective is to discover methods which will allow us to improve time which is consumed by this algorithm for calculate public keys.

სარჩევი

შესავალი

თემის აქტუალობა: კრიპტოგრაფია ერთ-ერთი უძველესი მეცნიერებაა რომელიც ინფორმაციის შიფრაციას (ღია ინფორმაციის დახურულად გარდაქმნა) და დეშიფრაციას (დახურული ინფორმაციის ღიად გარდაქმნა) შეისწავლის . მისი ისტორიის საწყისად ქრისტეს შობამდე 36 - ე საუკუნე შეგვიძლია მივიჩნიოთ, როდესაც წარმოიშვა როგორც შუმერების ლურსმული დამწერლობა, ასევე ეგვიპტური იეროგლიფები. მას მერე დიდმა დრომ განვლო , ჩამოყალიბდა ანბანური დამწერლობა , რომელმაც ახალი კრიპტოგრაფიული მეთოდები გამოკვეთა. დროის მსვლელობასთან ერთად განვითარდა ქვეყნები , განვითარდა პოლიტიკა და სხვა ბევრი ისეთი დარგი , რომელთა სწორედ წარმართვა კრიპტოგრაფიის გარეშე წარმოუდგენლად მიიჩნევა.

ამიტომ მთელ მსოფლიოში შეიცვალა ინტერესი კრიპტოგრაფიისადმი. გაფართოვდა კრიპტოგრაფიული მეთოდების გამოყენების სფერო ინტელექტუალური საკუთრების დასაცავად. გაიზარდა მოთხოვნა ინფორმაციის დაცვის პროდუქტებზე, განსაკუთრებით ინტერნეტ-აპლიკაციებში. კრიპტოგრაფიის აქტუალობა საკმაოდ მაღალია, რადგან ინფორმაციული საზოგადოების პირობებში საკუთარი მონაცემების დაცვა სჭირდებათ არა მარტო სპეცსამსახურებს და მსხვილ კომერციულ ფირმებს, არამედ ერთეულოვან მომხმარებლებსაც. ზემოდ თქმულიდან გამომდინარე ჩანს, რომ თემის აქტუალობა საკმაოდ მაღალია.

დღევანდელი კრიპტოგრაფია მკვეთრად განსხვავდება უძველესისგან, არსებობს უამრავი განსხვავებული ალგორითმი , თუმცა ყველას თავისი ადგილი აქვს დღევანდელ კრიპტოგრაფიულ სამყაროში. კრიპტოგრაფიული სისტემა ყოველთვის გულისხმობს 2 ან მეტ მონაწილეს, „გამგზავნს“ და „მიმღებს“, რომელთაც სურთ ერთმანეთს გადასცენ რაიმე სახის ინფორმაცია, ისე რომ ამ სისტემის გარეშე პირმა ვერ შეძლოს ამ ინფორმაციის მოპოვება.

- **შიფრაცია** - ინფორმაციის სახეცვლილება ისე, რომ დაფარულ იქნას მისი აზრი.
- **დეშიფრაცია** - შიფრაციის უკუპროცესი
- **შიფროტექსტ** - შიფრაციის განხორციელების შემდეგ მიღებული შედეგი

- **გასაღები** - საიდუმლო პარამეტრი რომელიც ცნობილია მხოლოდ ურთიერთმოკავშირე მხარეებისთვის და რომლის საშუალებითაც ხდება შიფრაცია და დეშიფრაცია.

თანამედროვე კრიპტოგრაფია შეიცავს **სიმეტრიულ** და **ასიმეტრიულ** კრიპტოსისტემებს.

სიმეტრიული კრიპტოგრაფია : წარმოადგენს კრიპტოსისტემას, რომლის დროსაც გამოიყენება ორი არხი : **ღია არხი** - დაშიფრული ინფორმაციის გადასაცემად და **დახურული არხი** - გასაღების გადასაცემად.

ასიმეტრიული კრიპტოგრაფია : წარმოადგენს კრიპტოსისტემას, რომლის დროსაც გამოიყენება **მხოლოდ ღია არხი** , რისი საშუალებითაც ხდება როგორც დაშიფრული ტექსტის , ასევე გასაღების გადაცემა. თუმცა უნდა აღინიშნოს , რომ სიმეტრიულიგან განსხვავებით , ასიმეტრიულ კრიპტოსისტემაში მონაწილეობს გასაღებების წყვილი , პირადი (საიდუმლო) და საერთო გასაღები.

სიმეტრიული და ასიმეტრიული კრიპტოსისტემები ასევე სისწრაფითაც განსხვავდებიან . მიუხედავად ასიმეტრიული კრიპტოსისტემების უფრო მეტად სანდოობისა , ისინი ბევრად ჩამოუვარდებიან სისწრაფით სიმეტრიულ კრიპტოსისტემებს (როგორც ბრიუს შნაიერი ამბობს სიმეტრიული ალგორითმები 100ჯერ და 1000ჯერ უფრო სწრაფები არიან ასიმეტრიულზე).

წინამდებარე ნაშრომში განხილული მატრიცული ცალმხრივი ფუნქცია და შესაბამისი გასაღების გაცვლის მატრიცული ალგორითმი პირველად მიღებული და გამოკვლეული იყო ნაშრომის ხელმძღვანელის ტექნ. მექნიერებათა დოქტორის, პროფესორ რ. მეგრელიშვილის მიერ.

გასაღების სწრაფი გაცვლის ამოცანა კრიპტოგრაფიაში (სამაგისტრო თემის გაშინაარსება). ზემოდ აღნიშნული ძირითადი პრობლემები დაკავშირებულია ცალმხრივი ფუნქციის თვისებებთან და გასაღების ღია არხით გაცვლის ამოცანასთან. ყოველი კრიპტოგრაფიული სისტემა იყენებს საკუთარ პროცედურას, გასაღებების ტიპს, მათი განაწილების მეთოდოლოგიას და შიფრაციის ალგორითმებს. ასიმეტრიული კრიპტოგრაფიის საფუძველს წარმოადგენს ცალმხრივი ფუნქციის

სპეციფიურობა. ცალმხრივი ფუნქცია - ისეთი f(x) ფუნქცია, რომლის მნიშვნელობის პოვნა ძალიან ადვილია თუ ცნობილია x, მაშინ როცა x - ის მნიშვნელობის პოვნა f(x) - ის მნიშვნელობის ცოდნის დროს შეუძლებელია რეალური დროის განმავლობაში.

ცალმხრივი ფუნქციები გამოიყენება დიფი - ჰელმანისა და RSA ალგორითმებში.

აღნიშნული ახალი ასიმეტრიული ალგორითმი უდაოდ წინ გადაგმული ნაბიჯია კრიტოგრაფიის ისტორიაში. იყენებს რა ახალ მატრიცულ , ცალმხრივ ფუნქციას გასაღებების გაცვლისათვის . მას ასევე აქვს პრეტენზია , რომ ამ ალგორითმის საშუალებით გასაღებების გენერირება მოხდება უფრო სწრაფად, ვიდრე ამას აკეთებენ აქამდე არსებული ასიმეტრიული ალგორითმები.

სადიპლომო ნაშრომში აღწერილი ორიგინალური მატრიცული ალგორითმი გარკვეულწილად დიფი – ჰელმანის ღია არხით გასაღების გაცვლის ალგორითმის ანალოგიური მოდელია. მაშინ როცა დიფი - ჰელმანის ალოგორითმის სიმტკიცე დამოკიდებულია p მარტივი რიცხვის დიდ მნიშვნელობებზე (ანუ დისკრეტული ლოგარითმის პრობლემაზე), ასევე მატრიცული ცალმხრივი ფუნქციის სიმტკიცეც დამოკიდებულია *A* სიმრავლის მაღალ სიმძლავრეზე. ამის გარდა, ცალმხრივი მატრიცული ფუნქციის სიმტკიცე დამოკიდებულია მატრიცის შიდა რეკურსიის არსებობის პრობლემაზე. აქვე ავღნიშნოთ, რომ შიდა რეკურსია არის დამოკიდებულება მატრიცის სტრიქონებს შორის. ეს არ არის ვექტორებს შორის წრფივი დამოკიდებულება, რადგან ასეთ შემთხვევაში მატრიცები იქნებოდნენ გადაგვარებულნი.

ზემოდ აღნიშნულიდან გამომდინარე, სამაგისტრო ნაშრომში გამოკვლეულია ახალი მატრიცული ფუნქცია და მის საფუძველზე შედგენილი ახალი ალგორითმი , მისი თვისებები და რეალიზაციის მეთოდები.

კვლევის პერიოდში განვიხილით სხვადასხვა მეთოდები ახალი კრიპტოგრაფიული ალგორითმის შედეგის გასაუმჯობესებლად. შევისწავლეთ და განვიხილეთ პრობლემის როგორც სქემური , ასევე პროგრამული გადაწყვეტის რამოდენიმე მეთოდი. შევჯერდით რა საბოლოოდ პოგრამულ რეალიზაციაზე

(რომელიც წარმოადგენს აღნიშნულ ალგორითმზე დაფუძნებული პროდუქტის შექმნის პირველ , ინოვაციურ პრეცენდენტს) , მივაკვლიეთ და განვიხილეთ რამოდენიმე ალგორითმი , რათა მიგვეღო მაქსიმალურად საუკეთესო შედეგი. ამისათვის საჭირო იყო მიგვეკვლია ისეთი მეთოდებისთვის , რომლებიც ვექტორის მატრიცზე ნამრავლს მაქსიმალურად სწრაფად შეასრულებდა. კვლევის პერიოდში განვიხილეთ გადამრავლების კლასიკური მეთოდი , მრავალ-ნაკადური მეთოდი , შტრასენის ალგორითმი , სხვადასხვა პროგრამული ბიბლიოთეკები , თუმცა საბოლოოდ შევჯერდით „ოთხი რუსის ალგორითმზე“ , რომელმაც ამ ეტაპზე მოგვცა საუკეთესო შედეგი . ამასთან ერთად მოძიებული იქნა დიფი-ჰელმანის რეალიზაციისთვის ამ დროისათვის არსებული საუკეთესო მეთოდი, რომელიც აღწერილი იყო ერთ-ერთი ფართოდ გავრცელებულ პროგრამულ ბიბლიოთეკაში , რომელიც მაქსიმალურად სწრაფად ახორციელებს დიფი-ჰელმანის ალგორითმისთვის საჭირო გამოთვლებს .

აღნიშნული მეთოდების პროგრამული რეალიზაციისას გამოყენების შედეგად მივიღეთ , რომ ახალი მატრიცული ალგორითმი გასაღებების გამოთვლას ახორციელებს საშუალოდ დაახლოებით 0,000006 წამში , ეს შედეგი დაახლოებით ოცჯერ სწრაფია დიფი-ჰელმანის ალგორითთან შედარებით , რომელიც გასაღებების გამოთვლას საშუალოდ 0.0001146 წამს ანდომებს.

წინამდებარე ნაშრომში მოყვანილია მიღებული შედეგისკენ მიმავალი გზები. პირველ თავში მოყვანილია კრიპტოგრაფიის განვითარების ქრონოლოგია, გამოყოფილია საკვანძო თარიღები და დაწვრილებით აღწერილია ის მოვლენები, რომელთაც გარდატეხა შეიტანეს კრიპტოგრაფიის განვითარებაში. მეორე თავში მოყვანილია დიფი-ჰელმანის ალგორითმი, მისი მუშაობის პრინციპი და დღეისათვის ერთ-ერთი საუკეთესო რეალიზაციის მეთოდის განხილვა. ასევე აღწერილია ახალი ცანხრივი ფუქნცია, მასზე დაფუძნებული მატრიცული ალგორითმი , მოყვანილია და განხილულია მისი რეალიზაციის მეთოდები და არგუმეტირებულია ის ფაქტი , თუ რატომ და როგორ პასუხობს ის დღეისათვის აქტუალურ პრობლემას, კერძოდ სწრაფქმედი ასიმეტრიული ალგორითმების შექმნას.

თავი I

კრიპტოგრაფიის განვითარების ქრონოლოგია

კრიპტოგრაფია უძველესი მეცნიერებაა , შეგვიძლია მივიჩნიოთ, რომ იგი შეიქმნა დამწერლობასთან ერთად . შექმნის შემდეგ კრიპტოგრაფიამ დიდი გზა გამოიარა დღევანდელობამდე და დაფიქსირდა უამრავი საინტერესო ფაქტი, რომელმაც არა მხოლოდ კრიპტოგრაფიის , არამედ კაცობრიობის ისტორიაც შეცვალა.

1.1.ქრისტეს შობამდელი კრიპტოგრაფია:

- 36 -ე საუკუნე : შუმერების შექმნილი ლურსმული დამწერლობა და ეგვიპტელების იეროგლიფები.
- მე-16 საუკუნე: ფინიკიელებმა შექმენას პირველი ანბანი.

  ზოგადად ანბანის შექმნა მნიშვნელოვნად წინ გადადგმული ნაბიჯი გახლდათ არა მარტო კაციობრიობის , არამედ კრიპტოგრაფიის ისტორიისთვისაც. მრავალი საუკუნის განმავლობაში ანბანი წარმოადგენდა შიფრაციის ერთ-ერთ მნიშვნელოვან მეთოდს. ასევე სწორედ ანბანის გარეშე შეუძლებელი იქნებოდა იმ უამრავი შიფრების და მეთოდების განვითარება , რომელიც დღეს სახეზე გვაქვს და რომლის გარეშეც ჩვენი ცხოვრება წარმოუდგენელია.
- 600-500 - ებრაელმა სწავლულებმა შექმნეს პირველი მარტივი წანაცვლებითი შიფრი (ატბაში)

- c. 400 - სპარტელებმა შექმენს სციტალი

  სციტალის შესაქმნელად გამოიყენებოდა პერგამნეტის ლენტი და ხის ძელაკი , პერგამენტს ახვევდნენ ძელაკზე და წერდნენ ტექსტს , შემდეგ გადმოაბრუნებდნენ ლენტს და იმეორებდნენ იგივეს, ლენტის გაშლისას შეუძლებელი იყო დაშიფრული ინფორმაციის წაკითხვა . შიფრის გასაღებს წარმოადგენდა ძელაკის დიამეტრი და სიგრძე , ხოლო დეშიფრაციის დროს დაახვევდნენ ლენტს იგივე ზომის ძელაკზე და ამ გზით შესაძლებელი იყო ტექსტის წაკითხვა. სციტალეს შიფრის გატეხვის ავტორად ითვლება არისტოტელე, რომელიც ახვევდა ლენტს კონუსოიდურ ჯოხს

მანამ, სანამ არ გამოჩნდებოდა ტექსტის ნაწილი, რომლის წაკითხვაც იყო შესაძლებელი.

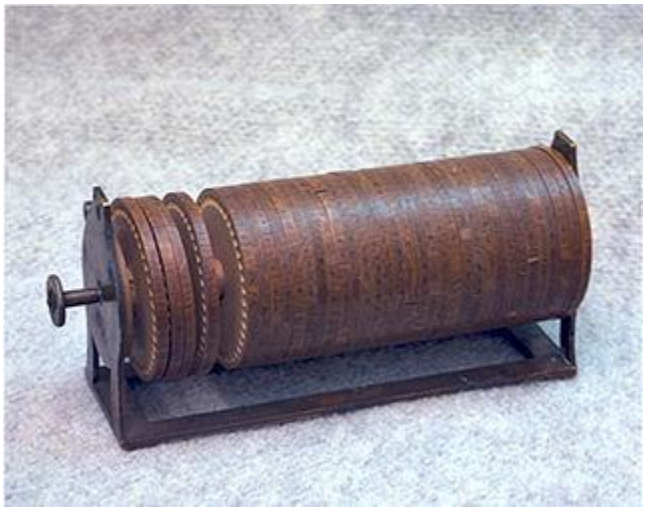
- c. 400 - ჰეროდოტემ სპარსეთიდან საბერძნეთში გაგზავნა პირველი სტენოგრაფიული რეპორტი (ტატუ გადაპარსულ თავზე)
- 100-1 CE - რომის იმპერიის შიფრი , ცნობილია როგორც ცეზარის შიფრი.
  იულიუს ცეზარი აღწერს შიფრს, რომელშიც ასოები ინაცვლებიან ჩანაცვლების მიხედვით, რომელშიც თითოეული ასო ჩანაცვლებულია სამი პოზოციით მარჯვნივ.

1.2.ქრისტეს შობიდან 1 - 1799 წლები

- 801–873 – განვითარდა კრიპტოანალიზი და მონოანბანური შიფრების გატეხვის სტატისტიკური მეთოდები მუსლიმი მათემატიკოსის ალ-კინდის მიერ.
- 1355-1418 – აჰმად ალ-ქალქაშანდიმ დაწერა სუბ ალ-ა'შა , 14 - თავიანი ენციკლოპედია, რომელიც შეიცავდა კრიპტოგრაფიის სექციას , რომელშიც შესული იყო იბნ ალ-დურაიჰიმის (1312-1361) ნაშრომები. შიფრების სია , რომლების შედიოდა ამ ნაშრომში , მოიცავდა ცვლილებებსა და ტრანსპოზიციას. ასევე პირველად ისტორიაში იყი წარმოდგენილი შიფრი განსხვავებული ცვლილებებით, განსხვავებული ტექსტებისთვის (Multi Substitutions). ასევე წარმოდგენილი იყო სტატისტიკური ანალიზის ცხრილი და იმ სიმბოლოების სია , რომლებიც ერთად არ ხვდებოდა არცერთ სიტყვაში.
- 1450 – ჩინელებმა შეიმუშავეს ხის ბლოკებით გადანაცვლებადი ბეჭდვა.
- 1450-1520 – შეიქმნა ვოინიჩის მანუსკრიპტი .
- 1466 - ლეონ ბატისტა ალბერტიმ გამოიგონა პოლიანბანური შიფრი , ცნობილი როგორც პირველი მექანიკური შიფრ-მანქანა.
- 1518 - იოჰან ტრითემუსის წიგნი კრიპტოგრაფიაზე.
- 1553 - ბელასომ აღწერა შიფრი, რომელიც შემდგომში ვიჟინერმა გააუმჯობესა და დღეს ცნობილია , როგორც ვიჟინერის შიფრი. აღსანიშნავია , რომ შიფრაციას შემოაქვს ცნება **სიტყვა-გასაღები.** სიტყვა-გასაღები ძირითადად გვევლინება ერთი სიტყვის ან ფრაზის სახით. შიფრაცია სრულდება შემდეგნაირად: მზადდება

ჩანაცვლების ტაბულა, რომელშიც პირველი სტრიქონი არის ანბანი, მეორე არის ანბანი გადანაცვლებული ერთი ბიჯით და ა.შ. დაშიფრისთვის ყოველ ნიშანზე იყენებენ სიტყვის გასაღებს, რომ შესრულდეს შენაცვლება. ცხადია, რაც უფრო გრძელი და მრავალფეროვანია სიტყვა გასაღები მით უკეთესად არის დაშიფრული ტექსტი და უკეთესად დაცული. იყო დრო როდესაც ლიტერატურული ნაწარმოებების მთელი პასაჟები გამოიყენებოდა ყველაზე დიდი საიდუმლოებების დაშიფრისთვის. ორივე კორესპონდენტს, გამგზავნსაც და მიმღებსაც, ხელში მხოლოდ ერთი და იმავე წიგნის ეგზემპლიარი ეკავათ, რომ დარწმუნებულიყვნენ შეტყობინების სწორად გაგებაში. ყოველი დაუშიფრავი ტექსტისთვის უნდა შეირჩეს შესაფერისი კოლონა და ყოველი სიტყვა-გასაღებისთვის უნდა შეირჩეს ადეკვატური ხაზი, შემდეგ ხაზის და კოლონის გადაკვეთაზე შევხვდებით დაშიფრულ ასოს. სიტყვა-გასაღების ტექსტი ერთვება იმ მიმდევრობაში, რომელშიც არსებობს და მეორდება გასაღები რგოლში მანამ, სანამ საჭიროა.

- 1585 - ვიჟინერის წიგნი შიფრებზე
- 1586 - კრიპტოანალიზი გამოყენებული იქნა უმაღლესი ჯაშუშის სერ ფრენსის ვოლსინგჰემის მიერ რათა ჩაერია შოტრლანდიის დედოფალი მერი დედოფალი ელიზაბეტ პირველის მოსაკლავად (დედოფალი მერი სიკვდილთ დასაჯეს)
- 1641 - Wilkins' Mercury (ინგლისური კრიპტოგრაფიის წიგნი)
- 1793 - კლაუდ ჩაპმა გამოიგონა პირველი შორ მანძილზე გადაცემადი სემაფორული სიგნალები.
- 1795 - ტომას ჯეფერსონმა გამოიგონა ჯეფერსონის შიფრ-დისკი, რომელიც 100 წლის შემდგ გაუმჯობესდა ითან ბაზერის მიერ.



ჯეფერსონის დისკი წარმოადგენდა შიფრაციის სისტემას , რომელიც წარმოადგენდა დისკების ნაკრებს. თითოეულ დისკის გარშემო მოთავსებული იყო ანბანის 26 სიმბოლო. დისკებზე სიმბოლოთა განლაგება განსხვავებული იყო თითოეული დისკისთვის , ასევე ყველა დისკს გააჩნდა უნიკალური ნომერი. დისკის ცენტრში იყო ხვრელი , რომლის საშუალებითაც დისკები მოთავსებული იყო ღერძზე. შესაძლებელი იყო დისკების მოძრობა და ღერზე მათი განთავსება ნებისმიერი მიმდევრობით. სწორედ დისკების თანმიმდევრობა წარმოადგენდა შიფრის გასაღებს და მიმღებსაც და გამგზავნსაც უნდა ქონოდათ დისკები ერთი და იგივე რიგით დალაგებული.(ჯეფერსონის ამ შიფრის ვერსიას გააჩნდა 36 დისკი). როდესაც გამგზავნი დაალაგებდა დისკებს თავისი სასურველი რიგით, ატრიალებდა დისკებს მანამ , სანამ არ მიიღებდა სასურველ ტექსტს. მიმღებსაც უნდა დაელაგებინა დისკები იგივე რიგით და იგი მოახერხებდა დაშიფრული ინფორმაციის წაკთხვას. აღნიშნული შიფრი არ იყო პოპულარუი ჯეფერსონის დროს, იგი 100 წლის შემდეგ გაუმჯობესდა ითან ბაზერის მიერ, ამ შემთხვევაში შიფრმა დიდი პოპულარობა მოიპოვა და გამოიყენებოდა კიდეც ამერიკის შეერთებული შტატების არმიის მიერ.

1.3. 1800-1899 წლები

- 1809-14 ჯორჯ სქოველის ნაშრომი ნაპოლეონურ შიფრზე ნახევარკუნძულის ომის დროს.
- 1831 - იოზეფ ჰენრიმ ააგო პირველი ელექტრული ტელეგრაფი.
- 1835 - სემუელ მორზემ გამოიგონა მორზეს ანბანი.

მორზეს ანბანი არის სიმბოლოთა კოდირების ერთ-ერთი საშუალება. მისი საშუალებით ანბანის თითოეული ასოს, ციფრების და სასვენი ნიშნების ნაცვლად გამოიყენება გრძელი და მოკლე სტანდარტული ელემენტები. ეს ელემენტები შეიძლება იყოს ხმოვანი სიგნალები ან ნიშნები და ცნობილია როგორც „წერტილები“ და „ტირეები“. მორზეს ანბანში ყოველი სიმბოლო წარმოდგენილია , როგორც წერტილებისა და ტირეების უნიკალური მიმდევრობა . ტირეს ხანგძლივობა სამჯერ მეტია წერტილის ხანგძლივობაზე . ყოველი წერტილის და ტირის შემდეგ არის წერტილის დროის ტოლი სიჩუმე , ყოველი სიმბოლოს შემდეგ ტირის ტოლი სიჩუმე , ხოლო ყოველი სიტყვის შემდეგ არის შვიდი წერტილის ტოლი სიჩუმე . მორზეს ანბანი დღესდღეობით გამოიყენება არმიაში,საავიაციო და საზღვაო დარგში. მორზეს ანბანის თანამედროვე ვარიანტი გაჩნდა 1939 წელს.

- 1854 - ჩარლს ვითსთოუნმა გამოიგონა Playfair შიფრი.
- 1854 - ჩარლზ ბებიჯის მეთოდი პოლიანბანური შიფრების გატეხვისთვის.
- 1883 - გამოქვეყნდა ოგუსტ კერკროფსის „ La Cryptographie militare“
- 1883 - გამოქვეყნდა ფრიდრიხ კაზისკის წიგნი მრავალანბანური შიფრის გატეხვის შესახებ ვიჟინერის შიფრის მაგალითზე.

წლების განმავლობაში მიიჩნეოდა , რომ ვიჟინერის შიფრის გატეხვა შეუძლებელი იყო, თუმცა კაზისკიმ შემოთავაზა ლოზუნგში ასოების რაოდენობის სტატისტიკური განსაზვრის მეთოდი, რომელიც ეფუძნება შემდეგ იდეას: ასოების განმეორებადობა ლოზუნგში ღია ტექსტში განმეორებადობასთან ერთად იძლევა ასოების განმეორებადობას დაშიფრულ ტექსტში. ავტორი მივიდა იმ დასკვნამდე, რომ შიფროტექსტში განმეორებების მანძილი იქნება ლოზინდგის პერიოდის, ანუ მისი მანძილის, ტოლი ან მისი ჯერადი. ლოზუნგის სიგრძის განსაზღვრის მერე შიფროტექსტი იხლიჩება ნაწილებად, რომლებიც ლოზუნგის სიგრძის ტოლია, და საწყისი ამოცანა დაიყვანება მარტივი ჩანაცვლების დეშიფრაციაზე. დეშიფრაციის ამ მეთოდს ეწოდება “კაზისკის მეთოდი“.

- 1894 - დრეიფუსის საქმე საფრანგეთში რომლის დროსაც ჩანს კრიპტოგრაფიის ბოროტად გამოყენება ყალბ დოკუმენტებთან დაკავშირებით.

1.4.1900 – 1949 წლები

- 1915 - უილიამ ფრაიდმანმა ჩართო სტატისტიკა კრიპტოანალიზში.
- 1917 - ჯილბერ ვერნამმა შეიმუშავა ვერნამის ალგორითმი

  ვერნამის ალგორითმი წარმოადგენს ცეზარის და ვიჟინერის ალგორითმების შემდგომ განვითარებას. ვერნამის ალგორითმი წარმოადგენდა იმ დროისთვის ერთადერ სრულყოფილ ალგორითმს, რომელიც აკმაყოფილებდა შენონის მიერ შემუშავებულ კრიტერიუმებს. ვერნამის შიფრის დროს გასაღების სიგრძე , ცეზარის ალგორითმისგან განსხვავებით გახდა ერთზე მეტი და ემთხვევა კიდეც დასაშიფრი ტექსტის სიგრძეს, ასევე გასაღები ვერნამის ალგორითმში გამოიყენება ერთჯერადად. თვითონ ვერნამის შიფრს იყენებდნენ ამერიკისა და საბჭოთა კავშირის ლიდერები. თუმცა მის მთავარ პრობლემას წარმოადგენდა სინქრონიზაცია და გასაღების ფორმირების ამოცანა. გასაღებს ზოგჯერ ფსევდოშეთანხმებითი სახე, ზოგჯერ კი რომელიმე მხატვრული ნაწარმოების მკაცრად შეთანხმებული ტექსტის სახე ქონდა .
- 1917 - ჯილბერტ ვერნამმა განავითარა ნაკადური შიფრის პირველი პრაქტიკული გამოყენება.

ნაკადური შიფრი ქმნის განუსაზღვრელი სიგრძის გასაღებს, რომელიც შემდგომ უერთდება საწყის ინფორმაციას (ბიტობრივად ან ბაიტობრივად). გამომავალი ინფორმაცია დამოკიდებულია შიფრის შინაგან მდგომარეობაზე, რომელიც მოქმედების მიმდინარეობისას იცვლება. ნაკადური შიფრაციის დროს დასაშიფრი ტექსტის ელემენტების გარკვეული რაოდენობა იშიფრება ერთდროულად. ნაკადური შიფრის ტექნოლოგია გამოიყენება RC4 - ის შიფრში . ამჟამად ყველაზე გავრცელებული ნაკადური შიფრის ერთ-ერთი მაგალითია **A5/1** , რომელიც უზრუნველყოფს GSM ოპერატორებისთვის გადასაცემი ინფორმაციის კონფიდენციალურობას.

- 1917 - მოხდა თავდასხმა ზიმერმანის ტელეგრამაზე და მოხდა მისი დეშიფრაცია ა.შ.შ.-ს პირველ მსოფლიო ომში ჩართვამდე.
- 1918 - არტურ შერბიუსმა შექმნა ერთ-ერთი ყველაზე წარმატებული როტორული მანქანა „ენიგმა“

  არტურ შერბიუსი გახლდათ გერმანელი ინჟინერი , მისი შექმნილი ენიგმა უკვე 1920 - იანი წლებიდან გამოიყენებოდა როგორც კომერციული, ასევე სახელმწიფო მიზნებისთვის. მანქანის ყველაზე ცნობილი მოდელი არის ე.წ. ვერმახტის ენიგმა , რომელსაც აქტიურად იყენებდა გერმანია მეორე მსოფლიო ომის დროს. მიუხედავად იმისა , რომ თანამედროვე გადმოსახედიდან ენიგმას შიფრი არც ისე ძლიერია , იმ დროისთვის მისი გატეხვა ბრიტანელმა მეცნიერებმა მხოლოდ პროცედურული შეცდომებისა და მანქანის და გასაღებების ცხრილების ხელში ჩაგდების შემდეგ შეძლეს. ზოგადად ენიგმა შიფრაციისთვის იყენებდა როტორებს და რეფლექტორს. როტორი წარმოადგენდა დისკს , რომელსაც ორივე მხარეს ქონდა 26-26 კონტაქტი, ხოლო რეფლექტორი დისკს , მხოლოდ ერთ მხარეს კონტაქტებით. როტორები ერთმანეთის გვერდით იყვნენ განლაგებულები (ვერმახტის ენიგმას ქონდა 3 როტორი) და ერთი როტორის გამოსასვლელები უკავშირდებოდა შესასვლელებს, ბოლო როტორი უკავშირდებოდა რეფლექტორს. ყოველი ასოს დაშიფრვის შემდეგ ხდებოდა როტორების განსაზღვრული წესით მობრუნება. ეს მობრუნების წესი განსხვავებული იყო სხვადასხვა მოდელებში. ენიგმა ასევე იყენებდა კომუტაციურ

პანელს, რომლთაც ხდებოდა სიმბოლოების წყვილ-წყვილად დაკავშირება. ენიგმას გასაღები შედგებოდა რამდენიმე მონაცემისგან:

1. როტორების მოდელები და მათი თანმიმდევრობა
2. როტორების საწყისი მდგომარეობა
3. კომუტაციურ პანელზე დაწყვილებული ასოების ჩამონათვალი

ენიგმას შიფრს გააჩნდა სიმეტრიული თვისება , თუ როტორების და კომუტაციური პანელის მდგომარეობა ზუსტად იგივეა, დაშიფრული ტექსტის ხელახალი დაშიფრვისას მიიღებოდა საწყისი ტექსტი.

- 1919 - ედუარდ ჰებერნმა გამოიგონა და დააპატენტა პირველი როტორული მანქანის დიზაინი , იმავე წელს დამმს , შერიბუსს და კოშს ქონდათ იგივე შედეგები .
- 1921 - ვაშინგტონის კონფერენცია - ა.შ.შ. - ს მომლაპარაკებელთა ჯგუფმა დახმარება გასწია იაფონური დიპლომატიური ტელეგრამის დეშიფრაციისას.
- 1932 - გერმანული „ენიგმას“ გატეხვის პირველი მცდელობა პოლონელი მარიან რეჯევსკის მიერ.
- 1931 - ჰერბერტ იარდლიმ გამოაქვეყნა „ამერიკული შავი ოთახი“ , რომელიც ფარდას ხდიდა ამერიკული კრიპტოგრაფიის უამრავ საიდუმლოს.
- 1940 – SIS ჯგუფის მიერ მოხდა იაპონური PURPLE მანქანის შიფრის გატეხვა.
- აპრილი 1943 - მაქს ნიუმენმა , ვინ უილიამსმა და მისმა ჯგუფმა (ალან ტიურინგის ჩათვლით) სახელმწიფო საიდუმლოების დონეზე ააგეს "Heath Robinson". ეს იყო სპეციალური მანქანა , რომლის ძირითადი ფუნქცია იყო შიფრების გატეხვა.
- დეკემბერი 1943 - შექმნილი იქნა The Colossus (კომპიუტერი) , თომას ფლოვერსის მიერ ლონდონში , რათა გაეტეხათ გერმანული ლორენც შიფრი (SZ42) მეორე მსოფლიო ომის დროს . თუმცა ცუდ ხელში მოხვედრისგან თავდაცვის მიხზნით, აღნიშნული კომპიუტერი განადგურდა მასზე დაკისრებული საქმის შესრულებისთანავე.
- 1944 - დაპატენტდა SIGABA კოდირების მანქანა, რომელიც გამოყენებული იყო ა.შ.შ.- ს მიერ მეორე მსოფლიო ომში.
- 1946 - The Venona project - მა პირველად შეაღწია საბჭოთა ჯაშუშურ ტრეფიკში.

- 1948 - კლოდ შენონმა პირველად გამოაქვეყნა ინფორმაციის თეორიის მათემატიკური საწყისები.
- 1949 - Bell Labs ტექნიკურ ჟურნალში გამოქვეყნდა შენონის საიდუმლო სისტემების კომუნიკაციის თეორია.

1.5. 1950 – 1999 წლები

- 1951 - დაარსდა ა.შ.შ. სახელმწიფო უსაფრთხოების სააგენტო და მოგვიანებით წარმოდგენილი იქნა KL-7 როტორული მანქანა.
- 1957 - KW-26 ელექტორნული დაშიფრვრის სისტემა.
- 1964 - გამოქვეყნდა დევიდ კანის „The Codebreakers“.
- 1969 – ARPANET -ის (ინტერნეტის წინაპარი) ჰოსტები დაუკავშირდნენ ერთმანეთს.
- 1970 - ინფორმაციის კვანტური მდგომარეობით დეკოდირების გამოყენებით, შტეფან ვიზნერმა გამოიგონა შეწყვილებული კოდირება , რათა შეემუშავებინა პროექტი „ფულის გაყალბება ფიზიკურად შეუძლებელია“ (თუმცა აღნიშნული პროექტის ტექნიკური განხორციელება ჯერ კიდევ მიუწვდომელია)
- 1974 - ჰორს ფეისტელმა განავითარა ფეისტელ ნეთვორკ ბლოკური შიფრის დიზაინი.
- 1976 - ა.შ.შ-ს ფედერალური ინფორმაციის სამუშაო სტანდარტად ინფორმაციის შიფრაციის სტანდარტი დასახელდა.
- 1976 - გამოქვეყნდა დიფი-ჰელმანის ალგორითმი.

  1976 წელი თამამად შეგვიძლია მივიჩნიოთ უმნიშვნელოვანეს საკვანძო წლად კრიპტოგრაფიის და მისი განვითარების ისტორიაში . სწორედ ამ წელს უიტფილდ დიფმა და მარტინ ჰელმანმა შეიმუშავეს ახალი ალგორითმი და საფუძველი ჩაუყარეს ახალ, ასიმეტრიულ კრიპტოსისტემას, რომლის დროსაც სიმეტრიული კრიპტოსისტემებისგან განსხვავებით, გასაღებიც , ისევე როგორც დაშიფრული ტექსტი გადაეცემა ღია არხით. მათ ეს მოახერხეს მათემატიკაში მანამდე ხელუხლებელი ცალმხრივი ფუქნქციის დახმარებით. თუმცა უნდა აღინიშნოს , რომ გასაღებების ღია არხით გადაცემის იდეა ორი წლით ადრე დაებადა რალფ მერკლის,

რომელმაც ამ იდეის შესახებ შეატყობინა კიდეც თავის ერთ-ერთ ლექტორს, თუმცა მაშინ აღნიშნული ფაქტი იმდენად წარმოუდგენელი იყო , რომ პასუხად მხოლოდ დაცინვა მიიღო. აღნიშნულ ფაქტს უქმად არ ჩაუვლია, სწორედ მის იდეებზე დაყრდნობით შეიმუშავეს და განავითარეს ასიმეტრიული კრიპტოსისტემის იდეა.

- 1977 – RSA

  1977 წელს რონ რივესტის, ადი შამირის და ლენ ადლემანის ერთობლივი მუშაობის შედეგად შეიქმნა RSA ალგორითმი , რომელიც წარმოადგენს შიფრაციისა და ნამდვილობის (აუტენტიფიკაციის) ახალ მეთოდს. RSA დაპატენტებულია შეერთებულ შტატებში , ლიცენზირებულია სხვა ქვეყნებში და წარმოადგენს ფაქტიურ შიფრაციის სტანდარტს მსოფლიოს მრავალ ქვეყანაში , მნიშვენელოვან გამოყენებას ჰპოვებს ელექტრონულ კომერციაში, განსაკუთრებით საიდუმლო მონაცემების გასაცვლელად ინტერნეტში.
- 1978 წელს მერკლისა და ჰელმანის ერთობლივი მუშაობით გამოქვეყნდა მერკლი-ჰელმანის ალგორითმი.
- 1984 - ვიჟინერის იდეებზე დაყრდნობით ჩარლზ ბენეტმა და ჯილს ბრასარდმა შეიმუშავეს კვანტური კრიპტოგრაფიის პროტოკოლი BB84.
- 1985 - ტახირ ელგამალმის ციფრული ხემოწერა

  ტახირ ელგამალმა 1985 წელს წარმოადგინა ნაშრომი ციფრული ხელმოწერის შესახებ. ალგორითმის მიზანი არ ყოფილა ორ სიბიექტს შორის დაშიფრული ინფორმაციის მიმოცვლა და მერე მისი დეშიფრაცია. მისი მიზანი გახლდათ ის, რომ გარკვეული ღია ინფორმაცია , რომელსაც ერთი პიროვნება უგზავნის მეორეს არ დაზიანდეს გზად მესამე , გარეშე პიროვნების მიერ და მეორე პიროვნებამ მიიღოს ის იმავე სახით, რა სახითაც გაუგზავნეს მას . ელგამალის ალგორითმი არ იყო თავიდანვე დაპატანეტებული , რადგან იგი თავისი გამოთვლებისთვის იყნენებდა დიფი-ჰელმანის ალგორითმს, მხოლოდ 1991 წელს სტანდარტებისა და ტექნიკის ინსტიტუტმა (NITS) ელგამალის ალგორითმის ბაზაზე შექმნილი ციფრული ხელმოწერის ალგორითმის DSA -ს (Digital Signature Algorithm) მიხედვით შეიმუშავა ციფრული ხელმოწერის სტანდარტი DSS (Digital Signature Standard).

- 1986 - ა.შ.შ. - მ კომპიუტერული სისტემების გატეხვა შეიტანა კანონსაწინააღმდეგო ქმედებათა სიაში.
- 1989 - ტიმ ბერნერს-ლიმ და რობერტ კაიომ ცერნში ააგეს პროტოტიპული სისტემა, რომელიც შემდგომში გახდა მსოფლიო ქსელი (WWW).
- 1989 - ჩარლზ ბენეტმა მოახდინა პირველი კვანტრული კრიპტოგრაფიის ექსპერიმენტული დემონსტრირება.
- 1991 - ფილ ზიმერმანმა გამოაქვეყნა ღია არხით შიფრაციის პროგრამის (PGP) სორს კოდი , რომელიც სწრაფად გავრცელდა ინტერნეტში.
- 1994 - გამოიცა ბრიუს შნაიერის „გამოყენებითი კრიპტოგრაფია“.
- 1994 - Secure Sockets Layer (SSL) შიფრაციის პროტოკოლი გამოქვეყნდა Netscape-ს მიერ.
- 1994 - ინტერნეტში გამოქვეყნდა RC4 შიფრის ალგორითმი.
- 1995 - სახელმწიფო უსაფრთხოების სააგნეტომ გამოაქვეყნა SHA1 - ჰეშირების ალგორითმი, როგორც თავისი ციფრული ხელმოწერის სტანდარტი.დ
- July 1997 - გამოქვეყნდა OpenPGP სპეციფიკაცია (RFC 2440) .
- 1997 - გამოქვეყნდა Ciphersaber, RC4 - ზე დაფუძნებული შიფრაციის სისტემა.
- ოქტომბერი 1999 - DeCSS, ინტერნეტში გამოქვეყნდა პროგრამა , რომელსაც შეეძლო დვდ-ზე ინფორმაციის დეშიფრაცია.

1.6.2000 და ზემოთ

- 6 სექტემბერი, 2000 - RSA Security Inc. - მა გამოუშვა RSA ალგორითმი საზოგადოების მიერ წვდომად დომეინზე .
- 2001 - ბელგიელი რიჯნდილის ალგორითმი ამორჩეული იქნება როგორც ა.შ.შ-ს შიფრაციის სტანდარტი (Advanced Encryption Standard (AES))
- 2004 - ID Quantique - მ წარმოადგინა პირველი კომერციული კვანტური კრიპტოგრაფიული სისტემა.

- 2005 - მოხდა SHA1-ზე პოტენციური შეტევების დემონსტრირება
- 2005 - ა.შ.შ - ში ფედერალური ბიუროს აგენტებმა დემონსტრირება გაუკეთეს თავის შესაძლებლობებს **Wired Equivalent Privacy** (**WEP**) - გატეხვის შესახებ .
- 2007 – NIST - მა დააანონსა ჰეშ ფუნქციების კონკურსი.
- 2012 - NIST - მა შეარჩია კესაკის ალგორითმი SHA-3 - ჰეშ ფუნქციების კონკურის გამარჯვებულად.
- 2013 - NSA -მ გამოაქვეყნა საიმონის და სპეკის მსუბუქი ბლოკური შიფრი.
- 2015 - წელი , როდეცას NIST - მა გაავრცელა რჩევა 80 ბიტიანი გასაღებების დასრულების შესახებ.

თავი II : გასაღების სწრაფი გაცვლის ამოცანა კრიპტოგრაფიაში

მოცემულ თავში განხილულია შემდეგი საკითხები : სიმეტრიული და ასიმეტრიული კრიპტოსისტემები, ცალმხრივი ფუნქცია, დიფი-ჰელმანის

2.1. სიმეტრიული და ასიმეტრიული კრიპტოსისტემები

კრიპტოგრაფიის დროსი განვითარებამ გვაჩვენა, რომ საბოლოო ჯამში კრიპტოსისტემები ორ დიდ, ძირითად ჯგუფში გადანაწილდა, ესენია სიმტერიული და ასიმეტრიული კრიპტოსისტემები.

სიმეტრიული კრიპტოსისტემა წარმოადგენს ისეთ სისტემას, რომელშიც ინფორმაციის შიფრაცია/დეშიფრაციისათვის გამოიყენება 1 გასაღები. ხოლო მოკავშირე მხარეები იყენებენ ორ არხს. ერთი არის ღია არხი , შიფროტექსტის გადასაცემად , ხოლო მეორე არის დახურული არხი , გასაღების გადასაცემად.

მისგან განსხვავებით ასიმეტრიული კრიპტოსისტემა წარმოადგენს კრიპტოსისტემას, რომელიც იყენებს გასაღებების წყვილს — ღია და პირად გასაღებებს. ამ შემთხვევაში დახურული არხი აღარ გამოიყენება , რადგაც როგორც შიფროტექსტის , ისე გასაღების გადაგზავნა ხორციელდება ღია არხით. ასიმეტრიული სისტემები აღნიშნული შედეგის მისაღწევად იყენებს ცალმხრივ ფუქნციას .

2.2. ცალმხრივი ფუნქცია

ცალმხრივი ფუნქცია წარმოადგენს ისეთ ფუნქციას , რომელის მნიშვნელობის გამოთვლა მარტივია , თუ ვიცით არგუმენტის მნიშვნელობა . თუმცა მნიშვნელობიდან არგუმენტის მიღება კოლოსალურ დროს და რესურს მოითხოვს , თუმცა ასევე შეიძლება ითქვას , რომ რეალურ დროში ფუნქციის მნიშვნელობიდან არგუმენტის მიღება შეუძლებელია .

ეს ყველაფერი კარგად ჟღერს, მაგრამ ჯერჯერობით არ არის დამტკიცებული ცალმხრივი ფუნქციის არსებობა თეორემის სახით. მიუხედავათ ამისა, არსებობს

ისეთი ფუნქციები, რომლებსაც აქვთ ცალმხრივი ფუნციის თვისებები, ანუ ჩვენ შეგვიძლია მარტივად გამოვთვალოთ მათი მნიშვნელობა, მაგრამ არ არის ცნობილი ეფექტური ალგორითმი, რომლითაც შეგვეძლება გამოვთვალოთ არგუმენტის მნიშვნელობა ფუნქციის მნიშვნელობიდან გამომდინარე.

დღესდღეობით ცნობილია შემდეგი ცალმხრივი ფუნქციები

$a^x \equiv y \bmod p$,

სადაც $1 < a, x, y < p$.

$a^{\varphi(N)} = 1 \bmod N$.

ეს ფუნქციები გამოიყენება ცნობილ ალგორითმებში შესაბამისად დიფი - ჰელმანის და RSA ალგორითმებში

ცალმხრივი ფუნქციებიდან აღსანიშნავია ასევე ბატონი რიჩარდ მეგრელიშვილის მიერ აღმოჩენილი და გამოკვლეული ახალი მატრიცული ცალმხრივი ფუნქცია , რომლის კვლევა და გასაღებების გაცვლის ალგორითმში გამოყენებაც წარმოადგენდა სწორედ აღნიშნული სამაგისტრო ნაშრომის მიზანს. აღნიშნულ ფუნქციას აქვს შემდეგი სახე :

$vA = u$,

სადაც v და u არის ვექტორები V_n ვექტორული სივრციდან, რომელიც განსაზღვრულია GF(2) ველზე, ხოლო A არის საწყისი მატრიცი GF(2) ველზე. $A \in A$, სადაც A წარმოადგენს გადაუგვარებელ მატრიცთა კლასს (მატრიცთა მულტიპლიკაციურ ჯგუფს).

2.3. დიფი-ჰელმანის ალგორითმი

1976 წელს გადატრიალება მოხდა კრიპტოგრაფიაში . სწორედ ამ წელს უიტფილდ დიფიმ და მარტინ ჰელმანმა შეიმუშავეს ახალი კრიპტოგრაფიული ალგორითმი და საფუძველი ჩაუყარეს ახალ მიმართულებას კრიპტოგრაფიაში, კერძოდ ასიმეტრიულ კრიპტოსისტემებს. ასიმეტრიული კრიპტოსისტემები როგორც უკვე ავღნიშნეთ წარმოადგენს დაშიფრული ინფორმაციისა და გასაღებების გაცვლის ახალ სტანდარტს , კერძოდ ასიმეტრიულ სისტემებში გამქრალია დახურული არხის

არსებობის საჭიროება , რადგან გასაღები გადაეცემა ღია არხის საშუალებით. ამ პრობლემის გადასაწყეტად დიფიმ და ჰელმანმა გამოიყენეს ცალმხრივი ფუნქცია . მას შემდეგ ცალხრივი ფუნქცია ასიმეტრიული სისტემების განუყოფელ ნაწილად იქცა.

სწორედ ასეთი ფუნქცია გამოიყენეს დიფი-ჰელმანმა თავიანთი ალგორითმისთვის . მათ ცალმხრივ ფუნქციას ქონდა შემდეგი სახე :

$$y=a^x \pmod p$$

სადაც p არის საკმაოდ დიდი მარტივი რიცხვი , ხოლო a და x ისთვის სრულდება შემდეგი პირობა :

$$1 < a,x < p$$

დიფი - ჰელმანის პროტოკოლი:

1. არის პროტოკოლი ექპონენცილაური გასაღებით;
2. საშუალებას აძლევს ორ მომხმარებელს გაცვალონ ერთმანეთში საიდუმლო გასაღებები;
3. არ საჭიროებს ადრინდელ საიდუმლო არხს.

ინფორმაციის გადაცემის უსაფრთხოება არის კრიტიკული მრავალი ქსელური და ინტერნეტ - აპლიკაციისთვის და საჭიროა, რომ მომხმარებლებმა გაუზიაროს გარკვეულ მომხმარებლებს ინფორმაცია ისე, რომ სხვებმა ვერ მოახდინონ მისი (ინფორმაციის) დეშიფრაცია. ბრუს შნაიერი წერდა: "საკმარისი არ არის დავიცვათ საკუთარი თავი კანონებით; ჩვენ გვესაჭიროება საკუთარი თავის დაცვა მათემატიკით".

დიფი-ჰელმანის ალგორითმის საშუალებით გასაღებების გენერირება

დიფი - ჰელმანის ალგორითმი შემდეგნაირად მუშაობს :

პირველი პიროვნება ირჩევს კერძო გასაღებს x - ს , ასრულებს შემდეგ გამოთვლებს :

$$C_1 = a^x \pmod p$$

მიღებულ C_1 -ს უგზავნის მეორე პიროვნებას , რომელიც მიღებული ინფორმაციისა და თავისი კერძო გასაღების y - ის საშუალებით გამოითვლის პირველ საერთო გასაღებს :

$K_1 = (C_1)^y \pmod p = (a^x)^y \pmod p = a^{xy} \pmod p$;

შემდეგ მეორე პიროვნება თავისი კერძო გასაღების (y - ის) საშუალებით ასრულებს შემდეგ გამოთვლებს :

$C_2 = a^y \pmod p$

მიღებულ C_2 -ს უგზავნის პირველ პიროვნებას , რომელიც მირებული ინფორმაციისა და თავისი კერძო გასაღების x - ის საშუალებით გამოითვლის მეორე საერთო გასაღებს :

$K_2 = (C_2)^x \pmod p = (a^y)^x \pmod p = a^{yx} \pmod p$

ადვილი შესამჩნევია, რომ პირველი გასაღების შემთხვევაში a ადის xy ხარისხში , ხოლო მეორე გასაღების შემთხვევაში კი yx ხარისხში , იმის გათვალისწინებით , რომ x და y გამრავლების მიმართ კომუტაციურები არიან , ორივე კერძო გასაღები ტოლია და შეგვიძლია ჩავწეროთ :

$K = K_1 = K_2$

ანუ ორივე მხარეს აქვს ერთი და იგივე გასაღები და მათ თამამად შეუძლიათ გაცვალონ ერთმანეთში ამ საერთო გასაღებების საშუალებით დაშიფრული ინფორმაცია.

დიფი-ჰელმანის ალგორითმში ძირითად დაცვას წარმოადგენს p რიცხვის სიდიდე , ის საკმარისად დიდია იმისთვის ,რომ სრული გადარჩევის შემთხვევაში ალგორითმის გატეხვის მსურველმა, რეალურ დროში ვერ მოახერხოს, რადგან დისკრეტული ლოგარითმის გამოთვლა რთულია ხარისხში აყვანის გამოთვლასთან შედარებით (დიფი - ჰელმანის პრობლემა). დღესდღეობით არ არის ცნობილი ალგორითმის გატეხვის რომელიმე წარმატებული სტრატეგია.

2.3.1. დიფი-ჰელმანის პროგრამული რეალიზაციის მეთოდები

როგორც ალგორითმის სტრუქტურიდან ჩანს , დიფი-ჰელმანის ალგორითმი იყენებს ხარისხში აყვანას, რაც პროგრამულად საკმაოდ „მძიმე“ ოპერაციაა, განსაკუთრებით კი ისეთ დიდ რიცხვებთან რომელიც გამოიყენება აღნიშნულ ალგორითმში . სწორედ ამიტომ პროგრამული გზით , ჩვეულებრივი ხარისხში აყვანა

და მერე მოდულარული გაყოფა მოგვცემს იმდენად ცუდ შედეგს დროის თვალსაზრისით, რომ აზრს კარგავს ამ ალგორითმის გამოყენება. ჩვენს მიერ ჩატარებულმა ძიებამ გამოავლინა კომპანია “Oracle” -ის თანაარსებობით შექმნილი პროგრამული ბიბლიოთეკა , რომელსაც „BigInteger“ ქვია , იგი თავდაპირველად შეიქმნა Java - სთვის , ხოლო შემდეგ გავრცელდა სხვა პროგრამულ ტექნოლოგიებზე. აღნიშნული ბიბლიოთეკა წარმოადგენს „აბსოლუტური სიზუსტის არითმტიკის“ (Arbitrary-precision arithmetic) სტილის ბიბლიოთეკას , რომელიც კომპიუტერულ მეცნიერებებში ასევე ცნობილია როგორც დიდი რიცხვების არითმეტიკა. აღნიშნული BigInteger ბიბლიოთეკის შექმნის ძირითად მიზანს სწორედ კრიპტოგრაფიული ოპერაციების (დიფი-ჰელმანი, RSA და ა.შ) წარმოადგენდა და ამ ბიბლიოთეკაში არსებული და განსაზღვრული მეთოდი : ModPow ასრულებს ზუსტად იმ გამოთვლას რაც საჭიროა დიფი - ჰელმანში. ModPow მეთოდს გადაეცემა სამი პარამეტრი (პირობითად a, x და p) და შესრულების შედეგად მეთოდი აბრუნებს a^x (mod p) მნიშვნელობას . გარდა იმისა , რომ აღნიშნული მეთოდი ასრულებს ზუსტად იმ ოპერაციას , რაც ჭირდება დიფი-ჰელმანის ალგორითმს , იგი ამ ყველაფერს აკეთებს ძალიან სწრაფად .

2.4. ღია არხით გასაღებების გაცვლის ახალი მატრიცული ალგორითმი

გასაღებების გაცვლის მატრიცული ალგორითმი არის ახალი , ორიგინალური ალგორითმი, რომელიც 2006 წელს გამოაქვეყნა ტექნიქურ მეცნიერებათა დოქტორმა, პროფესორმა,ზუსტ და აბუმებისმეტყველო მეცნიერებათა ფაკულტეტის ასოცირებული პროფესორმა, ბატონმა რიჩარდ მეგრელიშვილმა. ალგორითის მუშაობის პრინციპი გავს დიფი-ჰელმანის მუშაობის პრინციპს , თუმცა განსხვავდება მისგან სხვა ცალმხრივი ფუნქციის გამოყენებითა და სწრაფქმედებით.

როგორც ზემოთ ავღნიშნეთ ახალი ალგორითმი იყენებს მატრიცულ ცალმხრივ ფუნქციას :

$u = v * A$

სადაც v და A შესაბამისად GF(2) ველზე განსაზღვრული ვექტორი და მატრიცა.

დიფი-ჰელმანის მიერ გამოყენებული ცალმხრივი ფუნქციისგან განსხვავებით, რომელიც იყენებს ხარისხში აყვანას და რომელიც საკმაოდ "მძიმე" ოპერაციად მიიჩნევა , ახალი ცალმხრივი ფუნქცია გამოთვლების ჩასატარებლად იყენებს ვექტორის მატრიცზე ნამრავლს, რომელიც ნამრავლის და შეკრების ოპერაციათა გარკვეულ რაოდენობაზე დაიყვანება, ხოლო როგორც ცნობილია ნამრავლიც და შეკრებაც ბევრად „მუსუბუქი" ოპერაციებია ხარისხში აყვანასთან შედარებით.

ალგორითმი მუშაობს შემდეგი პრინციპით :

ორი პიროვნება წინასწარ თანხმდება v პარამეტრებზე, რომელიც არის ღია, ორობითი ვექტორი. ამის შემდეგ კი სრულდება შემდეგი გამოთვლები :

პირველი პიროვნება შემთხვევით ირჩევს A_1 (საიდუმლო გასაღებს) მატრიცს $\boldsymbol{A}$ GF(2) ველზე განსაზღვრული მატრიცთა ციკლურ მულტიპლიკაციური სიმრავლიდან, ამრავლებს მასზე v ვექტორს და მიღებულ შედეგს უგზავნის მეორე პიროვნებას :

$u_1 = v * A_1$

მეორე პიროვნება მიღებული შედეგის და თავისი კერძო(საიდუმლო) გასაღების A_2-ის საფუძველზე ითვლის პირველ საერთო გასაღებს:

$K_1 = u_1 * A_2 = v * A_1 * A_2$

ამის შემდეგ მეორე პიროვნება თავისი ჯერძო გასაღების (A_2) და v ვექტორის საშუალებით ითვლის u_2-ს და უგზავნის პირველ პიროვნებას :

$u_2 = v * A_2$

პირველი პიროვნება მიღებული შედეგის საფუძველზე ითვლის მეორე საერთო გასაღებს :

$K_2 = u_2 * A_1 = v * A_2 * A_1$

რადგან აღნიშნული ალგორითმი ძლიერ გავს დიფი-ჰელმანის ალგორითმს , ამისათვის საჭიროა, რომ ორივე საერთო გასაღები იყოს ტოლი, თუმცა ეს მიიღწევა მხოლოდ მაშინ, როცა A_1 და A_2 მატრიცები იქნებიან კომუტატიურები. თუმცა მატრიცები კომუტატიურია (გვაქვს მატრიცთა მულტიპლიკაციური ჯგუფი და შესაბამისად მატრიცები კომუტატიურია), $A_1 * A_2 = A_2 * A_1$, და შესაბამისად მიღებული გასაღებები K_1 და K_2 ერთმანეთის ტოლია.

2.4.1. შიდა რეკურსია

ზოგიერთი არაგადაგვარებული მატრიცი (მატრიცი, რომლის დეტერმინანტი განსხვავდება ნოლისგან) შეიცავს შიდა რეკურსიულ დამოკიდებულებას. ეს დამოკიდებულება არსებობს მატრიცის სტრიქონებს ან სვეტებს შორის. თუმცა, ეს არ არის ჩვეულებრივი წრფივი დამოკიდებულება. ამიტომაც ეს მატრიცები არიან არაგადაგვარებული. ასეთი ტიპის მატრიცების გატეხვა ძალიან ადვილია, როდესაც ისინი გამოყენებულნი არიან კრიპტოგრაფიული მიზნებისათვის. შესაძლებელია მატრიცული შიდა რეკურსიული დამოკიდებულების მქონე სპეციალური კლასის აგება. მაგრამ რიგ შემთხვევებში (განსაკუთრებით, დიდი განზომილების მატრიცებისთვის) შიდა რეკურსიული დამოკიდებულების აღმოჩენა არ არის მარტივი საკითხი. ეს საკმაოდ დიდი პრობლემაა , რადგან ჩვენ მატრიცებს სწორედ კრიპტოგრაფიული მიზნებისთვის ვიყენებთ.

2.4.2. კომუტატიურ მატრიცთა ჯგუფი

როგორც ზემოთ ვახსენეთ ახალი მატრიცული ალგორითმის შესრულების მომენტში მხარეებს ჭირდებათ კომუტატიური მატრიცები, რადგან ალგორითმმა იმუშაოს სწორედ და ორივე მხარეს საბოლოოდ აღმოაჩნდეს საერთო გასაღები. აღნიშნული პრობლემის აღნიშვნისას ვახსენეთ ასევე მატრიცთა მულტიპლაკტიური ჯგუფი , რომლიდანაც იღებენ კიდეც აღნიშნულ მატრიცებს. შიდა რეკურსიის

პრობლემამ ასევე აჩვენა , რომ აღნიშნულ ჯგუფში მატრიცები უნდა იყვნენ არა მხოლოდ კომუტატიურები , ასევე თავისუფალიც უნდა იყვნენ თავისუფალი შიდა რეკურსიისგან. ანუ საჭიროა ასეთი ჯგუფის არსებობა. საბედნიეროდ ამ მიმართულებით გვაქვს რამოდენიმე შემთხვევა , როდესაც დაფიქსირდა აღნიშნული მატრიცთა მულტიპლიკატიური ჯგუფების შედგენის შემთხვევა. ამ მიმართულებით გარკვეული შედეგი აქვს მიღებული უკრაინელ მეცნიერს ბელეცკის , რომელმაც აღნიშნულ შედეგს მიაღწია გრეის კოდების გამოყენებით. მის მიერ მიღებული კლასი თავისუფალია შიდა რეკურსიისგან და მასში შემავალი მატრიცები კომუტატიურებია. იგივე შედეგი აქვს მღებული დოქტორანტ სოფო შენგელიას და ასევე არსებობს რიჩარდ მეგრელიშვილსი მიერ გამოკვლეული ე.წ. „მატრიცთა მოარშიების მეთოდი“, რომელის მიხედვითაც მატრიცთა კლასის გენერირება წარმოადგენდა აწ უკვე მაგისტრის ხარისხის მქონდა ლიანა კლოიანის სამაგისტრო ნაშრომს. აღსანიშნავია , რომ სამივე მეთოდი ერთმანეთისგან განსხვავებულია , თუმცა სამივე იძლევა ისეთ მატრიცთა კლასს, როგორიც საჭიროა ალგორითმის მუშაობისთვის.

უნდა აღინიშნოს , რომ ჩვემს მიერ ახალი მატრიცული ალგორითმის პროგრეამული რეალიზაცისას გამოყენებულია ლიანა კლოიანის პროგრამის მიერ დაგენერირებული მატრიცები.

2.4.3. ალგორითმის დაცვა

ალგორითმებისთვის და განსაკუთრებით კრიპტოგრაფიული ალგორითმებისათვის განსაკუთრებულ მნიშვნელობას წარმოადგენს მისი დაცვა. კრიპტოგრაფიული ალგორითმების გატეხვისადმი მედეგობის მნიშნველობა განპირობებულია მისი გამოყენების სფეროებით, იგი უნდა იყოს იმდენად ძლიერი , რომ გაშერეშე თავდასხმებისგან დაიცვას ყველა ის ინფორმაცია, რომელიც მისი საშუალებით იქნა დაშიფრული.

დაცვას საჭიროებს ახალი მატრიცული ალგორითმიც. აღსანიშნავია , რომ პირველ რიგში ალგორითმის სიმტკიცეს განსაზღვრავს მულტიპლიკაციური ჯგუფიდან აღებული მატრიცი. როგორც ალგორითმიდან ჩანს, მატრიცი ირჩევა

აღნიშნული მატრიცთა ჯგუფიდან შემთხვევით. ამისათვის საჭიროა, რომ ამ ჯგუფში მატრიცთა რაოდენობა იყოს საკმარისად მეტი , რათა მივიღოთ საკმარისი სიმტკიცე. თუმცა ამის პრობლემა ნამდვილად არ არსებობს. ამის დასამტკიცებლად შევადაროთ იგი დიფი-ჰელმანს , თუ დიფი-ჰელმანი p რიცხვად აირჩევს 2^{53} - ამდე არსებულ ბოლო მატრივ რიცხსვს , ჩვენ x არგუმენტის ამორჩევისთვის შეზღუდულები ვიქნებით 1 დან p-მდე , თუმცა როგორც ცნობილია , ასეთი მნიშვნელობა საკმარისი გახდა იმისთვის , რომ დიფი-ჰელმანის ალგორითმი დღემდე მტკიცედ დარჩენილიყო. რაც შეეხება მატრიცულ ალგორითმს , თუ გვექნება 53x53 მატრიცი , ჩვენ ამ მატრიცების ამორჩევა შეგვეძლება მატრიცთა მულტიპლიკატიური ჯგუფიდან , რომელშიც მატრიცთა რაოდენობა არის $2^{53} – 1$ განსხვავებული მატრიცი , რომელიც რიცხვობრივად ტოლია : 9007199254740991.

თუმცა ალგორითმის დასაცავად არსებობს კიდევ ორი დაცვის მექანიზმი , ესენია ტროპიკული ოპერაციები და ელ-გამალის ციფრული ხელმოწერა.

ტროპიკული ოპერაციები :

ტროპიკული ოპერაციები წარმოადგენს არაკლასიკურ ოპერაციებს , რომელის დროსაც გარკვეული კლასიკური ოპერაციები მოქმედებენ სხვაგვარად. ტროპიკულ ოპერაციებში სხვაგვარადაა განსაზღვრული არითმეტიკული , გეომეტრიული და ტოპოლოგიური ოპერაციები და ჩვენც მატრიცთა მულტიპლიკატიური ჯგუფის გენერირებისას სწორედ არითმეტიკულ ტროპიკულ ოპერაციებს ვიყენებთ, კერძოდ გამრავლებას , რომლის დროსაც შეიძლება ითქვას , რომ შემოგვაქვს ახალი უცნობი, რომელიც უზრუნველყოფს ალგორითმის მედეგობას.

კლასიკური გამრავლება	ტროპიკული გამრავლება
0 x 0 = 0	0 x 0 = 0
0 x 1 = 0	0 x 1 = 1
1 x 0 = 0	1 x 0 = 1
1 x 1 = 1	1 x 1 = 1

ცალმხრივი ფუნქციის დაცვა:

დაცვის მეორე მეთოდად ცალმხრივი ფუნქციის დაცვა შეგვიძლია მივიჩნიოთ. როგორც ცნობილია v ვექტორზე მოკავშრე მხარეები თანხმდებიან წინასწარ, თუმცა შესაძლებელია რომ გადაცემამდე მესამე პირის მიერ მოხდეს ვექტორის შეცვლა და ამის შემდეგ უკვე ექნებათ რა სხვადასხვა სახის საწყისი ვექტორი ორივე მხარეს , მათ მიერ მიღებული საერთო გასაღებები იქნებიან ასევე სხვადასხვა, რაც შემდგომში გამოიწვევს შიფრაცია-დეშიფრაციის პრობლემას და შეუძლებელს გახდის მას. აღნიშნული პრობლემის აღმოსაფხვრელად ჩვენ ვიყენებთ დიფი-ჰელმანის ალგორითმს. აღნიშნული დაცვის მეთოდი შემდეგნაირად მუშაობს , ჩვენ მოვახდენთ გასაღებების გაცვლას დიფი-ჰელმანის ალგორითმის მეშვეობით, თუმცა გაცვლილ გასაღებებს გამოვიყენებთ საწყის v ვექტორად (აღსანიშნავია , რომ ანალოგიური მეთოდი გამოიყენა ელგამალმა 1985 წელს თავისი ცნობილი ციფრული ხელმოწერის ალგორითმის შესაქმნელად). დაცვის ეს მექანიზმი ორივე მხარეს დაარწმუნებს იმაში, რომ ისინი ერთიდაიმავე საწყისი მნიშვნელობით დაიწყებენ გამოთვლებს და შესაბამისად მიიღებენ ერთმანეთის ტოლ საერთო გასაღებებს და მოახდენენ შიფრაციასაც და დეშიფრაციასაც.

ეს მართალია დამატებით დროს მოითხოვს , თუმცა ეს დრო შეგვიძლია ვუგულებელყოთ, ვინაიდან ამ ოპერაციის ჩატარება მხოლოდ ერთჯერადად ხდება და ამ მეთოდით გადაგზავნილი v ვექტორის გამოყენება მრავალჯერ იქნება შესაძლებელი.

აღსანიშნავია , რომ ამ ეტაპზე ახალი მატრიცული ფუნქციის გატეხვის შემთხვევა არ დაფიქსირებულა.

2.5. რეალიზაციის მეთოდები

ახალი მატრიცული ალგორითმის პროგრამული რეალიზაცია მეტად მნიშვნელოვანი საკითხია აღნიშნული ალგორითმის ისტორიაში , რადგან შეიქმნა ინოვაციური პროდუქტი , რომელიც ახორციელებს არა მარტო გასაღებების შექმნას,

ასევე გასაღებების შესაქმნელად დახარჯული დროით ათვლას, დროის სტატისტიკურ ანალიზს და შედარებას დიფი-ჰელმანის ალგორითმთან. პროდუქტის ინოვაციურობა და უნიკალურობა მდგომარეობს იმაშიც, რომ აღნიშნული პროდუქტის შექმნის პრეცენდენტი ჯერ არ დაფიქსირებულა და ეს არის პირველი პროდუქტი.

პროგრამული რეალიზაციისათვის განხილული იყო რამოდენიმე მეთოდი, ასევე გამოკვლეული იქნა პროგრამული ბიბლიოთეკები, რათა ჩვენს მიერ მიღებული შედეგი ყოფილიყო საუკეთეო.

ჩვენი სამაგისტრო კვლევლი მიზანს პირველ რიგში ახალი მატრიცული ალგორითმის სწრაფქმედების გამოკვლება , მისი დამტკიცება და სხვა არსებული ალგორითმთან შედარებით მისი უპირატესობა იყო. ამის გამო საჭირო იყო პირველ რიგში გვეპოვა დიფი-ჰელმანის ალგორითმისთვის საუკეთესო რეალიზაციის მეთოდი, რათა ჩვენს მიერ მიღებული შედეგები ყოფილიყო ობიექტური და არ გვქონოდა მიკერძოებასთან საქმე. როგორც დიფი-ჰელმანის რეალიზაციისას ავღნიშნეთ , მივაკვლიეთ კიდეც ასეთ მეთოდს. ეს შედეგი ბუნებრივია, რადგან დიფი-ჰელმანის ალგორითმი უკვე 39 წელია არსებობს და მისი რეალიზაციისთვის მრავალი მეთოდი იქნებოდა გამოყენებული, გამოკვლეული და ჩვენც სწორედ საუკეთესო შევარჩიეთ, რომელზეც გვაქვს კიდეც საუბარი დიფი-ჰელმანის რეალიზაციისას.

რაც შეეხება ახალ მატრიცულ ალგორითმს , აქ ცოტა რთულად იყო საქმე, რადგან როგორც ვახსენე აღნიშნული პროდუქტი პირველია და უშუალოდ ამ ალგორითმზე მორგებული სისტემა აქამდე არ შექმნილა. ასე რომ საჭირო გახდა გამოგვეკვლია რამოდენიმე მეთოდი , რათა გავსულიყავით ჩვენს ხელთ არსებულ საუკეთესო შედეგებზე.

როგორც დიფი-ჰელმანის შემთხვევაში საჭირო იყო მოდულარული ახარისხების გამარტივებული მეთოდების მოძიება (რადგან დიფი-ჰელმანი იყენებს მოდულარულ ახარისხებას) , ჩვენს შემთხვევაში საჭირო იყო ვექტორის მატრიცზე

ნამრავლის ისეთი მეთდის პოვნა, რომელიც რასაკვირველია მოგვცემდა უკეთეს შედეგს ჩვენი სისტემისთვის.

2.5.1. კლასიკური მეთოდი:

ცნობილია, რომ ვექტორის მატრიცზე ნამრავლისას მიიღება იგივე განზომილების ვექტორი(ვექტორში ელემენტების რაოდენობა უნდა ემთხვეოდეს მატრიცში სტრიქონებისა და სვეტების რაოდენობას) კლასიკური მეთოდი მდგომარეობს შემდეგში:

ვექტორის პირველი ელემენტი მრავლდება მატრიცის პირველი სტრიქონის პირველ ელემენტზე, მეორე ელემენტი მატრიცის პირველი სტრიქონის პირველ ელემენტზე და ა.შ. მიღებული შედეგი შედეგები იკრიბება და დაიწერება შედეგი ვექტორის პირველ ელემენტად.

შემდეგ ვექტორი ანალოგიურად მრავლდებოდა მეორე სტრიქონზე და მიღებული შედეგი იწერებოდა მეორე ელემენტად და ა.შ.

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} \begin{pmatrix} a & b & c \\ x & y & z \\ k & l & m \end{pmatrix} = \begin{pmatrix} u*a+v*b+w*c \\ u*x+v*y+w*z \\ u*k+u*l+u*m \end{pmatrix}$$

თუმდა რასაკვირველია ეს მეთოდი არ არის ყველაზე ოპტიმალური ვექტორის მატრიცზე გადამრავლებისას , ამის გამო საჭირო გახდა სხვა მეთოდების გამოკვლევა.

2.5.2. ვექტორის მატრიცზე ნამრავლის მრავალნაკადიანი (Multithread) მეთოდი:

აღნიშნული მეთოდის იდეა წამოვიდა ნაკადური შიფრების ალგორითმებიდან. მრავალნაკადიანი მეთოდის მიზანი იყო კლასიკური მეთოდის მოდიფიცირება. კერძოდ ვექტორის ელემენტების გადამრავლება მატრიცის სტრიქონებზე უნდა მომხდარიყო ცალ-ცალკე პროგრამულ ნაკადში, თუმცა ამ მეთოდის გამოკვლევლისას წარმოიშვა გარკვეული პრობლემები, რის გამოც აღნიშნული მეთოდის გამოყენებაზე

უარი ითქვა. ამ პრობლემების წარმოსაჩენად პირველ რიგში ვთქვათ თუ რა არის მრავალნაკადური პროგრამირება. კომპიუტერულ არქიტექტურაში მრავალნაკადური პროგრამირება გულისხმობს პროცესების გადანაწილებას კომპიუტერის პროცესებზე, რათა გადანაწილებული პროცესები შესრულდეს ფაქტიურად პარალელურად. ანუ იმისათვის რომ აღნიშნულმა მეთოდმა მოგვცეს უკეთესი შედეგი, საჭიროა მრავალ ბირთვიანი კომპიუტერი , რომელსაც ბირთვების რაოდენობა პროცესებში შეუძლია აღნიშნული ამოცანის გადანაწილება. ამ დროს იქმნება ნაკადი , იწყებს გარკვეული ამოცანა მუშაობას და ისე რომ არ ელოდება აღნიშნული ამოცანის შესრულებას, პროცესორი იწყებს პირდაპირ ახალი ამოცანის ნაკადის შექმნას და შესაბამისად მის შესრულებას. მაგალთისთვის თუ ერთ ბირთვიან პროცესორით კლასიკურ მეთოდს ჭირდება n წამი , ორ-ბირთვიან პროცესორს დაჭირდება n/2 წამზე ოდნავ მეტი და ა.შ. ერთი შეხედვით ეს კარგი მეთოდია , მიუხედავად იმისა , რომ დამოკიდებულია კომპიუეტრის სიძლიერეზე , თუმცა კვლევისას გამოჩნდა ასევე სხვა პრობლემა , რამაც ხელი შეგვიშალა მრავალნაკადური პროგრამირების და სხვა,შემდგომში განხილულ მეთოდებთან კომბინირებაში, ეს არის ნაკადებად გადანაწილების დრო. კვლევებისას აღმოჩნდა , რომ ის დრო რომელიც ჭირდება ჩვენს შემთხვევაში ვექტორის ელემენტების კონკრეტული სტრიქონის ელემენტებზე გადამრავლებას, ნაკლებია იმ დროზე , რომელიც იგივე ამოცანისთვის ცალკე ნაკადის შექმნას ჭირდება. ანუ მიუხედავად ჩვენი სურვილისა არ გამოდიოდა ამოცანების გაპარალელება, არამედ მაინც ხდებოდა მათი მიმდევრობითი შერულება , რაც არანაირ მოგებას არ გვაძლევდა დროის თვალსაზრისით. სწორედ ამ პრობლემების გამო ითქვა უარი აღნიშნულ მრავალნაკადიან მეთოდზე.

2.5.3. შტრასენის ალგორითმი

1969 წელს ვოლკერ შტრასენმა გამოაქვეყნა მატრიცთა გადამრავლების ახალი ალგორითმი და დაამტკიცა, რომ მატრიცების გადამრავლების კლასიკური ალგორითი, რომელიც იყო $O(n^3)$ რიგის არ იყო ოპტიმალური . როგორც ვიცით

მატიცთა გადამრავლებისთვის საჭიროა შეკრებისა და გამრვალების ოპერაციათა ერთობლიობა. იმის გამო , რომ გამრავლების ოპერაცია უფრო რთული ოპერაციაა ვიდრე შეკრების, ამისთვის შტრასენმა მიზნად დაისახა გადამრავლების ალგორითმში გადამრავლებების რაოდენობის შემცირება. მაგალითისთვის მოვიყვანოთ პირველ რიგში 2x2 მატრიცი:

კლასიკური მეთოდი :

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_{1,1} & \mathbf{A}_{1,2} \\ \mathbf{A}_{2,1} & \mathbf{A}_{2,2} \end{bmatrix}, \mathbf{B} = \begin{bmatrix} \mathbf{B}_{1,1} & \mathbf{B}_{1,2} \\ \mathbf{B}_{2,1} & \mathbf{B}_{2,2} \end{bmatrix}, \mathbf{C} = \begin{bmatrix} \mathbf{C}_{1,1} & \mathbf{C}_{1,2} \\ \mathbf{C}_{2,1} & \mathbf{C}_{2,2} \end{bmatrix}$$

ორი A და B მატრიცების გადამრავლებისთვის გვჭირდება შემდეგი ოპერაციები :

$$\begin{aligned} \mathbf{C}_{1,1} &= \mathbf{A}_{1,1}\mathbf{B}_{1,1} + \mathbf{A}_{1,2}\mathbf{B}_{2,1} \\ \mathbf{C}_{1,2} &= \mathbf{A}_{1,1}\mathbf{B}_{1,2} + \mathbf{A}_{1,2}\mathbf{B}_{2,2} \\ \mathbf{C}_{2,1} &= \mathbf{A}_{2,1}\mathbf{B}_{1,1} + \mathbf{A}_{2,2}\mathbf{B}_{2,1} \\ \mathbf{C}_{2,2} &= \mathbf{A}_{2,1}\mathbf{B}_{1,2} + \mathbf{A}_{2,2}\mathbf{B}_{2,2} \end{aligned}$$

ანუ გამოიყენება რვა გამრავლების ოპერაცია.

შტრასენის ალგორითმი კი გულისხმობს გამრავლებებოს რაოდენობის შვიდამდე დაყვანას, ამას კი შემდეგნაირად ახერხებს :

$$\begin{aligned} \mathbf{M}_1 &:= (\mathbf{A}_{1,1} + \mathbf{A}_{2,2})(\mathbf{B}_{1,1} + \mathbf{B}_{2,2}) \\ \mathbf{M}_2 &:= (\mathbf{A}_{2,1} + \mathbf{A}_{2,2})\mathbf{B}_{1,1} \\ \mathbf{M}_3 &:= \mathbf{A}_{1,1}(\mathbf{B}_{1,2} - \mathbf{B}_{2,2}) \\ \mathbf{M}_4 &:= \mathbf{A}_{2,2}(\mathbf{B}_{2,1} - \mathbf{B}_{1,1}) \\ \mathbf{M}_5 &:= (\mathbf{A}_{1,1} + \mathbf{A}_{1,2})\mathbf{B}_{2,2} \\ \mathbf{M}_6 &:= (\mathbf{A}_{2,1} - \mathbf{A}_{1,1})(\mathbf{B}_{1,1} + \mathbf{B}_{1,2}) \\ \mathbf{M}_7 &:= (\mathbf{A}_{1,2} - \mathbf{A}_{2,2})(\mathbf{B}_{2,1} + \mathbf{B}_{2,2}) \end{aligned}$$

ანუ შეკრება-გამოკლებისა და შვიდი გამრავლების გამოყენებით ითვლის შვიდ მნიშვნელობებს, ხოლო შემდეგ ასევე ამ შვიდი მნიშვნელობებით იღებს მატრიცთა ნამრავლს :

$$\begin{aligned} \mathbf{C}_{1,1} &= \mathbf{M}_1 + \mathbf{M}_4 - \mathbf{M}_5 + \mathbf{M}_7 \\ \mathbf{C}_{1,2} &= \mathbf{M}_3 + \mathbf{M}_5 \\ \mathbf{C}_{2,1} &= \mathbf{M}_2 + \mathbf{M}_4 \\ \mathbf{C}_{2,2} &= \mathbf{M}_1 - \mathbf{M}_2 + \mathbf{M}_3 + \mathbf{M}_6 \end{aligned}$$

ეს იყო თითქოს ერთ-ერთი კერძო შემთხვევა , თუმცა ზოგადად აგორითმის პრინციპი გულისხმობს იმას, რომ მრავალგანზომილებიანი მატრიცების შემთხვევაში ხდება მატრიცების რეკურსიული დაყოფა იმგვარად, რომ საბოლოო ჯამში ვიღებთ აღნიშნულ შემთხვევებზე გამოთვლებს.

აღნიშნულმა ალგორითმმა შემდგომში მოიპოვა განვითარება დონ კოპერსმიტის და სამუელ ვინოგრადის მიერ, რამაც საბოლოოდ მატრიცთა გადამრავლება დაიყვანა $O(n^{2,37})$ რიგის ალგორითმად.

ჩვენს შემთხვევაში საჭირო იყო შტრასენის ალგორითმის კერძო შემთხვევა, რომელიც მოიცავდა ვექტორის მატრიცზე ნამრავლს. აღნიშნული პრობლემის გადასაწყვეტად მოვიძიეთ და გამოვიკვლიეთ პროგრამული ბიბლიოთეკები. ძიების შედეგად აღმოვაჩინეთ პროგრამული ბიბლიოთემა BLAS (Basic Linear Algebra Subprograms) , რომელიც იყენებს შტრასენის (შემდგომში კოპერსმიტ-ვინოგრადის) ალგორითმს. აღნიშნულ ბიბლიოთეკას გააჩნია სამი დონე , პირველი დონე მოიცავს ვექტორთა ურთიერთქმედების ოპერაციებს , მეორე დონე ვექტორის და მატრიცის უერთიერთქმედების ოპერაციებს , ხოლო მესამე დონე მატრიცთა ურთიერთქმედების ოპერაციებს. ჩვენ გვჭირდებოდა მეორე დონე, გამოვიყენეთ კიდეც მასში განსაზღვრული ვექტორის მატრიცზე ნამრავლი და მივიღეთ საკმაოდ კარგი შედეგი, თუმცა ჩვენ აღნიშნულ შედეგზე არ გავჩერებულვართ , გავაგრძელეთ კვლევა და აღმოვაჩნეთ ახალი მეთოდი, რომელმაც ამ დროისათვის მოგვცა საუკეთესო შედეგი. ამ მეთოდს „ოთხი რუსის მეთოდი“ ქვია.

2.5.4. ოთხი რუსის მეთოდი

1970 წელს ვ.ლ.არლაზაროვმა, ე.ა.დინიკმა, მ.ა.კრონროდმა და ი.ა.ფარადზევმა წარმოადგინეას მატრიცთა გადამრავლების ალგორითმი, რომელიც შემდგომში ოთხი რუსის ალგორითმი ეწეოდა, მიუხედავად იმისა , რომ აღნიშნული ავტორებიდან მხოლოდ ორის შესახებ (არლაზაროვი , კრონროდი) არის ცნობილი, რომ ისინი დანამდვილებით რუსები იყვნენ.

ალგორითმი მუშაობს მხოლოდ ბულის მატრიცებზე (რომელის ელემენტები არიან მხოლოდ 0 ან 1) და იმის გათვალისწინებით, რომ ახალი მატრიცული ალგორითმის განსაზღვრულია GF(2) ველზე , ჩვენ მისი გამოყენება თავისუფლად შეგვიძლია.

მოცემული გვაქვს ორი ბულის მატრიცი , მათი გადამრავლებისის კლასიკური მეთოდისგან განსხვებით,რომელიც იყენებს შეკრებას და გამრავლებას, იგი დაიყვანება შედარების და XOR ოპერაციებზე.

ოთხი რუსის მეთოდი შემდეგნაირია:

ორი , ტოლგანზომილებიანი, კვადრატული მატრიცის (პირობითად A და B) გამრავლებისას შედეგში ვღებულობთ იგივე განზომილებებიან კვადრატულ მატრიცს (პირობითად C), რომელშიც იქნება სვეტები და სტრიქონები. გამრავლებისას ჯერ ვიღებთ A მატრიცის პირველ სტრიქონს და ვამრავლებთ მასზე მეორე, B მატრიცს , მიღებულ შედეგს კი ვწერთ C მატრიცის პირველ სტრიქონად. თვითონ ვექტორის მატრიცზე ნამრავლი ხდება შემდეგნაირად : თუ A მატრიცის პირველი სტრიქონის (ვექტორის) i-ური ელემენტი 1 - ის ტოლია , B მატრიცის შესაბამის i-ურ სტრიქონს ვტოვებთ „ხელუხლებლად“ , ხოლო თუ A მატრიცის პირველი სტრიქონის (ვექტორის) i-ური ელემენტი 0 - ის ტოლია , B მატრიცის შესაბამის i-ურ სტრიქონს „ვშლით“. ამის შემდეგ ვიღებთ ყველა „ხელუხლებელ“ სტრიქონებისთვის სრულდება XOR ოპერაცია და მიღებული შედეგი ჩაიწერება სწორედ C მატრიცის შესაბამის სტრიქონად. ამ პროცედურებს ვიმეორებთ იმდენჯერ, რამდენი სტრიქონიც გვექნება A მატრიცში.

დავუშვათ გვაქვს შემდეგი მატრიცები:

$$A = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix} B = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

C მატრიცის პირველი პირველი სტრიქონი გამოითვლება შემდეგნაირად:

რადგან A მატრიცის პირველი სტრიქონის მხოლოდ მესამე და მეხუთე ელემენტებია 1 - ის ტოლი, XOR ოპერაცია შესრულდება მხოლოდ B მატრიცის მესამე და მეხუთე სტრიქონებისთვის :

0	1	1	0	1
XOR				
1	1	0	0	1
=				
1	0	1	0	0

ჩვენს შემთხვევაშიც აღნიშნული მეთოდის სწორედ ერთი ნაწილი გამოიყენება, კერძოდ ვექტორის მატრიცზე ნამრავლი.

მისი სწრაფქმედება თავიდანვე ჩანს , ვინაიდან განსხვავებით კლასიკური ვექტორის მატრიცზე ნამრავლისგან , გვაქვს მხოლოდ შედარების(რიცხვი არის 1 თუ 0) და სტრიქონების XOR ოპერაცია.

კვლევების , ძიების და პროგრამული მოდულის შექმნის შედეგად, მივიღეთ ჩვენთვის მისაღები შედეგი , კერძოდ ახალმა მატრიცულმა ალგორითმმა მოახდინა გასაღებების გამოთვლა უფრო სწრაფად, ვიდრე ამას აკეთებდა დიფი-ჰელმანის ალგორითმი.

ჩვენს წინაშე უკვე დადგა არა ის საკითხი , რომ გვეპოვნა მატრიცის ვექტორზე გადამრავლების სწრაფი მეთოდი, არამედ ის , თუ როგორ მოგვეხერხებინა , რომ ორ ვექტორს შორის ჩაგვეტარებინა XOR ოპერაცია უფრო სწრაფად. ჩვენ მივკავლიეთ კიდეც ერთ-ერთ პროგრამულ ბიბლიოთეკას (BitArray), რომელშიც განსაზღვრულია XOR - ის ფუნქცია და იგი მუშაობს იმდენად სწრაფად, რომ ახალი მატრიცული ალგორითმი ორი საერთო (და შესაბამისად საერთო) გასაღებისთვის გამოთვლას საშუალოდ ანდომებს 0.000006 წამს (53x53 მატრიცების შემთხვევაში) , განსხვავებით დიფი ჰელმანის ალგორითმისა , რომელიც (p=900719925474088 1 , 2^{53} - ზე ნაკლები პირველი მატრივი რიცხვი) გასაღებების გამოთვლისთვის ხარჯავს საშუალოდ 0.0001146 წამს. ანუ ეს გვაძლევს ამ ეტაპისთვის საკმარის შედეგს იმისთვის, რომ დავრწმუნდეთ ახალი მატრიცული ალგორითმის სწრაფქმედებაში.

მიუხედავად ჩვენი მცდელობისა კიდევ უფრო გაგვეუმჯობესებინა ჩვენს მიერ მიღებული შედეგი, არსებული მომენტისთვის უკეთესი შედეგის პოვნა სამწუხაროდ ვერ მოხერხდა. თუმცა მიღებული შედეგი , ჩვენის აზრით, ამ ეტაპისთვის , როდესაც პირველად მოხდა ახალი ალგორითმის ბაზაზე პროგრამული პროდუქტის შექმნა, სავსებით საკმარისია.

2.5.5. პროგრამული რეალიზაციის შესახებ

ახალი მატრიცული ალგორითმის რეალიზაციაში , გამოვიყენეთ ზემთხსენებული „ოთხი რუსის მეთოდი“, რომლის საშვალებითაც ასევე ვითვლით შესაბამის K_1 და K_2 გასაღებებს, ვაჩვენებთ მათ და სურვილის შემთხვევაში ვინახავთ კიდეც, ასევე ვითვლით ამ გასაღებების დათვლისთვის დახარჯულ დროს.

სტატისტიკური ნაწილი წარმოადგენს შედარებით გრაფიკს დიფი-ჰელმანის ალგორითმისთვის და ახალი მატრიცული ალგორითმისთვისაც, (გრაფიკზე ნაჩვენებია ალგორითმების მრავალჯერ მუშაობის შედეგად დახარჯული დროები, რიგითობის მიხედვით) რათა უკეთ დავინახოთ განსხვავება ამ ორი ალგორითმის მუშაობის შესრულებულ დროზე. ასევე ეს ნაწილი აჩვენებს ოირვე ალგორითმის შერულებულ მინიმალურ, მაქსიმალურ და საშუალო დროებს.

მთელი პროგრამული რეალიზაცია დაწერილია ენაზე C# და დაკომპილირებულია პროდუქტში Visual Studio 2013 ოპერაციულ სისტემაზე Windows. გრაფიკის რეალიზებისთვის გამოყენებულია DevExpress 14.1.2. ვერსია. პროგრამის გასაშვებად საჭიროა, რომ კომპიუტერზე იყოს დაინსტალირებული Framework .NET 4.5. ასევე მონაცემთა ბაზისთვის გამოყენებულია MsSQL Server 2012 - ს კომუტატიური მატრიცთა კლასის ჯგუფის ჩასაწერად.

დასკვნა

წინამდებარე სამაგისტრო ნაშრომში განხილული იქნა ახალი მატრიცული ცალმხრივი ფუნქციისა და ღია არხით გასაღების გაცვლის ალგორითმის ანალიზი და მისი ინოვაციური განხორციელება. ნაშრომში შემოტანილი და განხილულია ახალი მატრიცული ცალმხრივი ფუნქცია და მის საფუძველზე შექმნილი ალგორითმის თვისებები.

ნაშრომში განხილულია დიფი-ჰელმანის ალგორითმი, მისი თვისებები და ნაჩვენებია მისი რეალიზაციისთვის ჩვენს ხელთ არსებული საუკეთესო მეთოდი.

ნაშორმში განხილულია ახალი მატრიცული ფუნქციის რამოდენიმე რეალიზაციის მეთოდი, რომელთა მოძიება და გამოკვლევა მოხდა ნაშორმის შესრულების პერიოდში. მოყვანილი და განხილულია კლასიკურ მეთოდზე დაფუძნებული რეალიზაციის ვერსია, თუმცა დასაბუთებულია მისი არაოპტიმალურობის მეცნიერული დასაბუთება შტრასენის ალგორითმის საშუალებით. რაც შეეხება შტრასენის ალგორითმს , აღნიშნულია როგორ თვითონ ალგორითმის , ასევე მასზე დაფუძნებული პროგრამული ბიბლიოთეკის (BLAS) ის დადებითი მხარე, რომელიც ასე საჭიროა აღნიშნული პრობლემის გადასაწყვეტად. ასევე მოყვანილი მატრიცთა გადამრავლების მრავალნაკადური მეთოდი და არგუმენტირებულია ჩვენს მიერ მისი არგამოყენების მიზეზი და საბოლოოდ მოყვანილი, განმარტებული და დასაბუთებულია „ოთხი რუსის მეთოდი“, მისი დადებითი მხარეები არამარტო მატრიცთა გადამრავლების, არამედ ახალი მატრიცული ფუნქციის რეალიზაციის საკითხში.

ნაშრომის ძირითად მიზანს წარმოადგენდა თანამედროვე კრიპტოგრაფიაში უდიდესი გამოწვევის, სწრაფი ასიმეტრიული კრიპტოსისტემების შექმნის

დაძლევისადმი პირველი ნაბიჯის გადადგმა და ეს უდიდესი ნაბიჯი უდაოდ შეგვიძლია მივიჩნიოთ გადადგმულად , ვინაიდან მივიღეთ ალგორითმი რომელიც გასაღებების გამოთვლას ასრულებს საშუალოდ დაახლოებით 0,000006 წამში , ეს შედეგი კი დიფი-ჰელმანის ალგორითთან შედარებით , რომელიც გასაღებების გამოთვლას დაახლოებით 0.0001146 წამს ანდომებს, დაახლოებით 20 ჯერ სწრაფ შედეგს გვაძლევს. აღნიშნული მონაცემებით ჩვენ თამამად შეგვიძლია ვთქვათ, რომ წარმოვადგენთ დღეისათვის, სწრაფქმედების თვალსაზრისით, საუკეთესოს თუ არა ერთ-ერთ საუკეთესო კრიპტოგრაფიულ, გასაღებების გაცვლის ალგორითმს.

გამოყენებული ლიტერატურა

1. R.Megrelishvili, M. Chelidze, K. Chelidze, on the construction of secret and public-key cryptosystems, Iv. Javakhishvili Tbilisi State University I.Vekua Institute of Applied Mathematics, Applied Mathematics, Informatics and Mechanics, AMIM, v.11, N2, 2006, pp. 29-36.
2. Shneier .B, "Applied Cryptography", Wiley, 1995, pp. 37 – 39.
3. Diffie W. and Hellman M.E., "New Directions in Cryptography.IEEE Transactions on Information Theory", v. IT-22, n.6, Nov, 1976, pp. 644-654.
4. R.L. Rivest, A. Shamir, and L.M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, v. 21, n. 2, Feb 1978, pp. 120-126.
5. Megrelishvili R., Sikarulidze A. New matrix-sets generation and the cryptosystems. Proceedings of the European Computing Conference and 3 rd International conference on Computational Intelligence, Tbilisi, Georgia, June, 26-28, 2009, pp. 253-255.
6. Megrelishvili R., Chelidze M., Besiashvili G.Investigation of new matrix-key function for the public cryptosystems. The Third International Conference "Problems of Cybernetics and Information", Volume 1, September 6-8, Baku, Azerbaijan, 2010, pp. 75-78.
7. Shneier B., "Applied Cryptography", Wiley, 1995, pp. 430 – 432.
8. The Codebreakers, David Kahn, 1967, pp. 192–195
9. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. Introduction to Algorithms, Second Edition. MIT Press and McGraw-Hill, 2001. ISBN 0-262-03293-7. Chapter 28: Section 28.2: Strassen's algorithm for matrix multiplication, pp. 735-741
10. Bard, Gregory V. (2009), Algebraic Cryptanalysis, Springer, ISBN 978-0-387-88756-2

11. Dennis W. Ross, "Morse Code: A Place in the Mind," QST, March, 1992, p. 51
12. Knuth, Donald (2008). Seminumerical Algorithms. The Art of Computer Programming 2 (3rd ed.). Addison-Wesley. ISBN 0-201-89684-2{{inconsistent citations}}, Section 4.3.1: The Classical Algorithms
13. Singh, Simon (1999). The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. London: Fourth Estate. p. 127. ISBN 1-85702-879-1.
14. An interview with Jack J. Dongarra Conducted by Thomas Haigh on 26 April, 2004 University of Tennessee, Knoxville, TN Interview conducted by the Society for Industrial and Applied Mathematics, as part of grant # DE-FG02-01ER25547 awarded by the US Department of Energy.
15. R.P.Megrelishvili, Analysisi of the Matrix One-way Function and two vaiants of its implementations. International Journal of Multidisciplinary Research and Advances in Engineergin(IJMRAE) , Vol.5 .No IV (October 2013) , pp.99-105.