გულნარა კოტრიკაძე

ინფორმაციის დაცვა კომპიუტერულ სისტემებში

წარმოდგენილია დოქტორის აკადემიური ხარისხის
მოსაპოვებლად

საქართველოს ტექნიკური უნივერსიტეტი
თბილისი, 0175, საქართველო
დეკემბერი, 2008

საქართველოს ტექნიკური უნივერსიტეტი

ინფორმატიკისა და მართვის სისტემების ფაკულტეტი

ჩვენ, ქვემორე ხელისმომწერნი ვადასტურებთ, რომ გავეცანით გულნარა კოტრიკაძის მიერ შესრულებულ სადისერტაციო ნაშრომს დასახელებით: ინფორმაციის დაცვა კომპიუტერულ სისტემებში და ვაძლევთ რეკომენდაციას საქარველოს ტექნიკური უნივერსიტეტის ინფორმატიკისა და მართვის სისტემების ფაკულტეტის სადისერტაციო საბჭოში მის განხილვას დოქტორის აკადემიური ხარისხის მოსაპოვებლად.

თარიღი

ხელმძღვანელი: _____

რეცენზენტი: _____

რეცენზენტი: _____

რეცენზენტი: _____

საქართველოს ტექნიკური უნივერსიტეტი

2008

ავტორი: კოტრიკაძე გულნარა

დასახელება: ინფორმაციის დაცვა კომპიუტერულ სისტემებში

ფაკულტეტი : ინფორმატიკისა და მართვის სისტემების

ხარისხი: დოქტორი

სხდომა ჩატარდა: თარიღი

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

ნაშრომში “ინფორმაციის დაცვა კომპიუტერულ სისტემებში” წარმოდგენილია და აღწერილია კრიპტოგრაფიის ორიგინალური მეთოდი.

ამ მეთოდის მისაღებად, დამუშავებულ იქნა შესაბამისი მასალა, ისეთი როგორიცაა:

კრიპტოგრაფიის **სიმეტრიული და ასიმეტრიული** სისტემების ყველა არსებული მეთოდები, ანუ დახურული და ღია არხები, მათი გამოყენების არეალი, როგორც პრაქტიკულ ასევე სამხედრო სამსახურში.

სიმეტრიული სისტემის დროს, საიდუმლო გასაღების გაცვლა ხორციელდება დახურული არხით, ანუ კურიერის გამოყენებით. ორმა კანონიერმა მომხმარებელმა იცის გასაღები, შემდგომ ამ გასაღებით ერთ-ერთი მომხმარებელი დაშიფრავს ინფორმაციას და შესაბამისად მეორე კი – გაშიფრავს.

განხილულ იქნა სიმეტრიული სისტემის მეთოდები:

1. ცეზარის ალგორითმი – გასაღები შეადგენს ერთ სიმბოლოს და ყოველ სიმბოლოს შეესაბამება ანბანის რიგითი ნომერი.

2. ვიჟინერის ალგორითმი – გასაღების სიგრძე არის სამის ტოლი. გასაღების სიგრძე გაიზარდა, რამაც გამოიწვია ინფორმაციის დაყოფა ბლოკებად, ალგორითმი შესაბამისად უფრო გართულდა. ამ ალგორითმშიც ყოველ სიმბოლოს შეესაბამება ანბანის რიგითი ნომერი.

3. ვერნამის ალგორითმი – არის ვიჟინერის მეთოდში გამოყენებული ალგორითმის ფართო სპექტრი. ანუ ვერნამის ალგორითმი გამომდინარეობს ვიჟინერის ალგორითმიდან. n სიგრძის სრული ტექსტი იშიფრება მისი ტოლი L სიგრძის საიდუმლო გასაღებით, ე.ი. L=n.

ასიმეტრიული სისტემის დროს, გასაღების მიღება ორ კანონიერ მომხმარებელს შორის ხდება ღია არხით, კურიერის ანუ მესამე პირის ჩარევა არ არის საჭირო. შესაბამისად ინფორმაციის დაშიფვრა, გაგზავნა და გაშიფვრაც ხდება სრულიად ღიად.

განხილულ იქნა ასიმეტრიული სისტემის მეთოდები:

1. დიფი-ჰელმანის ალგორითმი – ალგორითმი ეყრდნობა GF(P) ველში ლოგარითმის გამოთვლის სირთულეს, გამოყენებულია ახარის-

ხება საიდუმლო ნატურალური რიცხვებით, რომელსაც ირჩევს ორივე მხარე საიდუმლოდ. საბოლოოდ ორივე მხარე იღებს ერთიდაიგივე გასაღებს. შემდგომში ერთ-ერთი დაშიფრავს ინფორმაციას მიღებული გასაღებით და მეორე კი – გაშიფრავს. ამ მეთოდის საიმედოობა ეფუძნება სწორედ აღნიშნული საიდუმლო ნატურალური რიცხვების ამოცნობის სირთულეს.

2. რაივესტ-შამირ-ეიდელმანის ალგორითმი – ალგორითმი ეყრდნობა ეილერის ცნობილ თეორემას: $\Phi(N)=(p-1)(q-1)$, p და q საიდუმლო რიცხვებია.

3. ელგამალის ალგორითმი – გამოიყენება ციფრული ხელმოწერისათვის. ტექსტის დაშიფრვა არ ხდება, მაგრამ მას დაემატება S, R პარამეტრები, რომლებიც წარმოადგენენ ციფრულ ხელმოწერას.

სიმეტრიული მეთოდების მახასიათებლებია: მაღალი შიფრაციის სიჩქარე, რადგან გამოყენებულია გადანაცვლება-ჩანაცვლების ფუნქციები; გასაღების სიგრძე დაბალი; კრიპტოსირთულეს წარმოადგენს გასაღების გადარჩევა მთელ სივრცეში; გასაღების გენერაციის დრო მილიწამები, მაგრამ სამაგიეროდ **ასიმეტრიული** მეთოდები ხასიათდება უფრო მაღალი საიმედოობით. სიმეტრიულ მეთოდებში სიჩქარე მაღალია, გამოიყენება გადანაცვლების ფუნქცია და ა.შ., ხოლო ასიმეტრიულ მეთოდებში კი სიჩქარე დაბალია, სამაგიეროდ გამოიყენება ახარისხების ფუნქცია, რაც იძლევა მაღალ საიმედოობას.

ჩვენს მიერ მიღებულ იქნა სხვადასხვა მეთოდები, როგორც სიმეტრიული ასევე ასიმეტრიული მეთოდის გამოყენებით, ანუ მოხდა არსებული მეთოდების სინთეზი და მივიღეთ ახალი ორიგინალური მეთოდები.

მიღებულ იქნა შემდეგი შედეგები:

- **ასიმეტრიული მატრიცული მეთოდი**. დიფი-ჰელმანის მეთოდის გამოყენებით, შეიქმნა ახალი მეთოდი, ოღონდ ახარისხება შეცვლილი იქნა მატრიცაზე გამრავლებით. ვექტორი და მატრიცათა სიმრავლე, საიდანაც ხდება ამ მატრიცათა ამორჩევა, არის ყველასათვის ხელმისაწვდომი.

- **სიმეტრიული და ასიმეტრიული მეთოდების სინთეზი**. ვექტორი, რომელიც წინა მეთოდში იყო ყველასათვის ცნობილი, ამ შემთხვევაში დავასაიდუმლოვეთ და შედეგმაც არ დააყოვნა. მატრიცის განზომილება გახდა უცნობი და აქედან გამომდინარე სხვა სუბიექტი (ჰაკერი, არაკანონიერი მომხმარებელი) ვერ მოახერხებს ინფორმაციის დაყოფას ბლოკებად და შესაბამისად გაშიფვრას. თუმცაღა, აღნიშნული, არც პირველ მეთოდშია შესაძლებელი, მაგრამ ამ მეთოდში მედეგობა უფრო მაღალია.

- **მატრიცის დასაიდუმლოება**. ვექტორთან ერთად საიდუმლოდ ავიღეთ მატრიცაც, ანუ კურიერის სახით ხდება მათი გაცვლა და შემდგომ ორივე მხარეს გასაღების მიღება, ამით გასაღების გენერაციის დრო შემცირდა, ანუ საბოლოო ჯამში შიფრაციის სიჩქარე გაიზარდა.

- **სხვადასხვა სახის მატრიცათა განხილვა**. აღნიშნული მეთოდის საიმედოობისათვის, განვიხილეთ სხვადასხვა მოდულისა და განზომილების მქონე მატრიცები, როგორც ორობითი ასევე ათობითი.

- **კომუტატიურ მატრიცათა სიმრავლის აგება**. გალუას $GF(p^m)$ ველებზე დაყრდნობით მოვახდინეთ $(m\times n)$ კომუტატიურ-კვადრატულ მატრიცათა სიმრავლის აგება, ანუ $A_1\times A_2=A_2\times A_1$, როგორც ორობით ასევე ათობით ველზე.

- **მიღებული მეთოდის საიმედოობა**. განვიხილეთ მატრიცათა სიმრავლე, რომელიც რიცხობრივად შეადგენს $M^{m\times n}$, სადაც $m=n$ – სვეტებისა და სტრიქონების რაოდენობა, რადგან აღნიშნულ მეთოდში გამოიყენება კვადრატული მატრიცები; ხოლო M არის მატრიცაში შემავალი ელემენტების სიდიდე. მიღებული მეთოდის კრიპტოსირთულე ეფუძნება ამ სიმრავლიდან მატრიცათა ამორჩევის სირთულეს.

სიმეტრიული და ასიმეტრიული სისტემების სინთეზი გვაძლევს საიმედო შედეგს, რომელიც გამოირჩევა მაღალი მედეგობით.

მიუხედავად იმისა, რომ ყველა სიდიდე ცნობილია გარდა იმ ორი კონკრეტული მატრიცისა, ამ მეთოდის გატეხვა, შეუძლებელია არაკანონიერი მომხმარებლის მიერ.

მაშასადამე, ამ მეთოდის მაღალი მედეგობა ეფუძნება A_1 და A_2 მატრიცათა ამორჩევის სირთულეს, მოცემული მატრიცათა სიმრავლიდან.

აქვე უნდა აღინიშნოს ის ფაქტი, იმისათვის რომ ზემოთ აღნიშნული მეთოდები იყოს საიმედო და გამოირჩეოდეს მაღალი მედეგობით, **აუცილებელია და საკმარისი**, რომ მატრიცები იყოს **კომუტატიური** ანუ გადასმადი.

აღნიშნული მეთოდის მიღებისათვის, დამუშავებული და მიღებული იქნა **კომუტატიურ მატრიცათა სიმრავლე**, რომელიც გამოიყენება გასაღების მიღებისათვის, რათა შემდგომ მოხდეს ამ გასაღებით ინფორმაციის დაშიფვრა და შემდგომ გაშიფვრა.

კომუტატიური მატრიცების აგება ადვილად ხორციელდება. A და B მატრიცები არიან კომუტატიური, თუ A მატრიცას ნამრავლი B მატრიცაზე მარცხნიდან უდრის B მატრიცას ნამრავლს A მატრიცაზე მარჯვნიდან, მაშინ შეგვიძლია ვთქვათ, რომ AB=BA. გარდა ამისა, თუ ავიღებთ რაიმე მატრიცას და გავამრავლებთ საკუთარ თავზე, მიღებული მატრიცა და საწყისი მატრიცა არის კომუტატიური მატრიცები. გარდა აღნიშნულისა უნდა აკმაყოფილებდნენ გარკვეულ თვისებებს, რომლებიც აღწერილია მესამე თავში.

მატრიცათა სიმრავლე არის მატრიცათა ველი, ჩაკეტილი სიმრავლე. ანუ ორი მატრიცის გამრავლებით მივიღებთ ისეთ მესამე მატრიცას, რომელიც მოთავსებულია ამავე მატრიცათა სიმრავლეში.

... და ბოლოს, მიღებული ახალი მეთოდები, მიეკუთვნება ასიმეტრიულ მეთოდს და გამოირჩევა **მაღალი საიმედოობით**.

კრიპტოსირთულეს წარმოადგენს მატრიცათა სიმრავლიდან ამორჩევის სირთულე, რასაც ემყარება მიღებული მეთოდების საიმედოობა.

ყოველივე ზემოთ აღნიშნული – აღწერილია, განხილულია თითოეული მეთოდი, მოყვანილია მაგალითები, ცხრილები, ნახაზები, დანართები, ყოველი თავის შემდეგ მოცემულია დასკვნები, ასევე საბოლოო დასკვნა.

Abstract

In the article “information defence in computer sistems” is described and presented original method of cryptography.

To recieve this method lots of materials were proceeded, such as: all this exsisted methods of **symmetrical and asymmetrical** sistems of cryptography, closed and opened channels, the areal of their use, as in practical as well as in military service.

To receive the above mentioned method, **commutational matrix multiply** was processed and received. Which is used to receive key. In order to happen ciphering with the help of the key.

In symmetrical system, the exchange of the secret key is executed by closed channel or; by use of courier. Two legitimate users know the key, with this key one of the users ciphers information and the second – codes.

Symmetrical system methods were examined:

1. **Tsezar algorithm** – The key contains one symbol and every symbol is corresponding to the ordinal number of alphabet.
2. **Vijiner algorithm** – The length of the key is three. The key length has grown and this provoked spacing out information into blocks, accordingly algorithm became more complicated. Every symbol is corresponding to the ordinal number of alphabet in this algorithm.
3. **Vernam algorithm**- There is used wide spectre of algorithm in Vijiner method, or Vernam algorithm follows that Vijiner algorithm. The complete text of n length is coding with its equal L length secret key, i.e L=n.

In asimmetrical system, receiving key between two users is accomplished by opened channel, the third person does not need interfering. Accordingly, ciphering of information, sending and coding is happening quite openly.

Asimmetrical system methods were examined:

1. **Dipi-Helman algorithm –** Algorithm is based on GF(P) field, the complication of logaritm calculation, there are used raising to the

power with the secret natural numbers, which two users select them secretly. Finally the both sides receive the same key. Afterwards one of the users will cipher information with the received key, and the second – will code it. The reliability of this method is based on complication of the marked secret natural recognition numbers.

2. **Raivest-Shamir-Fidelman algorithm** – Algorithm is based on well – known Filer's theorem: $\phi(N)=(p-1)(q-1)$, p and q are secret numbers.
3. **Elgamal algorithm –** It is used for digital signature. Text ciphering is not happening, but S, R parameters will be added, which are digital signature.

Symmetrical methods definitions are: High speed code, because there are used the function of shifting and insertion; the length of the key – low; cryptocomplication is to reselect the key into whole space; key generation is milisecond, but instead of **asymmetrical methods** are charecterized higher reliabilities. Speed is high in symmetrical methods, there is used shifting of function and so on, but speed is low in asymmetrical methods, instead of there is used the method of raising to the power, which gives high reliability.

With the use of symmetrical and asymmetrical methods is received various methods. After the synthesis of mathods we got new original method.

The following results are received:

- **Asimmetrical matrix method**. With the use of Dip-Helman's method was created the new method, but raise to the power was changed by multipling on matrix. Vector and matrix multiplication from where happens matrix choosen is available for everybody.
- **Synthesis of symmetrical and asymmetrical methods**. The vector that was known to everybody in the previous method in this case we have kept it in secret and the result didn't deley. The dimention of matrix became unknovn and another subject (haker, illegal user) will not manage to understand or devide information into the blocks. Although the mantioned fact isn't available in the first

method too, but the results in this method is higher quality than in a privious one.

- **Secrecy of matrix**. We took matrix with the vector in secrecy. With the help of courier happens exchange of following and receiving the key later on both side. With this the time of generation is reduced.
- **Discussion of various kinds of matrix**. For the reliability of this method, we have discussed matrix of defferent module and dimensions as bisection as well as decimal field.
- **Building comutational matrix multiply**. Depending on Galua's $GF(p^m)$ fields we got $(m \times n)$ construction of squared comutational matrix multiply. $A_1A_2=A_2A_1$ as bisectional as well as decimal field.
- **Safety of the received method**. We have discussed multipling of matrix, wich consists of $M^{n \times n}$ were the amount of columns and lines m=n as in the mantioned method squared matrix are used. M is the input size of matrix. The complexity of cryptography is based on complexity of the choosen matrix from multipling.

The results of the synthesis of symmetrical and asymmetrical sistemsare reliable, wich is different for its high quality.

In spite of all the known quqntities except those concriete matrix, braking this method is unavailable by the illegal user.

There-fore high quality of this method is based on difficulty of choosen matrix A_1 and A_2.

We must mention the fact that, in order to be above mentioned methods reliable and different with its high quality it is necesary matrix to be **commutative.**

Building **commutational matrix** is curried out easily A and B matrix are comutational, if A matrix multiplication on B matrix from the left is equal to B matrix multiplication on A matrix from the right. We can say, that AB=BA besides, if we take some kind of matrix and multiply it on itself. Recieve matrix and first matrix are comutational matrix.

Matrix multiplity is matrix field, closed multiplity . To multiply two matrices. We will receive such third matrix, which is situated between the multiplication of the same matrices.

In the end, already received new methods own asymmetrical methods and are distinguished with high reliabilities.

Gryptocomplication is complication from matrices multiplication, which are based on received reliability methods.

Above mentioned is described, are brought examples, schedules, draughts, as well as the final conclusion.

შინაარსი

ცხრილების ნუსხა

ნახაზების ნუსხა

დისერტაციაში გამოყენებული აბრევიატურები

RSA – რაივესტ-შამირ-ეიდელმანი.

DES – კლასიკური სიმეტრიული სისტემები.

IBM – გამომთვლელი მანქანა.

ე.გ.მ. – ელექტრონული გამომთვლელი მანქანა.

ე.ი. – ესეიგი.

სტუ – საქართველოს ტექნიკური უნივერსიტეტი.

მადლიერება

რასაკვირველია, ძალიან მადლიერი ვარ და მინდა გადაუხადო დიდი მადლობა, ჩემს ხელმძღვანელებს: **ბატონ რიჩარდ მეგრელიშვილს** და **ბატონ სერგო ცირამუას**. მათ ძალიან დიდი წვლილი მიუძღვით ჩემი ნაშრომის დამუშავებაში.

უღრმესი მადლობა.

შესავალი

რა არის ამ ნაშრომის მთავარი მიზანი და არსი ...

ორ კანონიერ მომხმარებელს შორის ინფორმაციის გაცვლა.

როდესაც ორ სუბიექტს შორის ხდება ინფორმაციის გაცვლა, იგი საჭიროებს დაცვას. როცა ინფორმაციის გაცვლა ხორციელდება დახურული არხით, ამ დროს გასაღების გაცვლისათვის გამოიყენება კურიერი, ანუ მესამე პირი. ხოლო როცა ინფორმაციის გაცვლა ხდება ღია არხით, ამ დროს ეს მეთოდი არ საჭიროებს კურიერს, გასაღების დაფიქსირება ორივე მხარეს ხდება ღია არხით. ამ დროს კი, მესამე სუბიექტმა რომ ჩაიჭიროს ეს ინფორმაცია, მან ვერ უნდა შეძლოს, რეალურ დროში, მისი გატეხვა, ანუ ინფორმაცია საჭიროებს საიმედო დაცვას.

ინფორმაციის დაცვა-დასაიდუმლოება გამოიყენება საბანკო-საფინანსო, სახელმწიფო, სამხედრო სტრუქტურებში. ასევე იმ დროსაც, როცა ნებისმიერი ორი სუბიექტი უგზავნის ერთმანეთს რაღაც ნებისმიერი სახის ინფორმაციას და არ უნდათ, რომ ეს ინფორმაცია ხელმისაწვდომი იყოს ვინმე სხვისთვის.

ასევე შესაძლებელია მესამე პირის თანხლებით, თუკი უკვე ამ ორმა პირმა გაცვალეს გასაღები, საუბრის დროს ამ გასაღებით დაშიფრონ ინფორმაცია და ისაუბრონ, ისე რომ მესამე იქვე მყოფი პირი ვერაფერს მიხვდეს [22, 23, 30].

თუმცაღა, ხდება ისეთი შემთხვევებიც, როცა ადგილი აქვს ინფორმაციის გამჟღავნებას, ხდება უფრო მეტიც – ინფორმაციის ჩანაცვლება, გაყალბება და ა.შ.

დავუშვათ, რომ გვაქვს ორი X და Y მხარეები, რომელთა შორის ხდება ინფორმაციის გაცვლა. ვთქვათ, რომ ვიყენებთ სიმეტრიულ სისტემას, ანუ გასაღების გაცვლა ხდება დახურული არხით. X მხარე იღებს გასაგზავნ ინფორმაციას, შემდგომ მას შიფრავს გასაღებით და უგზავნის Y მხარეს. Y მხარე შესაბამისად, მიღებულ ინფორმაციას გაშიფრავს იგივე გასაღებით და მიიღებს საწყის ინფორმაციას, ანუ მოახდენს ინფორმაციის დეშიფრაციას.

როგორც უკვე ავღნიშნეთ, არსებობს ორი სახის სისტემა სიმეტრიული და ასიმეტრიული. ორივე სისტემებში განხილული მეთოდები გამოირჩევა საიმედოობით, მაგრამ მაინც არის სხვადასხვა დადებითი და უარყოფითი მხარეები [34, 45, 46].

სიმეტრიული სისტემების დროს, კურიერის გამოყენება არის საჭირო, მაგრამ სამაგიეროდ ინფორმაციის დაშიფვრას სჭირდება გაცილებით მცირე დრო, ვიდრე ასიმეტრიულის დროს.

ასიმეტრიული სისტემების დროს კი, გასაღების გენერაციას ცალკე დრო სჭირდება და კიდევ ცალკე დრო არის საჭირო ინფორმაციის დაშიფვრისათვის, მაგრამ სამაგიეროდ მედეგობა გაცილებით მაღალია.

სიმეტრიული სისტემების დროს გამოიყენება ჩანაცვლება, გადანაცვლების ფუნქცია, ასიმეტრიულის დროს – ახარისხება, მამრავლებად დაშლა. შიფრაციის სიჩქარეც არის საკმაოდ განსხვავებული. სიმეტრიულის დროს შიფრაციის სიჩქარე არის მილიწამები, ასიმეტრიულის დროს – წუთები და ა.შ.

ორივე მეთოდი გამოირჩევა სხვადასხვა დადებითი მახასიათებლებით, ორივე მიღებულია და დამტკიცებულია კრიპტოგრაფიაში. თუ ინფორმაცია არის მცირე ზომის და მისი გაცვლა გვინდა რომ მოხდეს სწრაფად, ვიყენებთ სიმეტრიულ სისტემას, ხოლო თუ ინფორმაცია არის დიდი ზომის და საიმედოობას უფრო მეტი მნიშვნელობა ენიჭება ვიდრე სისწრაფეს, მაშინ გამოიყენება ასიმეტრიული მეთოდები, ანუ ორივე მეთოდს აქვს გარკვეული გამოყენების არეალი.

კანონიერ მომხმარებლებს შორის კავშირის არხში გადაცემული ინფორმაცია უნდა იყოს დაცული სხვადასხვა მეთოდებით, რომლებიც წინ აღუდგება ყველანაირ დაბრკოლებას, მრავალ საშიშროებას. ხაკერი ეცდება ჩაიჭიროს სუსტი რგოლი, ეს კი აუცილებლად უნდა გაითვალისწინოს მომხმარებელმა ინფორმაციის დაცვის დროს. გამოყენებული უნდა იქნეს ისეთი მექანიზმები, რომ ინფორმაცია იყოს მთლიანად დაცული არაკანონიერი მომხმარებლებისაგან.

გასაღებში იგულისხმება, როგორც მარტივი რიცხვი, ასევე ვექტორი, ასევე ტექსტი და ა.შ. შიფრო ტექსტი, შესაძლოა ხელში ჩაიგდოს არაკანონიერმა მომხმარებელმა, მაგრამ არ იცის გასაღები და ვერ ახდენს დეშიფრაციას.

მნიშვნელობა აქვს ასევე ინფორმაციის რაოდენობას, შესაბამისად გასაღების სიგრძეს და შიფრაციის სიჩქარეს. მართალია საიმედოობა არის წამოწეული წინა საფეხურზე, მაგრამ არც შიფრაციის სიჩქარე უნდა იყოს დიდი რიცხვი, რომ დროულად, სწრაფად ვერ მოხდეს გასაღების გენერაცია და შემდგომ გადაცემული (საწყისი) ინფორმაციის დაშიფვრა.

ამოცანის აქტუალობა: საერთოდ კრიპტოგრაფია საკმაოდ აქტიური თემაა და გამოყენებადია პრაქტიკაში. ჩვენს შემთხვევაში, ამოცანის აქტუალობა მდგომარეობს იმაში, რომ გამოყენებულია როგორც ასიმეტრიული მეთოდი ცალკე, და შექმნილია ორიგინალური მეთოდი, ასევე ორივე სიმეტრიული და ასიმეტრიული მეთოდების სინთეზი. განხილულია და აგებულია კომუტატიური მატრიცები გასაღების მიღებისათვის, იგება საკმაოდ მარტივად და თანაც მათი სიმრავლე არის იმდენად დიდი, რომ მათი მოძებნა და ამორჩევა ყველასათვის ცნობილი და ხელმისაწვდომი მატრიცათა სიმრავლიდან, რეალურ დროში, შეუძლებელია.

მიზანი: ჩვენი მიზანი იყო შეგვექმნა ისეთი ორიგინალური მეთოდი, რომელიც გამორჩეული იქნებოდა უკვე არსებული მეთოდებისგან. განვიხილეთ არსებული, პრაქტიკაში გამოყენებადი მეთოდები და მივიღეთ რამოდენიმე ახალი მეთოდი. მიღებულ მეთოდებში გამოიყენება როგორც სიმეტრიული ასევე ასიმეტრიული სისტემები. მეთოდი უნდა ხასიათდებოდეს მაღალი შიფრაციის სიჩქარით, კრიპტოსირთულით, გასაღების გენერაციის მაღალი სიჩქარით და საიმედოობით.

შევქმენით ისეთი მეთოდები, რომლებიც ხასიათდება აღნიშნული მახასიათებლებით.

ამოცანები:

1. ასიმეტრიული მეთოდი

გვაქვს ორი X და Y მხარეები.

გაცხადებულია (ცნობილია) P (მარტივი) რიცხვი, ცნობილია e ვექტორი. ე.ი. ცნობილია განზომილება, ასევე ცნობილია ვექტორის და მატრიცის ელემენტები, რადგან ვიცით P რიცხვი. ცნობილია მატრიცათა სიმრავლე, რაც ყველასათვის ხელმისწავდომია.

ე.ი. გამოვიყენება მხოლოდ ასიმეტრიული მეთოდი, კერძოდ: დიჰი-ჰელმანის მეთოდი

2. ასიმეტრიული მატრიცული მეთოდის სინთეზი სიმეტრიულ მეთოდთან.

გვაქვს ორი X და Y მხარეები, რომელთა შორის ხდება ერთიდაიგივე გასაღების დაფიქსირება, e ვექტორი უცნობია, გადაეცემა დახურული არხით, ინფორმაციის დაშიფვრა-გაშიფვრა და შესაბამისად გაცვლა ხდება ღია არხით (ამოცანა 1).

ე.ი. ამ მეთოდით ხდება სიმეტრიული და ასიმეტრიული მეთოდების სინთეზი.

3. ვექტორის და მატრიცის გადაცემა საიდუმლოდ.

რადგან სიმეტრიული მეთოდი უკვე გამოვიყენეთ ვექტორის გადასაცემად (ამოცანა 2), ამიტომ უმჯობესი იქნება, რომ მატრიცის გადაცემაც მოხდეს საიდუმლოდ.

ანუ ამ შემთხვევაშიც გამოიყენება ორივე მეთოდი, მაგრამ მატრიცის გადაცემაც ხდება საიდუმლოდ, აქედან გამომდინარე გასაღების გენერაციის დრო ხდება მილიწამებში.

სამეცნიერო სიახლე:

ამოცანა 1-ის ამოხსნისათვის გამოყენებული იქნა დიფი-ჰელმანის მეთოდი, მაგრამ ახარისხების ფუნქცია შევცვალეთ მატრიცაზე გამრავლებით, ამით გასაღების გენერაციის დრო შემცირდა, საიმედოობა კიდევ უფრო გაიზარდა.

ამოცანა 2-ში გამოყენებული იქნა მეთოდთა სინთეზი. სიმეტრიული მეთოდით ანუ დახურული არხით ხდება ვექტორის გადაცემა, ამის შემდეგ ღია არხით (ამოცანა 1) ხორციელდება გასაღების გენერაცია.

ამოცანა 3-ით ხდება ვექტორის და მატრიცის ერთდროულად საიდუმლოდ გადაცემა და შემდგომ დაშიფრული ინფორმაციის გაცვლა ღია არხით (ამოცანა 2), შიფრაციის სიჩქარე კიდევ უფრო იზრდება.

ე.ი. ამოცანა ერთში გამოიყენება მხოლოდ ასიმეტრიული მეთოდი; ამოცანა ორში – სიმეტრიული და ასიმეტრიული მატრიცების სინთეზი; მესამე ამოცანაშიც – სინთეზი.

აღნიშნულ მეთოდებში კი, გამოყენებულ იქნა კომუტატიური-კვადრატული მატრიცები, რამაც ძალიან კარგი შედეგი მოგვცა. ასეთი მატრიცები განხილული და აგებული იქნა $GF(p^m)$ გალუას ველებზე.

მივიღეთ ახალი ორიგინალური მეთოდი უკვე არსებულ მეთოდებზე დაყრდნობით და ზოგიერთი მეთოდების სინთეზის გამოყენებით, რომელიც გამოირჩევა მაღალი სიჩქარითა და საიმედოობით.

პრაქტიკული ღირებულება:

კრიპტოგრაფია ეს არის ინფორმაციის დაცვა – დასაიდუმლოება. არსებული მეთოდები გამოიყენება: სახელმწიფო საქმეებში, სამხედრო სამსახურში, ნებისმიერი სახის ინფორმაციის გაცვლისათვის როგორც ღია ასევე დახურული არხით.

ანალოგიურად, მიღებული ახალი მეთოდების გამოყენებით ჩვენ შეგვიძლია დავშიფროთ ნებისმიერი სახის ინფორმაცია და როგორც ღია, ასევე დახურული და სინთეზური მეთოდებით მოვახდინოთ მათი გადაცემა.

აღნიშნული მეთოდები გამოირჩევა მაღალი საიმედოობით, სიჩქარითა და კრიპტოსირთულით.

ასევე შესაძლოა მათი გამოყენება საბანკო საქმეებში.

მოცულობა და სტრუქტურა: ნაშრომი შედგება:

- შესავალი;
- ლიტერატურის მიმოხილვა, თავი I;
- შედეგები და მათი განსჯა, თავი II;
- ექსპერიმენტული ნაწილი, თავი III;
- სამივე თავის დასკვნა;
- საბოლოო დასკვნა;
- დანართი 1;
- დანართი 2;
- გამოყენებული ლიტერატურების ნუსხა;
- ნაშრომის მოცულობა შეადგენს 112 გვერდს.

ლიტერატურის მიმოხილვა,

თავი I. აღწერილია კრიპტოგრაფიული სისტემები. სიმეტრიული და ასიმეტრიული მეთოდები, მათი გამოყენების არეალი.

შედეგები და მათი განხჯა,

თავი II. განხილულია მიღებული ახალი მეთოდები, მოყვანილია მაგალითები. დამუშავებულია მატრიცული მეთოდი.

ექსპერიმენტული ნაწილი,

თავი III. განხილულია სხვადასხვა სახის მატრიცები, მატრიცათა სიმრავლეები, მატრიცათა ველი და მიღებულია საბოლოო შედეგი, როგორი მატრიცები არის მისაღები მატრიცული მეთოდისათვის კრიპტოგრაფიაში ჩვენს მიერ წარმოდგენილ ორიგინალურ მეთოდში.

ლიტერატურის მიმოხილვა

თავი I.

კრიპტოგრაფიული სისტემები

კრიპტოგრაფია ინფორმაციის დასაიდუმლოების სამეცნიერო-ტექნიკური დარგია, რომელსაც განვითარების მრავალსაუკუნოვანი ისტორია აქვს. განვითარების განსაკუთრებულ საფეხურს კრიპტოგრაფიამ გასული საუკუნის მეორე ნახევარში მიაღწია, როდესაც მისი მეთოდები მათემატიკურ სისტემებს დაეფუძნა. ხოლო 1976 წლიდან ღია გასაღებების მეთოდოლოგიამ მას თვისებრივად ახალი ხარისხი შესძინა.

საზოგადოდ, კრიპტოგრაფიას შეხება აქვს ინფორმაციის დაცვისა და დასაიდუმლოების მრავალ ასპექტთან, როგორებიცაა – ტექსტის შიფრაცია-დეშიფრაცია, დაცვა არასანქციონირებული შეღწევისაგან, ღია ტექსტის ელექტრონული (ციფრული) ხელმოწერა და სხვ. აქედან გამომდინარე, ფართოა მისი გამოყენების არეალიც: სამხედრო-სახელმწიფოებრივი დანიშნულებისა და საბანკო-საფინანსო კომერციული სისტემები, ლოკალური და გლობალური (ინტერნეტი) კომპიუტერული ქსელები და სხვ., რაც ინფორმატიზაციის თანამედროვე ეპოქაში მის აქტუალობასა და მნიშვნელობას განაპირობებს [10, 11, 21, 27, 30, 31, 45].

კრიპტოგრაფია ორი ძირითადი მიმართულებით ვითარდება:

1. **სიმეტრიული სისტემა**, რომელშიც ერთიდაიგივე გასაღები (შიფრი), ფორმირდება (მიიღება) გადამცემ X და მიმღებ Y მხარეებზე, და მათ შორის საიდუმლო გასაღების გაცვლა მოითხოვს საიდუმლო კავშირის არხის (ანუ კურიერის) არსებობას.

2. **ასიმეტრიული სისტემა**, რომელშიც საიდუმლო გასაღების გაცვლა ღია არხით ხორციელდება, ან საიდუმლო გასაღებს მხოლოდ ერთ-ერთი – X ან Y მხარე ფლობს.

სიმეტრიულ და ასიმეტრიულ სისტემებში გამოთვლითი ოპერაციები, ალგორითმების შესაბამისად, X და Y მხარეზე მნიშვნელოვნად განსხვავებულია.

1.1. ინფორმაციის ცნება

ინფორმაცია არ არის მატერიალური ან ენერგეტიკული ცნება. მისი არსება იმაშია, რომ მიმღებს უბიძგებს განსაზღვრული ქცევის არჩევაში – განსაკუთრებით აზროვნების სფეროში. ადამიანი ინფორმაციას ღებულობს სამი არხის საშუალებით:

ა. მემკვიდრეობითი ფაქტორებით (გენებით), რომლითაც ადამიანს მშობლებისაგან გადაეცემა ნივთიერი და სტრუქტურული ნიშნები;

ბ. ადამიანისაგან გადაეცემა ჩამოყალიბებული აზრებისა და მითითებების სახით (მაგ: წიგნის საშუალებით);

გ. უშუალოდ გარემო სინამდვილისაგან.

"ინფორმაციის" ცნება ერთ-ერთი ძირითადია ინფორმაციული სისტემების განხილვისას. არსებობს ინფორმაციის მრავალი განსხვავებული თვალსაზრისი და განსაზღვრება ზოგადი ფილოსოფიურიდან (როგორც – რეალური სამყაროს ასახვა-გამოხატულება) ყველაზე კერძო პრაქტიკულ განსაზღვრებამდე (როგორც – ცნობები, რაც გამიზნულია ინფორმაციის დამუშავების, შენახვისა და გადაცემისათვის). მნიშვნელოვანია ნ. ვინერის აზრი, რომ "ინფორმაცია არის ინფორმაცია და არა მატერია ან ენერგია" [12, 13].

ინფორმაციის გამოხატვის საშუალებები მატერიალურ-ენერგეტიკულია და ჩვენს შემთხვევაში წარმოადგენს ფიზიკურ სიგნალებს, ასონიშნებს, ციფრულ ჩანაწერებს, ფიგურებს, დიაგრამებსა და სხვ.

საუბარი ინფორმაციის დაცვის სისტემების შესახებ ფორმალურია, თუ ის ინფორმაციის არსებობის თვით ფაქტს არ ითვალისწინებს. ნებისმიერი კოდი ინფორმაციის მატარებელია.

კოდირების სისტემები ინფორმაციის დამუშავების, გადაცემისა და დამახსოვრებისათვის იქმნება, მაგრამ ბიოლოგიური (გენეტიკური) და სხვ. კოდებისაგან განსხვავებით ინფორმაციის დაცვისათვის გამიზნული კოდების მთავარი ფუნქციაა მიმდინარე პროცესების დაცვა გარეშე ზემოქმედებისაგან. მიუხედავად ამისა, არ უნდა დაგვავიწყდეს, რომ ინფორმაციის გადაცემისას ბუნებასა თუ ცოცხალ გარემოში, ტექნიკურ სისტემებსა თუ საზოგადოებაში, როგორიც არ უნდა იყოს მისი წყარო თუ მომხმარებელი, იქმნება ინფორმაციული გარემო, რომელშიც კოდი-

რების სისტემები საერთო ინფორმაციულ პროცესს ექვემდებარებიან, ხოლო ინფორმაციული სინერგიულობა (ურთიერთშეთანხმებულობა, ურთიერთთანწყობა), თვისობრივად მსგავს და პროცესებისათვის საერთო სტრუქტურათა წარმოქმნას განაპირობებს, რაც განსაკუთრებით კოდირების სისტემებით აისახება და ვლინდება.

ინფორმაცია არსებობს როგორც სემანტიკური (შინაარსობრივი მნიშვნელობის), ასევე რაოდენობრივი.

აღნიშნული თემატიკა არ ითვალისწინებს ინფორმაციის სემანტიკურ განხილვას. ისიც უნდა აღინიშნოს, რომ სემანტიკური ინფორმაციის საკითხი რთული და პრობლემატურია და არ არის სრულად დამუშავებული, მაგრამ რაოდენობრივ და სემანტიკურ ინფორმაციათა შორის განსხვავების აღნიშვნა და მისი გარკვევა საკუთრივ რაოდენობრივი ინფორმაციის ფორმულირების გაცნობიერებისათვის არის აუცილებელი.

ერთიდაიმავე მოვლენაში, თუ კოდურ გამოსახულებაში, სხვადასხვა დამკვირვებელმა შეიძლება დაინახოს არა მხოლოდ სხვადასხვა აქტუალობის შემცველი ინფორმაცია, არამედ ინფორმაცია, განსხვავებული თავისი შინაარსითაც, რაც მოვლენის განსხვავებულ შეფასებას (აღქმას) განაპირობებს [12, 27].

1.2. სიმეტრიული სისტემები

1. ცეზარის ალგორითმი. ცნობილი ალგორითმებიდან, ყველაზე უძველესი არის ე.წ. ცეზარის ალგორითმი. მასში ანბანის ყოველ $a_i \in A$ $(i=1,...,|A|)$ სიმბოლოს შეესაბამება გარკვეული რიცხვი, რაც შეიძლება მის ანბანურ რიგით ნომერს წარმოადგენდეს. ტექსტის შიფრაცია მარტივია: ფიქსირებული $a \in A$ სიმბოლო იკრიბება ტექსტის ცალკეულ ასონიშნებთან $|A|$ მოდულით.

მაგალითი:

ინფორმაცია: ABCDE ...
გასაღები: DDDDD ...
კრიპტოგრამა: EFGHI ...

ე.ი. აღნიშნულ ალგორითმში გასაღები, სიგრძით არის ერთის ტოლი, რომელიც გადაიცემა საიდუმლოდ.

გადასაცემი ინფორმაცია შესაძლოა წარმოვადგინოთ მათი ანბანური რიგითი ნომრების შესაბამისად. ამის შემდგომ, რიგითი ნომრების ანუ ციფრების სახით წარმოდგენილ ინფორმაციას ემატება საიდუმლოდ გადაცემული გასაღები მოდულით |A|, მიიღება დაშიფრული ინფორმაცია და ხდება მისი გადაცემა. მიმღები კი შესაბამისად გაშიფრავს ინფორმაციას იგივე საიდუმლო გასაღებით.

2. ვიჟინერის მეთოდი. ამ მეთოდში გამოყენებული ალგორითმი ანალოგიურია ცეზარის ალგორითმისა, მხოლოდ იმ განსხვავებით, რომ ინფორმაცია დაყოფილია ბლოკებად და შიფრი წარმოადგენს L სიგრძის გარკვეულ ბლოკს.

მაგალითი: თუ L=3, მაშინ:

ინფორმაცია: NOWISTHE ...

გასაღები: GAHGAHGA...

კრიპტოგრამა: IODOSANE ...

აღნიშნული მაგალითიდან ნათლად ჩანს, რომ ცეზარის ალგორითმისაგან განსხვავებით, გასაღების სიგრძე გაიზარდა, რამაც გამოიწვია ინფორმაციის დაყოფა ბლოკებად. თუმცაღა დაშიფვრის და გაშიფვრის პროცესი არის ანალოგიური პროცედურა, როგორც ეს ხდება ცეზარის ალგორითმში მოდულით |A|. მაგრამ ამ მეთოდში ცოტა სირთულეა მაინც შემოტანილი, რაც გამოიწვია გასაღების სიგრძის გაზრდამ და შესაბამისად საიმედოობაც შედარებით მაღალია.

3. ვერნამის ალგორითმი წარმოადგენს ვიჟინერის მეთოდში გამოყენებული ალგორითმის ფართო სპექტრს, გამოყენებული იდეის განვითარებას, ანუ ვერნამის ალგორითმი გამომდინარეობს ვიჟინერის ალგორითმიდან.

n სიგრძის სრული ტექსტი იშიფრება მისი ტოლი L სიგრძის საიდუმლო შიფრით (გასაღებით), ე.ი. L=n.

ე.ი. ამ შემთხვევაში გადასაცემი ინფორმაციის სიგრძე და დასაიდუმლოებული გასაღების სიგრძე არის ტოლი. გასაღების გაცვლა ხდება ისევდაისევ კურიერის სახით.

მაგალითი: ვთქვათ გვაქვს ორი X და Y მხარეები, რომლებიც ცვლიან ინფორმაციას. ხოლო გასაღებს იღებს X მხარე და აწვდის Y მხარეს კურიერის გამოყენებით. გასაღები კი ასეთია: ამათუიმ წიგნის, ამათუიმ გვერდის, ამათუიმ აბზაცის, ამათუიმ სიტყვიდან დაწყებული ინფორმაციის სიგრძის ჩათვლით. დანარჩენი პროცედურა კი ხდება ანალოგიურად ზემოთ აღწერილი მეთოდებისა.

ვერნამის ალგორითმი მაგალითია იმ შემთხვევისა, როდესაც ერთ-ერთი, – ერთი შეხედვით მარტივი, – ცეზარის ალგორითმი, კვლევის გარკვეულ სფეროში, აღმოჩნდება საუკეთესოთაგანი მეთოდებს შორის, რადგან ვერნამის ალგორითმი მიღებული იქნა ვიჟინერის ალგორითმიდან, ხოლო ვიჟინერის ალგორითმი – ცეზარის ალგორითმიდან. ე.ი. ვერნამის ალგორითმს საფუძველად უდევს ცეზარის ალგორითმი.

ვერნამის ალგორითმი წარმოადგენს პრაქტიკულად გაუხსნელ (გაუტეხავ) ალგორითმს, რომელიც დღესაც გამოიყენება ინფორმაციის სახელმწიფოთაშორისი გაცვლის დონეზე.

მაგრამ აქვე უნდა აღინიშნოს, რომ ყოველი დაშიფვრის და გაშიფვრის შემდეგ, დაშიფრული ტექსტი გადამცემ და მიმღებ მხარეების მიერ, აუცილებლად უნდა განადგურდეს.

4. სისტემა DES სიმეტრიული სისტემების კლასიკური მაგალითია, რომელიც ზემოთ განხილულ ალგორითმებსა და ინფორმაციის გარკვეული გარდაქმნების (გადანაცვლებისა და ჩანაცვლების) განხორციელებაზე არის დაფუძნებული.

DES სისტემა, ქვემოთ მოცემულ ასიმეტრულ სისტემებთან შედარებით, გაცილებით სწრაფქმედია. ეს სისტემა დამუშავებულია ფირმა IBM-ის მიერ, და არაერთგზის გახლავთ მოდიფიცირებული და წარმოადგენს 1977 წლიდან შეერთებული შტატების სახელმწიფო სტანდარტს.

კრიპტომედეგობა (საიმედოობა) ეფუძნება ალგორითმის გახსნის სირთულეს. შესაძლოა ყველა ინფორმაცია ჩაიგდოს ხელში არაკანონიერმა მომხმარებელმა, მაგრამ ალგორითმი უნდა იყოს იმდენად დაცული, რომ მან ვერ შეძლოს გასაღების მიღება.

30-იანი წლებისათვის საბოლოოდ ჩამოყალიბდა მათემატიკური მიმართულებანი, რომლებიც წარმოადგენს კრიპტოგრაფიის მეცნიერულ

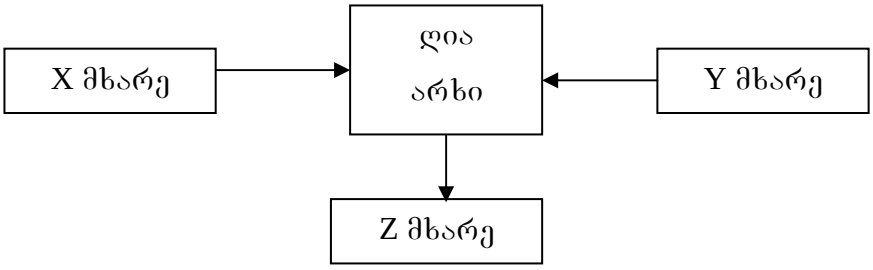
საფუძველს. როგორიცაა: ალბათობის თეორია, რიცხვთა თეორია, ზოგადი ალგებრა, კომბინატორიკა და ა.შ.

70-იანი წლების მეორე ნახევარში კი შეიქმნა ასიმეტრიული (ღია) კრიპტოსისტემა, რომელიც არ ითხოვს გასაღების გადაცემისათვის მესამე პირს ანუ კურიერს, გასაღები ფიქსირდება ღია არხით [13, 17, 23, 32, 34, 43, 46, 54, 56, 69].

1.3. ასიმეტრიული სისტემები

შეტყობინება ანუ გადასაცემი ტექსტი, შესაძლოა იყოს, როგორც ასონიშნები, ასევე ანბანის რიგითი ნომრები, ასევე ორობითი ან ათობითი სახით წარმოდგენილი.

ახლა უკვე ღია არხით, ხდება ერთიდაიგივე გასაღების მიღება კანონიერ მომხმარებლებს შორის და შემდგომ ამ გასაღებით ინფორმაციის დაშიფვრა, ინფორმაცია არ უნდა ჩაუვარდეს Z მხარეს. თუ მოახერხებს მის ჩაგდებას, რა თქმა უნდა ვერ უნდა გაშიფროს და შესაბამისად ვერ უნდა მიიღოს გადაცემული საწყისი ინფორმაცია, იხ. ნახ. 1. ღია არხით გადაცემის მარტივი სქემა.



ნახ. 1.

ამ სისტემაში ალგორითმის დამალვა არ ხდება. ანუ დაშიფვრა-გაშიფვრის პროცესი როგორ ხორციელდება ეს ცნობილია, რადგან მეთოდები ყველა მომხმარებელმა იცის.

აქვე აღსანიშნავია, რომ კრიპტოგრაფიაში 10^{30} არის ქვედა ზღვარი. ანუ ეს იმდენად დიდი რიცხვია, რომ, თუკი მეთოდში გამოყენებული ელემენტთა სიმრავლე მიუახლოვდება ამ რიცხვს, მაშინ ეს მეთოდი არის გაუტეხელი.

ეხლა კი განვიხილოთ არსებული მეთოდები.

1.3.1. დიფი-ჰელმანის ალგორითმი

1976 წელი არის ახალი ერა კრიპტოგრაფიაში. უ. დიფის და მ. ჰელმანის ნაშრომით დასაბამი დაედო ასიმეტრიული სისტემების განვითარებას, როდესაც გასაღების გაცვლა, ინფორმაციის შიფრაცია (დაშიფვრა) დეშიფრაცია(გაშიფვრა) ხდება ღია არხით.

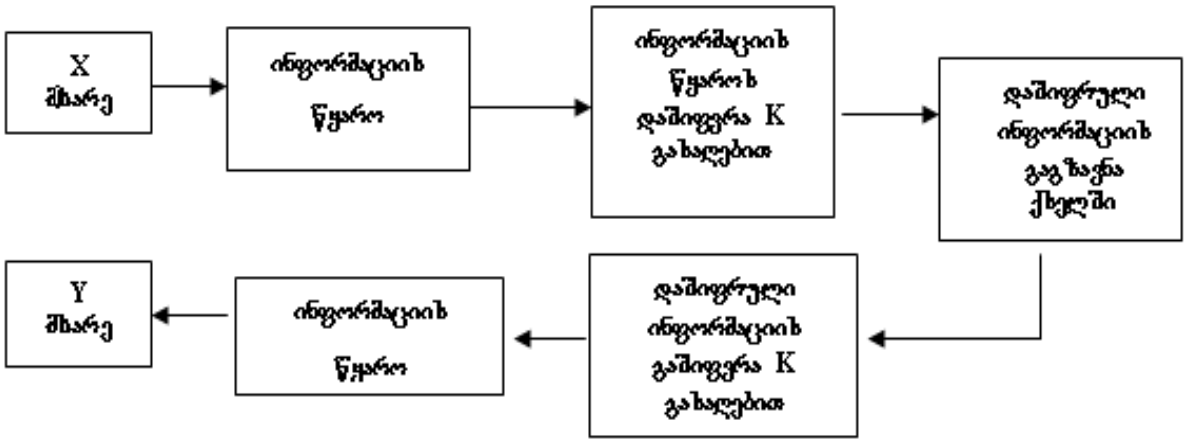
აღნიშნული პროცედურა თითქოს მარტივია, მაგრამ თანამედროვე კომპიუტერებითაც კი, რეალურ დროში, ვერ ახერხებენ გატეხვას.

ალგორითმი ეყრდნობა GF(P) ველში ლოგარითმების გამოთვლის სირთულეს.

გასაღების ღია არხით გაცვლა ხორციელდება შემდეგი სქემით:

X და Y მხარეებს შორის ხდება ინფორმაციის გადაცემა და მიღება, იხ. ნახ. 2. ინფორმაციის დაშიფვრის, გაშიფვრის და გადაცემის სქემატური წარმოდგენა.

გაცხადებულია (ცნობილია) P მარტივი, მაღალი რიგის რიცხვი $\approx 2^{500}$ და a - მთელი რიცხვები (1<a<P).



ნახ. 2.

X მხარე ირჩევს x_1 ნატურალურ საიდუმლო რიცხვს და კავშირის ღია არხით გადასცემს Y მხარეს

$$y_1 \equiv a^{x1} \bmod P \tag{1.1}$$

გამოთვლილ მნიშვნელობას.

Y მხარეც შერჩეული x_2 ნატურალური საიდუმლო რიცხვის მეშვეობით აფორმირებს K_1 გასაღებს:

$$K_1 = (a^{x1})^{x2} \equiv a^{x1x2} \bmod P, \tag{1.2}$$

თავის მხრივ, Y მხარე X მხარეს ღია არხით გადასცემს

$$y_2 \equiv a^{x2} \bmod P \tag{1.3}$$

მნიშვნელობას, ხოლო X-ი აფორმირებს იგივე K_2 გასაღებს:

$$K_2 = (a^{x2})^{x1} \equiv a^{x2x1} \bmod P. \tag{1.4}$$

მაშასადამე, ორივე მხარემ მიიღო ერთი და იგივე K გასაღები:

$$\mathbf{a^{x1x2} \bmod P = a^{x2x1} \bmod P = K_1 = K_2 = K}. \tag{1.5}$$

შიფრაციის მედეგობა (საიმედოობა) ეფუძნება X_1, X_2 საიდუმლო რიცხვების მიღების სირთულეს.

$y1 \equiv a^{x_1} \bmod P$ ამ განტოლებიდან

$$\mathbf{x_1 = \log_a y_1}. \tag{1.6}$$

ამ მეთოდის მედეგობა ეფუძნება სწორედ აღნიშნული ალგორითმის სირთულეს.

X_1 ელემენტის პოვნა გაცილებით რთულია, ვიდრე ვთქვათ Y_1-ის და მოითხოვს $p^{1/2}$ ოპერაციის ჩატარებას.

p რადგან არის მარტივი რიცხვი, იგი შედარებით ნაკლებია 2^n რიცხვზე, სადაც n არის ორობითი სიტყვის სიგრძე ანუ ვექტორის განზომილება), მაშინ ახარისხებას დასჭირდება ≈2n ოპერაცია GF(P) ველზე, ხოლო გალოგარითმებას – $2^{p/2}$.

თუ n=200, მაშინ დაახლოებით საჭიროა $2^{n/2}=2^{100}$ ოპერაციის ჩატარება დაახლოებით 10^{30} ოპერაცია, რაც პრაქტიკულად ვერ განხორციელდება. აღნიშნული რიცხვი არის კრიპტოგრაფიაში ქვედა ზღვარი.

განვიხილოთ მაგალითი:

$p = 7,\ \ a = 2,\ \ x_1 = 4,\ \ x_2 = 3,$ მაშინ

$$y_1 = 2^{\,4} \bmod 7 = 2,$$

$$K_1 = 2^3 \bmod 7 = 1,$$

$$y_2 = 2^{3} \bmod 7 = 1,$$

$$K_2 = 1^{4} \bmod 7 = 1,$$

$K_1 = K_2 = 1 = K$

ამის შემდგომ ხდება ინფორმაციის დაშიფვრა აღნიშნული საიდუმლო K გასაღებით და ხორციელდება მისი გაგზავნა ღია არხით.

ვთქვათ, n = 4 – განზომილება, ინფორმაცია არის ორობითი –

$$m = (0110), \text{ ე.ი. } M = 5.$$

X – დაშიფრავს ინფორმაციას და Y – გაშიფრავს.

Y – მხარე იღებს K^1 გასაღებს:

$$KK^1 = 1 \pmod{(p-1)}$$

ე.ი. $$1 \times x = 1 \pmod 6$$

X მხარე დაშიფრავს ტექსტს m = (0110), K = 1

$$M^K = 5^1 = 5 \pmod 7$$

მიღებულს უგზავნის Y მხარეს, რომელიც $K^1 = 7$ გასაღებით გაშიფრავს

$$M = M^{K1 \times K} = 5^7 = 5 \pmod 7.$$

Y მხარემ მიიღო ის ინფორმაცია, რაც სინამდვილეში გადაცემული იქნა X მხარის მიერ [20, 22, 24, 25, 28, 33, 36, 47, 70-72, 80, 81, 83].

1.3.2. RSA (რაივესტ-შამირ-ეიდელმანის) ალგორითმი

განსხვავებით დიფი-ჰელმანის ალგორითმისაგან, RSA ახორციელებს დაშიფრული ინფორმაციის ღია არხით გადაცემას. ალგორითმი ეყრდნობა ეილერის ცნობილ თეორემას:

$$X^{\Phi(N)} \equiv 1 \bmod N, \qquad (1.7)$$

სადაც Φ(N) ეილერის ფუნქციაა.

საზოგადოდ, Φ(N)-ის გამოთვლა დიდი რიცხვებისათვის რთულია, მაგრამ ცნობილია, რომ

$$\Phi(N) = (p-1) \times (q-1), \qquad (1.8)$$

როდესაც N=pq, სადაც p და q მარტივი რიცხვებია, მაგრამ p და q არ არის ურთიერთმარტივი რიცხვები, ამიტომ $\Phi(N) \neq \Phi(p) \times \Phi(q)$.

მოცემული M ინფორმაციისათვის

$$M^{KA(N)+1} \equiv M \bmod N. \qquad (1.9)$$

დაშიფრვა შემდეგი სქემით ხორციელდება: საიდუმლო p, q და Φ(N) რიცხვებისათვის X მხარე შეირჩევს ისეთ e და d რიცხვებს, რომლებიც აკმაყოფილებენ პირობას $ed \equiv 1 \bmod \Phi(N)$, ამასთან e და N რიცხვებს გააცხადებს, ხოლო d-ს დაასაიდუმლოებს, მაშინ Y მხარემ, შესაძლოა, e რიცხვის მეშვეობით დაშიფროს M ინფორმაცია:

$$M^e \equiv C \bmod N, \qquad (1.10)$$

რასაც გაშიფრავს მხოლოდ X მხარე:

$$(M^e)^d \equiv M. \qquad (1.11)$$

გარკვეული კომბინირებით შესაძლებელია X და **Y** მხარეებს შორის საიდუმლო ინფორმაციის გაცვლის განხორციელება ისე, რომ გამოირიცხოს მესამე **Z** სუბიექტის მონაწილეობის შესაძლებლობა შიფრაციისა და დეშიფრაციის პროცესში.

მაგალითი: p = 5, q = 3; M = 3, მაშინ

$$N = pq = 5 \times 3 = 15, \quad \Phi(N) = (p-1)(q-1) = 4 \times 2 = 8$$

$$ed = \Phi(N) + 1 = 8 + 1 = 9,$$

ე.ი. $e = 3, \ d = 3$

Y მხარე მიიღებს:

$$M = C^d = 12^3 \equiv 3 \pmod{15}$$

1.3.3. ელგამალის ალგორითმი

ეს ალგორითმი გამოიყენება ღია M ტექსტის ციფრული ხელმოწერისათვის. ტექსტის დაშიფრვა არ მოხდება, მაგრამ მას დაემატება S, R პარამეტრები, რომლებიც წარმოადგენენ ციფრულ ხელმოწერას.

X მხარე S და R პარამეტრებს აფორმირებს ცნობილი – P მარტივი, $a > 1$ მთელი, $Y \equiv a^x \bmod p$ რიცხვებისათვის. x ($1<x<p$) საიდუმლო სიდიდეა (გასაღები).

$R \equiv a^k \bmod p$ (**K** ფსევდოშემთხვევითი რიცხვია),

$$S \equiv xR + KM' \pmod{(p-1)}, \qquad (1.12)$$

სადაც $M'=H(M)$, ხოლო $H(M)$ ჰეშირების ცალმხრივი ფუნქციაა ($M'<P$).

Y მხარე ტექსტის სისწორეს ამოწმებს შემდეგი პირობით:

$$a^S \equiv y^R R^{M'} \bmod p \quad /M//R//S/ . \qquad (1.13)$$

ყოველ ტექსტს ან დოკუმენტს ბოლოში თან ერთვის ხელმოწერა, ხელმოწერა არის იურიდიული გარანტია დოკუმენტის ავტორობისა, რომ დოკუმენტი ნამდვილად ეკუთნის ავტორს და არა ვინმე სხვას.

R//S/ პარამეტრების შემოტანა უფრო ზრდის მედეგობას და შესაბამისად ართულებს ამოცნობის პროცესს, მაგრამ სამაგიეროდ, საიმედოობის გაზრდის ხარჯზე, იზრდება შიფრაციის დროც, რაც არ არის მისაღები. შიფრაციის დრო არ უნდა იყოს ძალიან დიდი და ასევე შიფრაციის პროცესი არ უნდა იყოს დაკავშირებული სირთულეებთან.

შესაძლოა ინფორმაციის გაცვლის დროს მოხდეს ასეთი ფაქტი: ინფორმაცია ჩაიჭიროს სხვამ და შეცვალოს და მის ნაცვლად მან მიმღებს მის მიერ შექმნილი ინფორმაცია გაუგზავნოს, ასეთი ფაქტებისაგან იცავს ხელმოწერის დამატება შიფროტექს [14, 16, 19, 35, 44, 67, 74, 76, 78, 86-89].

1.4. სიმეტრიული და ასიმეტრიული სისტემების შედარებითი ანალიზი

სიმეტრიული სისტემების ყველა ალგორითმი საჭიროებს კურიერის მონაწილეობას. ჯერ სანამ მოხდება ინფორმაციის გადაცემა, მანამდე ხდება გასაღების მიწოდება, რათა შემდგომ მოხდეს ამ გასაღებით გასაგზავნი ინფორმაციის დაშიფვრა და შესაბამისად მიღებული ინფორმაციის გაშიფვრაც.

სიმეტრიული სისტემებიდან დღეს-დღეობით ყველაზე გავრცელებულია DES (Data Encryption Standard) სისტემა.

ალგორითმი ამუშავებს 64 ბიტიანი განზომილების ღია ტექსტს და იყენებს 56 ბიტიან გასაღებს, თუმცა გასაღების ყოველი მე-8 ბიტი ლუწობაზე შემოწმებისათვის გამოიყენება, ამიტომ ძირითად ფუნქციას ასრულებს 56 ბიტი.

DES (Data Encryption Standard) სისტემა (100 – 1000) – ჯერ მეტია სწრაფქმედებით, ვიდრე ასიმეტრიული სისტემები, იხ. ცხრილი 1. DES (სიმეტრიული) და RSA (ასიმეტრიული) სისტემების მახასიათებელი პარამეტრების შედარებითი ანალიზის მაჩვენებლები.

№	**მახასიათებელი**	**DES**	**RSA**
1.	შიფრაციის სიჩქარე	მაღალი	დაბალი
2.	გამოყენებული ფუნქცია	გადანაცვლება, ჩასმა	ახარისხება
3.	გასაღების სიგრძე ბიტებში	56	500-ზე მეტი
4.	კრიპტოანალიზის სირთულე	გასაღების სივრცეში მთლიანი გადარჩევა	მამრავლებად დაშლა
5.	გასაღების გენერაციის დრო	მილიწამები	წუთები
6.	გასაღების ტიპი	სიმეტრიული	ასიმეტრიული

ცხრილი 1.

ნათლად ჩანს, DES და RSA სისტემების დადებითი და უარყოფითი მხარეები:

DES სისტემის გასაღების სიგრძე მოკლეა, მცირე დრო სჭირდება გასაღების გადასინჯვას, თანაც გამოყენებულია გადანაცვლების ფუნქცია, რაც იმას ნიშნავს, რომ გასაღების პოვნა უფრო შესაძლებელია. ე.ი. DES სისტემა ნაკლებად საიმედო, ადვილად გატეხვადია.

ხოლო RSA სისტემის გასაღების სიგრძე გაცილებით მეტია, ვიდრე DES გასაღების სიგრძე, გასაღების ამორჩევისათვის გამოიყენება ახარისხების ფუნქცია, რაც იმას ნიშნავს, რომ საკმაოდ დიდი დროა საჭირო გასაღების პოვნისათვის, რეალურ დროში შეუძლებელიც კი არის. ეს მიგვითითებს იმაზე, რომ RSA არის საიმედო და ხასიათდება მაღალი მედეგობით.

I თავის დასკვნა

განხილულ იქნა **კრიპტოგრაფია**, ინფორმაციის დაცვა – დასაიდუმლოება, მათი გამოყენების არეალი, მეთოდიკა და პრაქტიკული გამოყენების შესაძლებლობები.

კრიპტოგრაფია ორი მიმართულებით ვითარდება: სიმეტრიული და ასიმეტრიული.

სიმეტრიული არის ისეთი სისტემები, როდესაც გასაღების გაცვლა ხორციელდება დახურული არხით, ანუ მესამე პირის, კურიერის გამოყენებით.

ასიმეტრიული სისტემების გამოყენების დროს კი, გასაღების მიღება ორივე კანონიერ მომხმარებელს შორის ხდება სრულიად ღიად, ღია არხით, მაგრამ იმდენად დაცულად, რომ მისი გატეხვა მესამე არაკანონიერი მომხმარებლის მიერ (ჰაკერი) შეუძლებელია.

განვიხილულ და აღწერილ იქნა ორივე სისტემების შესაბამისი მეთოდები და ალგორითმები, მაგალითები და მათი მახასიათებლები, დადებითი და უარყოფითი მხარეები.

შედეგები და მათი განსჯა

თავი II.

ასიმეტრიული სისტემის მატრიცული მეთოდის შემუშავება

ზემოთ უკვე აღნიშნულ და განხილულ იქნა ასიმეტრიული და სიმეტრიული სისტემები, მათი დადებითი და უარყოფითი მხარეები. განხილული იქნა სხვადასხვა მაგალითები.

ამ შემთხვევაში, ჩვენ ვიყენებთ ასიმეტრიული სისტემებიდან ერთერთს, დიფი-ჰელმანის მეთოდს.

2.1. ასიმეტრიული მეთოდი

ამოცანა 1. გვაქვს ორი X და Y მხარეები.

გაცხადებულია (ცნობილია) P (მარტივი) რიცხვი, ცნობილია e ვექტორი. ე.ი. ცნობილია განზომილება, ასევე ცნობილია ვექტორის და მატრიცის ელემენტები, რადგან ვიცით P რიცხვი.

მაშასადამე, ცნობილია მატრიცათა სიმრავლე, რაც ყველასათვის ხელმისწავდომია.

X მხარე ირჩევს თავის A_1 საიდუმლო მატრიცას მატრიცათა სიმრავლიდან და კავშირის ღია არხით გადასცემს Y მხარეს გამოთვლილ y_1 მნიშვნელობას

$$y_1 \equiv e \times A_1 \bmod P . \qquad (2.1)$$

Y-ი შეარჩევს თავის A_2 საიდუმლო მატრიცას და აფორმირებს K გასაღებს:

$$K_1 = (e \times A_1) \times A_2 \equiv e \times A_1 \times A_2 \bmod P . \qquad (2.2)$$

თავის მხრივ Y მხარე X მხარეს ღია არხით გადასცემს გამოთვლილ y_2 მნიშვნელობას

$$y_2 \equiv e \times A_2 \bmod P , \qquad (2.3)$$

ხოლო X-ი აფორმირებს K გასაღებს:

$$K_2 = (e\times A_2)\times A_1 \equiv e\times A_2\times A_1 \bmod P\ . \qquad (2.4)$$

მაშასადამე, ორივე მხარემ მიიღო ერთიდაიგივე K გასაღები –

$$\mathbf{K = e\times A_1\times A_2 \bmod P \equiv e\times A_2\times A_1 \bmod P}\ . \qquad (2.5)$$

შიფრაციის მედეგობა (საიმედოობა) ეფუძნება, A_1 და A_2 საიდუმლო მატრიცების, მატრიცათა სიმრავლიდან ამორჩევის სირთულეს.

აქვე უნდა აღვნიშნოთ განხილული მეთოდის მნიშვნელოვანი საკითხი, რაც მდგომარეობს შემდეგში: იმისათვის რომ, ორივე მხარემ, მიიღოს ერთიდაიგივე K გასაღები აუცილებელია და საკმარისი, ისეთი A_1 და A_2 მატრიცები, და საერთოდ, მატრიცათა სიმრავლე, საიდანაც მოხდება ამ მატრიცების ამორჩევა, აუცილებლად შედგებოდეს ურთიერთკომუტატიური მატრიცებისაგან, რაც იმას ნიშნავს, რომ

$$A_1\times A_2 \equiv A_2\times A_1\ , \qquad (2.6)$$

წინააღმდეგ შემთხვევაში, X და Y მხარეები ერთიდაიგივე K გასაღებს ვერ მიიღებენ, რაც აუცილებელია წარმოდგენილი მეთოდისათვის.

მაშასადამე, ჯერ უნდა შეიქმნას კომუტატიურ მატრიცათა სიმრავლე და მხოლოდ მას შემდეგ, X და Y მხარეები ამ სიმრავლიდან აირჩევენ ნებისმიერ A_1 და A_2 საიდუმლო მატრიცებს და შემდგომ გამოიყენებენ ამ ამოცანისათვის.

ე.ი. შიფრაციის მედეგობა ეფუძნება A_1 და A_2 საიდუმლო მატრიცების, მოცემული მატრიცათა სიმრავლიდან ამორჩევის სირთულეს, მიუხედავად იმისა, რომ წინასწარ ცნობილია კომუტატიურ მატრიცათა სიმრავლე, ასევე ცნობილია განზომილება და შესაბამისად ცნობილია e ვექტორის სიგრძეც, ცნობილია e ვექტორში და საერთოდ მატრიცათა სიმრავლეში შემავალი თითოეული მატრიცის შემცველი ელემენტები, რომელთა მნიშვნელობა არ აღემატება P მარტივ რიცხვს, რომლის მნიშვნელობაც წინასწარ გაცხადებულია, მაგრამ მაინც, მიუხედავად ამისა, შეუძლებელია ასეთი მატრიცების აგება ცალსახად და, საერთოდ, ასეთი მატრიცების სიმრავლე არის $M^{(n\times n)}$, სადაც M – მატრიცაში შემავალი ელემენტების სიდიდეა, n კი – განზომილება. ვთქვათ, M=10, ხოლო n=6, ე.ი. გვაქვს 10^{36} სიმრავლე, ეს კი ისეთი სიმრავლეა საიდანაც, რეალურ დროში, შეუძლებელია მატრიცის ამორჩევა.

ე.ი. რაც მეტია e ვექტორის სიგრძე ანუ შესაბამისად მეტია მატრიცის განზომილებაც, მით ძნელია და საერთოდ შეუძლებელი ხდება ამ მეთოდის გატეხვა. განზომილების გაზრდასთან ერთად, საკმაოდ სწრაფად იზრდება მატრიცათა სიმრავლეში შემავალი მატრიცათა რაოდენობა და შესაბამისად, მესამე Z სუბიექტისათვის, მით უფრო რთულდება და ეტაპობრივად შეუძლებელი ხდება, მოცემული მატრიცათა სიმრავლიდან, იმ ორი კონკრეტული A_1 და A_2 საიდუმლო მატრიცების ამორჩევა, რასაც გვიდასტურებს ამ მეთოდის მახასიათებლები, იხ. ცხრილი 2. მიღებული ასიმეტრიული მეთოდის მახასიათებლები.

№	**მახასიათებლები**	**ამოცანის შედეგები**
1.	შიფრაციის სიჩქარე	მაღალი
2.	გამოყენებული ფუნქცია	გამრავლება
3.	გასაღების სიგრძე	6 განზ. მატრიცა
4.	კრიპტოანალიზის სირთულე	სიმრავლიდან ამორჩევა
5.	გასაღების გენერაციის დრო	წამები
6.	გასაღების ტიპი	ასიმეტრიული

ცხრილი 2.

ნათლად ჩანს, რომ განხილული ამოცანა იძლევა კარგ შედეგს: მაღალი შიფრაციის სიჩქარე, გამრავლების ფუნქცია, გასაღების სიგრძე დაბალი, მატრიცათა სიმრავლიდან ამორჩევის სირთულე, გასაღების გენერაციისათვის საჭირო წამები, გასაღების ტიპი – ასიმეტრიული სისტემა.

ზემოაღნიშნულიდან გამომდინარე, შეიძლება ვთქვათ, რომ ეს ამოცანა გვაძლევს კარგ შედეგს.

ამოცანაში წარმოდგენილი მეთოდი და შესაბამისად, მასში განხილული ალგორითმი არის საიმედო, მის სირთულეს წარმოადგენს მატრიცათა სიმრავლიდან A_1 და A_2 მატრიცების ამორჩევას, P მოდულით.

ამ მეთოდის მედეგობა ეფუძნება A_1 და A_2 მატრიცების ამორჩევის სირთულეს. ამორჩევის პროცესი კი საკმაოდ დაცულია და "განსაზღვრულ" (კონკრეტულ) დროში შეუძლებელია მათი ამორჩევა.

ე.ი. ამოცანაში აღწერილი, ასიმეტრიული სისტემის ახალი მეთოდი, გამოირჩევა მაღალი მედეგობით [97-109].

მაგალითი: $e = (0,1,1)$

$$A_1 = \begin{array}{|c|c|c|}\hline 0 & 1 & 1 \\ \hline 1 & 1 & 0 \\ \hline 1 & 0 & 0 \\ \hline \end{array}$$

$$A_2 = A_1^2 = \begin{array}{|c|c|c|}\hline 0 & 1 & 1 \\ \hline 1 & 1 & 0 \\ \hline 1 & 0 & 0 \\ \hline \end{array} \times \begin{array}{|c|c|c|}\hline 0 & 1 & 1 \\ \hline 1 & 1 & 0 \\ \hline 1 & 0 & 0 \\ \hline \end{array} = \begin{array}{|c|c|c|}\hline 0 & 1 & 0 \\ \hline 1 & 0 & 1 \\ \hline 0 & 1 & 1 \\ \hline \end{array} \pmod 2$$

X მხარე (2.1) ფორმულით გამოთვლის –

$$eA_1 = \begin{array}{|c|c|c|}\hline 0 & 1 & 1 \\ \hline \end{array} \times \begin{array}{|c|c|c|}\hline 0 & 1 & 1 \\ \hline 1 & 1 & 0 \\ \hline 1 & 0 & 0 \\ \hline \end{array} = \begin{array}{|c|c|c|}\hline 0 & 1 & 0 \\ \hline \end{array} \pmod 2 = b_1$$

Y მხარე (2.2) ფორმულით მიიღებს გასაღებს –

$$b_1A_2 = \begin{array}{|c|c|c|}\hline 0 & 1 & 0 \\ \hline \end{array} \times \begin{array}{|c|c|c|}\hline 0 & 1 & 0 \\ \hline 1 & 0 & 1 \\ \hline 0 & 1 & 1 \\ \hline \end{array} = \begin{array}{|c|c|c|}\hline 1 & 0 & 1 \\ \hline \end{array} \pmod 2 = K_1$$

Y მხარე (2.3) – ით მიიღებს –

$$eA_2 = \begin{array}{|c|c|c|}\hline 0 & 1 & 1 \\ \hline \end{array} \times \begin{array}{|c|c|c|}\hline 0 & 1 & 0 \\ \hline 1 & 0 & 1 \\ \hline 0 & 1 & 1 \\ \hline \end{array} = \begin{array}{|c|c|c|}\hline 1 & 1 & 0 \\ \hline \end{array} \pmod 2 = b_2$$

X მხარე (2.4) ფორმულით მიიღებს გასაღებს –

$$b_2A_1 = \begin{bmatrix} 1 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \end{bmatrix} \pmod 2 = K_2$$

$$\mathbf{K_1 = K_2 = K.}$$

რაც გვინდოდა დაგვემტკიცებინა, მაგრამ ერთიდაიგივე K გასაღები მიიღება მხოლოდ იმ შემთხვევაში, როცა მატრიცები არის კომუტატიური ანუ

$$A_1 \times A_2 = A_2 \times A_1$$

$$A_1A_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} \pmod 2$$

$$A_2A_1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} \pmod 2$$

აღნიშნულ მეთოდში, როგორც ზემოთ არის განხილული, მოცემულია მოდული, მაშასადამე ცნობილია მატრიცის ელემენტების სიდიდე M; მოცემულია ვექტორი, ე.ი. ცნობილია განზომილება n, როგორც მატრიცის ასევე ვექტორის; აქედან გამომდინარე შესაძლებელია ინფორმაციის დაყოფა ზუსტად ბლოკებად არაკანონიერი მომხმარებლის მიერ; ცნობილია მატრიცათა სიმრავლე $M^{n \times n}$, საიდანაც ხდება მათი ამორჩევა.

საკმარისია M = 10, n = 6, ამ შემთხვევაში მატრიცათა სიმრავლე იქნება 10^{36}, ეს კი იმდენად დიდი რიცხვია, რომ ასეთი სიმრავლიდან იმ ორი კონკრეტული მატრიცის ამორჩევა, რეალურ დროში, არის შეუძლებელი.

მიუხედავად იმისა, რომ ყველა სიდიდე ცნობილია გარდა იმ ორი კონკრეტული მატრიცისა, ამ მეთოდის გატეხვა შეუძლებელია არაკანონიერი მომხმარებლის მიერ.

მაშასადამე, ამ მეთოდის მაღალი მედეგობა ეფუძნება A_1 და A_2 მატრიცათა ამორჩევის სირთულეს, მოცემული მატრიცათა სიმრავლიდან.

2.2. ასიმეტრიული სისტემის მატრიცული მეთოდის სინთეზი სიმეტრიულ მეთოდთან

ამოცანა 2. გვაქვს ორი X და Y მხარეები, რომელთა შორის ხდება ერთიდაიგივე გასაღების დაფიქსირება და შემდგომ კი ამ გასაღებით, ინფორმაციის დაშიფვრა-გაშიფვრა და შესაბამისად გაცვლა.

ამ მეთოდით ხდება სიმეტრიული და ასიმეტრიული მეთოდების სინთეზი.

პირველ რიგში სანამ დაფიქსირდება გასაღები, სიმეტრიული მეთოდის გამოყენებით, ანუ კურიერით ხდება e ვექტორის გაცვლა. ამის შემდეგ უკვე ასიმეტრიული (ღია) მეთოდით ხდება ყველა დანარჩენი ოპერაციების ჩატარება.

გაცხადებულია (ცნობილია) P – მარტივი რიცხვი, ე.ი. ცნობილია ვექტორის და მატრიცის ელემენტების სიდიდე.

აგრეთვე ყველასათვის ცნობილია მატრიცათა სიმრავლე, საიდანაც ხდება მატრიცათა ამორჩევა, რომლებიც გამოიყენება, რათა ორივე X და Y მხარეებმა მიიღონ ერთიდაიგივე K გასაღები.

X მხარე ირჩევს თავის A_1 საიდუმლო მატრიცას და კავშირის ღია არხით გადასცემს Y მხარეს გამოთვლილ y_1 მნიშვნელობას

$$y_1 \equiv e \times A_1 \bmod P . \qquad (2.7)$$

Y-ი შეარჩევს თავის A_2 საიდუმლო მატრიცას და აფორმირებს K გასაღებს:

$$K = (e \times A_1) \times A_2 \equiv e \times A_1 \times A_2 \bmod P . \qquad (2.8)$$

თავის მხრივ Y მხარე X მხარეს ღია არხით გადასცემს გამოთვლილ y_2 მნიშვნელობას

$$y_2 \equiv e \times A_2 \bmod P , \qquad (2.9)$$

ხოლო X-ი აფორმირებს K გასაღებს:

$$K = (e\times A_2)\times A_1 \equiv e\times A_2\times A_1 \bmod P . \quad (2.10)$$

მაშასადამე, ორივე მხარემ მიიღო ერთიდაიგივე K გასაღები:

$$K = e\times A_1\times A_2 \bmod P \equiv e\times A_2\times A_1 \bmod P . \quad (2.11)$$

შიფრაციის მედეგობა (საიმედოობა) ეფუძნება, A_1 და A_2 საიდუმლო მატრიცების, მატრიცათა სიმრავლიდან ამორჩევის სირთულეს და კიდევ გარდა ამისა, რადგან უცნობია e ვექტორი, შესაბამისად უცნობია განზომილება. აქედან გამომდინარე არაკანონიერი მომხმარებელი ვერ მოახდენს ინფორმაციის დაყოფას ბლოკებად, რაც მას სერიოზულ პრობლემებს შეუქმნის. შესაბამისად ვერ მიხვდება, რომელი განზომილების მატრიცები გამოიყენოს, რომელი სიმრავლიდან. e ვექტორის დასაიდუმლოებამ ამოცანის ისედაც მაღალი მედეგობა კიდევ უფრო გაზარდა, იხ. ცხრილი 3. სიმეტრიული და ასიმეტრიული მატრიცული მეთოდის სინთეზის შედეგად მიღებული ახალი მეთოდის მახასიათებლები.

№	**მახასიათებელი**	**ამოცანის შედეგები**
1.	შიფრაციის სიჩქარე	საშუალო
2.	გამოყენებული ფუნქცია	გამრავლება
3.	გასაღების სიგრძე	6 განზ. მატრიცა
4.	კრიპტოანალიზის სირთულე	სიმრავლიდან ამორჩევა
5.	გასაღების გენერაციის დრო	წამები-წუთები
6.	გასაღების ტიპი	სინთეზი

ცხრილი 3.

ე.ი. ნათლად ჩანს, რომ განხილული ამოცანა იძლევა კარგ შედეგს: საშუალო სიჩქარე, გამრავლების ფუნქცია, გასაღების სიგრძე დაბალი, მატრიცათა სიმრავლიდან ამორჩევის სირთულე, გასაღების გენერაციისათვის საჭირო წუთები, გასაღების ტიპი – სიმეტრიული და ასიმეტრიული სისტემების სინთეზი.

ამოცანაში წარმოდგენილი მეთოდი და შესაბამისად, მასში განხილული ალგორითმი არის საიმედო.

ამ მეთოდის მედეგობა ეფუძნება A_1 და A_2 მატრიცების ამორჩევის სირთულეს $M^{n\times n}$ სიმრავლიდან და კიდევ ვექტორთა ამორჩევა n! სიმრავლიდან.. ამორჩევის პროცესი კი საკმაოდ დაცულია და "განსაზღვრულ" (კონკრეტულ) დროში შეუძლებელია მათი ამორჩევა.

ე.ი. ამოცანაში აღწერილი, სიმეტრიული და ასიმეტრიული სისტემების სინთეზის ახალი მეთოდი, გამოირჩევა მაღალი მედეგობით [90, 92, 93-96, 105, 106, 108].

2.3. მატრიცის დასაიდუმლოება

ამოცანა 3. ზემოთ აღნიშნულ მეთოდებში შესაძლოა კიდევ მცირე ცვლილება შევიტანოთ, მივიღებთ მეთოდს, რომელშიც გასაღების გენერაცია მოხდება ძალიან სწრაფად, მილიწამებში.

ამოცანა 2-ში უცნობია ვექტორი, დანარჩენი ყველაფერი დარჩა იგივე და საიმედოობა ძალიან გაიზარდა, რაც გამოიწვია ვექტორის დასაიდუმლოებამ.

ამოცანა: რადგან სიმეტრიული მეთოდი უკვე გამოვიყენეთ ვექტორის გადასაცემად, ამიტომ უმჯობესი იქნება, რომ მატრიცის გადაცემაც მოხდეს საიდუმლოდ.

ე.ი. სიმეტრიული მეთოდის ანუ კურიერის გამოყენებით ერთდროულად მოხდება ვექტორის და მატრიცის გადაცემა, ამის შემდგომ კი გასაღების დაფიქსირება და ინფორმაციის შიფრაცია-დეშიფრაცია მოხდება ანალოგიურად, როგორც ეს ზემოთ არის აღნიშნული.

რადგან მატრიცას გადავცემთ საიდუმლოდ, მიმღები მილიწამებში მოახდენს მიღებული მატრიცის კომუტატიური მატრიცის პოვნას, შესაბამისად მილიწამებში მოახდენს გასაღების გენერაციას. ამის შემდეგ კი შიფრაციის დრო კი არ შეიცვლება, რჩება იგივე, მაგრამ ჯამში შეგვიძლია ვთქვათ, რომ შიფრაციის სიჩქარე მაღალია.

აღნიშნულ მეთოდში გასაღების გენერაციის დრო არის მილიწამები, რაც არის საკმაოდ მცირე ვიდრე წინა მეთოდებთან შედარებით.

2.4. არსებული და მიღებული ახალი მეთოდების შედარებითი ანალიზი

როგორც ზემოთ არის აღნიშნული **სიმეტრიული** მეთოდები ანუ დახურული მეთოდები კურიერის გამოყენებით არის ძალიან სწრაფი და მაღალი მახასიათებლებით ხასიათდება, სამაგიეროდ მედეგობა არის დაბალი. მაგრამ თუკი გვინდა, რომ რაღაც ინფორმაცია გადავცეთ ერთჯერადად, ან ინფორმაცია არის მცირე ზომის, ან გვინდა რომ ინფორმაციის მიწოდება მიმღებ მხარეს მოხდეს რაც შეიძლება ძალიან სწრაფად, მაშინ უფრო გამოყენებადია სიმეტრიული მეთოდები. თუმცა-ღა ვიჟინერის მეთოდი სხვა დანარჩენი სიმეტრიულ მეთოდებთან შედარებით ყველაზე საიმედოა.

რაც შეეხება **ასიმეტრიულ** მეთოდებს, როგორიცაა დიფი-ჰელმანის მეთოდი, ელგამალის ალგორითმი, ხელმოწერის ალგორითმი და ა.შ., მათი საიმედოობა არის გაცილებით მაღალი ვიდრე სიმეტრიულის, მაგრამ სამაგიეროდ შიფრაციის სიჩქარე არის დაბალი, რაც ნათლად ჩანს მის მახასიათებლებში. მაგრამ თუკი, გვინდა რომ გადავაგზავნოთ დიდი ზომის ინფორმაცია და ჩვენთვის ამ შემთხვევაში უფრო მეტი მნიშვნელობა აქვს საიმედოობას ვიდრე შიფრაციის სიჩქარეს, მაშინ ვიყენებთ ასიმეტრიულ მეთოდებს.

ამ ორ მეთოდში ჩანს რომ, თუ ვიგებთ ერთ რომელიმე მახასიათებელში ვაგებთ მეორეში ან პირიქით.

ჩვენს მიერ კი, განხილულ და მიღებულ იქნა სხვადასხვა მეთოდები:

1. დიფი-ჰელმანის მეთოდის გამოყენებით შევქმენით ახალი მეთოდი, ოღონდ დიფი-ჰელმანის ახარისხება შევცვალეთ **მატრიცაზე გამრავლებით**. ახარისხებას უფრო მეტი დრო სჭირდება (მამრავლებად დაშლა) ვიდრე მატრიცაზე გამრავლებას, ანუ შიფრაციის სიჩქარე გაიზარდა, ასევე გაიზარდა გასაღების გენერაციის დროც, და თანაც მეთოდი არის ასიმეტრიული.

2. მეორე შემთხვევაში გამოვიყენეთ ორივე მეთოდის **სინთეზი**, სიმეტრიულიც და ასიმეტრიულიც. ვექტორის გადაცემა ხდება დახურული არხით და შემდგომ კი, ყველა პროცედურა ხორციელდება ღია

არხით. ამ ფაქტმა მოგვცა, ის რომ შიფრაციის სიჩქარე შემცირდა, მაგრამ სამაგიეროდ კიდევ უფრო გაიზარდა მედეგობა. განზომილება გახდა უცნობი, რის გამოც არაკანონიერი მომხმარებელი ვერ შეძლებს ინფორმაციის დაყოფას ბლოკებად, რაც ინფორმაციის გაშიფვრისათვის ერთ-ერთი მთავარი ეტაპია.

3. მესამე შემთხვევაში კი, რადგან უკვე მეორე მეთოდში გამოყენებული გვქონდა ორივე მეთოდი, ამ შემთხვევაში კი ერთდროულად მოვახდინეთ დახურული არხით, ანუ კურიერით, **ვექტორის და მატრიცის გადაცემა**, რამაც მოგვცა საუკეთესო შედეგი. მიმღები მილიწამებში აფიქსირებს კომუტატიურ მატრიცას და შესაბამისად გასაღებსაც. ანუ გასაღების გენერაციის დრო კიდევ უფრო შემცირდა, სიჩქარე გაიზარდა; მაგრამ ეს არ მომხდარა მედეგობის ხარჯზე. შეიძლება ითქვას, რომ მედეგობა უცვლელია ანუ საკმაოდ მაღალია და შესაბამისად მეთოდიც საიმედოა.

II თავის დასკვნა

ჩვენს მიერ შექმნილი იქნა ახალი მეთოდები, არსებულ მეთოდებზე დაყრდნობით, რომლებიც განხილულ იქნა პირველ თავში.

გამოყენებულ იქნა სიმეტრიული და ასიმეტრიული სისტემები, მოვახდინეთ მათი სინთეზი.

პირველი მეთოდით განვახორციელეთ გასაღების მიღება და ინფორმაციის დაშიფვრა ღია არხით, ანუ გამოიყენებულ იქნა ასიმეტრიული მეთოდი, კერძოდ – დიფი-ჰელმანის მეთოდი. აღნიშნულ მეთოდში გამოყენებული ახარისხების ფუნქცია, შეცვლილი იქნა მატრიცაზე გამრავლებით.

მეორე მეთოდში, სიმეტრიული (დახურული) არხით მოვახდინეთ ვექტორის გაცვლა, შემდგომ კი ღია არხით ორივე მომხმარებელი იღებს გასაღებს და მიღებული გასაღები გამოიყენება ინფორმაციის დაშიფვრისათვის და შესაბამისად გაშიფვრისათვისაც, როგორც პირველ

მეთოდში. ვექტორის დასაიდუმლოებამ, კიდევ უფრო გაზარდა საიმედოობა, რადგან არაკანონიერი მომხმარებლისათვის უცნობი ხდება განზომილება, აქედან გამომდინარე იგი ინფორმაციას ვერ დაყოფს ბლოკებად, მისთვის უცნობი იქნება ასევე რა განზომილების მატრიცა უნდა გამოიყენოს და შესაბამისად ვერ გაშიფრავს ინფორმაციას, რეალურ დროში, თუნდაც რომ, იგი მთლიანად ჩაუვარდეს ხელში.

მესამე მეთოდში კი – რადგან დახურული არხი უკვე გამოყენებულ იქნა, ვექტორთან ერთად გადავცემთ საიდუმლო მატრიცასაც. მიმღები მილიწამებში აგებს კომუტატიურ მატრიცას და გასაღებიც ორივე მხარეს დაფიქსირდება ძალიან სწრაფად.

ე.ი. მივიღეთ სხვადასხვა მეთოდები, რომლებიც ხასიათდება უკეთესი მახასიათებლებით, ვიდრე არსებული: გამოირჩევა მაღალი სიჩქარით და საიმედოობით, გამოიყენება გადანაცვლების ფუნქცია, კრიპტოსირთულეს წარმოადგენს მატრიცათა სიმრავლიდან ამორჩევის სირთულე.

აღნიშნული მეთოდების ფუნქციონირებისათვის აუცილებელია და საკმარისი, რომ მატრიცები იყოს კომუტატიური, ანუ ურთიერთგადასმადი.

აღნიშნულ მატრიცათა სიმრავლის შექმნა და გამოყენება მოცემულია მესამე თავში.

ექსპერიმენტული ნაწილი

თავი III.

კომუტატიური მატრიცათა სიმრავლის გამოყენება ახალი მეთოდისათვის

ამოცანა მდგომარეობს შემდეგში: ავაგოთ სიმეტრიული და კომუტატიური მატრიცების სიმრავლე. შემდგომ ეს სიმრავლე გამოვიყენოთ კრიპტოგრაფიაში, კერძოდ ზემოთ აღნიშნულ მეთოდებში. მოვახდინო ინფორმაციის დასაიდუმლოება ე.ი. დაშიფვრა ამ სიმრავლიდან აღებული ნებისმიერი მატრიცის გამოყენებით და მიმღებმა უნდა მოახდინოს მიღებული ინფორმაციის გაშიფვრა, ამ სიმრავლიდან ნებისმერი მატრიცის აღებით.

3.1. სხვადასხვა სახის მატრიცების განხილვა

მატრიცა არის ნულოვანი, თუ მისი ყველა ელემენტი ნულის ტოლია.

მატრიცა არის ერთეულოვანი, თუ მისი დიაგონალზე მოთავსებული ელემენტები არის ერთის ტოლი.

მატრიცა არის გადაუგვარებელი ნიშნავს, რომ აქვს შებრუნებული, ე.ი. დეტერმინანტი არ უდრის ნულს.

$$A\,A^{-1} = 1. \tag{3.1}$$

A მატრიცას ტრანსპონირებული მატრიცა აღინიშნება A^T და აკმაყოფილებს პირობას

$$A\,A^T = 0\,. \tag{3.2}$$

მატრიცა არის სიმეტრიული, თუ იგი არ იცვლება ტრანსპონირების დროს, ანუ

$$A = A^T\,, \tag{3.3}$$

$$(A^T)^T = A\,. \tag{3.4}$$

მატრიცა არის ორთოგონალური, თუ

$$A^{-1} = A^T\,. \tag{3.5}$$

მატრიცა არის კვადრატული, თუ მისი სვეტებისა და სტრიქონების რაოდენობა ტოლია. იმისათვის, რომ შევქმნათ კომუტატიურ მატრიცათა სიმრავლე, პირველ რიგში უნდა გავითვალისწინოთ, რომ ყოველი მატრიცა უნდა იყოს კვადრატული

$$A_{mn} = \begin{array}{|c|c|c|c|c|} \hline A_{11} & A_{12} & A_{13} & \dots & A_{1n} \\ \hline A_{21} & A_{22} & A_{23} & \dots & A_{2n} \\ \hline A_{31} & A_{32} & A_{33} & \dots & A_{3n} \\ \hline \dots & \dots & \dots & \dots & \dots \\ \hline A_{m1} & A_{m2} & A_{m3} & \dots & A_{mn} \\ \hline \end{array} \qquad (3.6)$$

როცა m = n ანუ სვეტების და სტრიქონების რაოდენობა ტოლია, ანუ მატრიცა კვადრატულია, მაშინ შესაძლოა კომუტატიური მატრიცების აგება [1-9].

3.2. კომუტატიური-კვადრატული მატრიცები

ე.ი. იმისათვის რომ მატრიცები იყოს კომუტატიური, ერთ-ერთი აუცილებელია პირობაა, რომ მატრიცები იყოს კვადრატული.

კვადრატული მატრიცის ზოგადი სახე:

$$\left\| \begin{array}{l} a_{11}\ a_{12}\ \dots\ a_{1n} \\ a_{21}\ a_{22}\ \dots\ a_{2n} \\ \dots\dots\dots\quad \dots\dots\dots \\ a_{m1}\ a_{m2}\ \dots\ a_{mn} \end{array} \right\| \qquad (3.7)$$

როცა m=n –ს, ასეთ მატრიცას ეწოდება კვადრატული. პირველ ინდექსად ყოველთვის არის სტრიქონების რაოდენობა, მეორე კი – სვეტების. ე.ი. m არის სტრიქონების რაოდენობა, n – სვეტების [28, 62, 90].

აღნიშნული მატრიცა მოკლედ შეგვიძლია ჩავწეროთ:

$$\left\| a_{ik} \right\| \quad (i = 1, 2, ..., m;\ k = 1, 2, ..., n).$$

შეგვიძლია მატრიცა ჩავწეროთ ასეთი სახით: $A = \left\| a_{ik} \right\|_1^n$

ვთქვათ გვაქვს ორი მატრიცა A და B.

განსაზღვრება: ორი კვადრატული მატრიცის $A = \left\| a_{ik} \right\|$ და $B = \left\| b_{ik} \right\|$ ჯამი უდრის მესამე $C = \left\| c_{ik} \right\|$ მატრიცას იგივე m×n განზომილებით:

$$C = A + B ,$$

თუ $c_{ik} = a_{ik} + b_{ik}$ (i = 1, 2, ..., m; k = 1, 2, ..., n).

მაგალითად: $\left\| a_1 a_2 a_3 \right\| + \left\| c_1 c_2 c_3 \right\| = \left\| a_1 + c_1, a_2 + c_2, a_3 + c_3 \right\|$,
$\left\| b_1 b_2 b_3 \right\| \quad \left\| d_1 d_2 d_3 \right\| \quad \left\| b_1 + d_1, b_2 + d_2, b_3 + d_3 \right\|$

$$\alpha \left\| a_1 a_2 a_3 \right\| = \left\| \alpha a_1 \alpha a_2 \alpha a_3 \right\|,$$
$$\left\| b_1 b_2 b_3 \right\| \quad \left\| \alpha b_1 \alpha b_2 \alpha b_3 \right\|$$

აქედან ჩანს რომ:

$$\left.\begin{array}{c} a(A + B) = aA + aB \\ (a + \beta)A - aA + \beta A \\ (a\beta)A = a(\beta A) \\ A - B = A + (-1)B \end{array}\right\} \qquad (3.8)$$

მატრიცების გამრავლება:

$$\left\| a_1 a_2 a_3 \right\| \times \left\| \begin{matrix} c_1 d_1 e_1 \\ c_2 d_2 e_2 \\ c_3 d_3 e_3 \end{matrix} \right\| = \left\| a_1 c_1 + a_2 c_2 + a_3 c_3, a_1 d_1 + a_2 d_2 + a_3 d_3, a_1 e_1 + a_2 e_2 + a_3 e_3 \right\| \qquad (3.9)$$
$$\left\| b_1 b_2 b_3 \right\| \quad \left\| b_1 c_1 + b_2 c_2 + b_3 c_3, b_1 d + b_2 d_2 + b_3 d_3, b_1 e_1 + b_2 e_2 + b_3 e_3 \right\|$$

მაგალითი: $\left\| 1,2 \right\| \times \left\| 2,0 \right\| = \left\| 1 \cdot 2 + 2 \cdot 3, 1 \cdot 0 + 2 \cdot 1, \right\| = \left\| 8,2 \right\|$
$\left\| 3,4 \right\| \quad \left\| 3,1 \right\| \quad \left\| 3 \cdot 2 + 4 \cdot 3, 3 \cdot 0 + 4 \cdot 1 \right\| \quad \left\| 18,4 \right\|$

მაგრამ თუ გავითვალისწინებთ მოდულს, და ავიღებთ ხუთის ტოლს, მაშინ მივიღებთ

$$\left\| 8,2 \right\| \bmod(5) = \left\| 3,2 \right\|$$
$$\left\| 18,4 \right\| \quad \left\| 3,4 \right\|$$

კვადრატული მატრიცის თვისებები:

1. კვადრატული მატრიცის ნებისმიერი ორი სვეტის ან სტრიქონის გადაადგილებით მივიღებთ სხვა მატრიცას, მაგრამ განზომილება არ შეიცვლება.

2. თუ კვადრატულ მატრიცას აქვს ორი ერთნაირი სვეტი ან სტრიქონი, მაშინ მისი დეტერმინანტი ნულის ტოლია.

3. თუ კვადრატული მატრიცის ორი რომელიმე სვეტის ან სტრიქონის ელემენტები პროპორციულია, მაშინ მისი დეტერმინანტი ნულის ტოლია.

4. თუ მატრიცის სვეტი ან სტრიქონი არის რომელიმე სხვა სვეტის ან სტრიქონის წრფივი კომბინაცია, მაშინ ასეთი მატრიცის დეტერმინანტი ნულის ტოლია.

5. საერთო მამრავლი სვეტის ან სტრიქონის შეგვიძლია გამოვყოთ

$$\begin{vmatrix} \lambda a_{11} & a_{12} \\ \lambda a_{21} & a_{22} \end{vmatrix} = \lambda a_{11}a_{22}-\lambda a_{21}a_{12} = \lambda(a_{11}a_{22}-a_{21}a_{12}) = \lambda \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$$

6. კვადრატული მატრიცის დეტერმინანტი არ შეიცვლება, თუ რომელიმე სვეტის ან სტრიქონის ელემენტებს დავამატებთ მისი სტრიქონის ან სვეტის შესატყვის ელემენტებს, ნებისმიერ რიცხვზე გამრავლებით:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21}+\lambda a_{11} & a_{22}+\lambda a_{12} \end{vmatrix} = a_{11}(a_{22}+\lambda a_{12})-a_{12}(a_{21}+\lambda a_{11}) =$$

$$= a_{11}a_{22} - a_{12}a_{21} + \lambda(a_{12}a_{11} - a_{12}a_{11}) = a_{11}a_{22} - a_{12}a_{21}$$

7. კვადრატული მატრიცის ნებისმიერი სვეტებისა და სტრიქონების ელემენტების ჯამი ალგებრული დამატებებით მისი შესატყვისი სვეტებითა და სტრიქონებით ნულის ტოლია.

$$a_{i1}A_{j1} + a_{i2}A_{j2} + \ldots + a_{im}A_{jn} = 0, \text{ როცა } i \neq j$$

8. დეტერმინანტი ორი მატრიცის ნამრავლისა უდრის ამ ორი მატრიცის დეტერმინანტთა ნამრავლს

$$\det(AB) = \det(A) \times \det(B)$$

A, B, C მატრიცები უნდა აკმაყოფილებდნენ პირობებს, როგორიცაა: კომუტატიურობა, ასოციაციურობა და დისტრიბიციულობა:

$$\left.\begin{aligned} A + B &= B + A \\ A + (B + C) &= (A + B) + C \\ (F + G)(A + B) &= FA + FB + GA + GB \end{aligned}\right\} \qquad (3.10)$$

ვთქვათ A, B და C მატრიცები აკმაყოფილებენ შემდეგ თვისებებს:

$$\left.\begin{aligned} (A\,B)\,C &= A\,(B\,C) \\ A\,(B + C) &= AB + AC \\ (A + B)\,C &= AC + BC \\ (AB)^{T} &= B^{T} A^{T} \end{aligned}\right\} \qquad (3.11)$$

A(s B) = s A B სადაც s არის რიცხვი [9, 39, 57, 106, 109].

A და B ორი მატრიცა აკმაყოფილებს შემდეგ პირობას: AB ნამრავლზე შეგვიძლია ვთქვათ, რომ “A მატრიცა მრავლდება B მატრიცაზე მარცხნიდან” ან “B მატრიცა მრავლდება A მატრიცაზე მარჯვნიდან”, თუ ორივე მატრიცა არის კვადრატული და ერთიდაიგივე განზომილების, მაშინ შეგვიძლია ვთქვათ, რომ ორივე ნამრავლი AB და BA, მიუხედავად იმისა, რომ მათი ელემენტები განსხვავებულია ერთმანეთისაგან

$$AB = BA\,. \qquad (3.12)$$

ასეთ მატრიცებს ეწოდება ურთიერთკომუტატიური მატრიცები ანუ გადასმადი.

$$AB = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} \times \begin{vmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{vmatrix} =$$

$\sum_{j=1}^{3} a_{1j}b_{j1}$	$\sum_{j=1}^{3} a_{1j}b_{j2}$	$\sum_{j=1}^{3} a_{1j}b_{j3}$
$\sum_{j=1}^{3} a_{2j}b_{j1}$	$\sum_{j=1}^{3} a_{2j}b_{j2}$	$\sum_{j=1}^{3} a_{2j}b_{j3}$
$\sum_{j=1}^{3} a_{3j}b_{j1}$	$\sum_{j=1}^{3} a_{3j}b_{j2}$	$\sum_{j=1}^{3} a_{3j}b_{j3}$

(3.13)

თუ A და B მატრიცების რანგი ტოლია, მაშინ ასეთი მატრიცები არის ექვივალენტური r (A) = r (B) [15, 18, 26, 29, 37-42].

ჩვენს მიერ შექმნილ მეთოდში გამოიყენება სწორედ ასეთი თვისებების მქონე მატრიცები. გარდა ამისა ჩვენს ამოცანაში ვექტორს ვამრავლებთ მატრიცაზე. შეგვიძლია წარმოვადგინოთ ვექტორი როგორც ერთგანზომილებიანი სვეტის მქონე მატრიცა.

a	b	c		x		a	b	c		x	0	0
d	e	f	×	y	=	d	e	f	×	y	0	0
g	h	i		z		g	h	i		z	0	0

და საერთოდ აღნიშნული მატრიცა

a	b	c
d	e	f
g	h	i

შესაძლოა წარმოვადგინოთ შემდეგი სახით:

a	b	c	0	0
d	e	f	0	0
g	h	i	0	0
0	0	0	0	0
0	0	0	0	0

მიღებული ხუთ განზომილებიანი მატრიცა და ზემოთ აღნიშნული სამ განზომილებიანი მატრიცა, არის აბსოლუტურად ერთიდაიგივე.

გავითვალისწინეთ რა, ზემოთ აღნიშნული მატრიცათა ყველა თვისებები და მივიღეთ შემდეგი შედეგები.

განვიხილოთ მაგალითები:

1) თავიდან ავიღოთ პატარა განზომილების მატრიცები, მაგრამ მალე იწყებს მატრიცა გამეორებას. ე.ი. ბაზა არ იქმნება.

2) შემდგომში დავაკვირდეთ მერამდენე მატიცაზე იწყებს გამეორებას, ასევე დავაკავშიროთ მოდულსაც, მაგრამ რაიმე კანონზომიერებას ვერ მივაკვლევთ.

3) შემდეგ ეტაპზე ვცვალოთ – ხან განზომილება – ხან მოდული და დავაკვირდეთ გამეორების პრინციპს, მივალთ ერთ დასკვნამდე, რომ მოდულის გაზრდა უფრო დიდ ეფექტს გვაძლევს ვიდრე განზომილების გაზრდა, რაც იმას ნიშნავს, რომ როცა განზომილებას ვზრდით და მოდულს იგივეს ვტოვებთ მატრიცა მაინც მალე მეორდება, შეიძლება უფრო ადრეც ვიდრე შეცვლამდე, მაგრამ როცა განზომილებას ვტოვებთ იგივეს და გავზარდით მოდულს ე.ი. მატრიცაში შემავალი ელემენტების სიმრავლეს, მაშინ მატრიცა უფრო გვიან იწყებს გამეორებას. აქედან დასკვნა: მოდულის გაზრდა იძლევა უფრო კარგ შედეგს ვიდრე განზომილების გაზრდა.

4) ახალ კი ავიღოთ ისეთი მატრიცები, რომლებიც მოგვცემს ისეთ სიმრავლეს, რომლის რიცხვი იქნება დაახლოებით 10^{30}.

ნებისმიერი მატრიცები: მოდულით 5:

1) განვიხილოთ სხვადასხვა სახის მატრიცები 5-ის მოდულით – როცა n=4 , m=5 ; სიმრავლე იქნება - 5^{16}– სიმრავლე, ცვლადების რიცხვია – 16.

შემდგომ გადავსინჯოთ სიმეტრიული მატრიცები მოდულით 5:

1) n=4 m=5 5^{16} – სიმრავლე, ცვლადების რიცხვია – 16, ამ შემთხვევაშიც კარგი შედეგი მიიღება.

ამის შემდეგ ვნახოთ ნებისმიერი მატრიცები ოღონდ გავზარდოთ მოდული:

1) n=4 , m=11 11^{16} – სიმრავლე, 16 - ცვლადების რიცხვი. გამეორება იწყება ძალიან გვიან, ფაქტიურად შეიძლება ითქვას, რომ ბაზა შედგა.

ახლა კი, უნდა განვიხილოთ ისევ სიმეტრიული მატრიცები, ოღონდ სიმრავლე მიახლოებული უნდა იყოს ზემოდან 10^{30} რიცხვს.

განვიხილოთ ასეთი მაგალითები:

1) ჯერ განვიხილოთ ასეთი მაგალითი:

განზომილება n=5

მოდული d=11

სიმრავლე $N=11^{25}$

მაგრამ ცვალდების რაოდენობა არის 25

2) განვიხილოთ შემდეგი მაგალითი:

განზომილება n=7

მოდული d=11

სიმრავლე $N=11^{49}$

მაგრამ ცვალდების რაოდენობა არის 49.

ამ შემთხვევებშიც გვიან იწყებს მატრიცა გამეორებას, ანუ სიმრავლე იქმნება.

3.3. ნებისმიერი სახის მატრიცები

შემდგომ განვიხილოთ ნებისმიერი სახის მატრიცები, ოღონდ სიმრავლე მიახლოებული უნდა იყოს ზემოდან 10^{30} რიცხვს.

1) პირველ ეტაპზე ვიხილავთ ასეთ მაგალითს:

განზომილება n=7

მოდული d=11

სიმრავლე $N=11^{49}$

მაგრამ ცვალდების რაოდენობა არის 49.

2) შემდეგ ვიხილავთ ასეთ მაგალითს:

განზომილება n=9

მოდული d=11

სიმრავლე $N=11^{81}$

მაგრამ ცვალდების რაოდენობა არის 81.

ფაქტობრივად გამეორება აღარც კი დაფიქსირდა.

შემდგომ განვიხილოთ ნებისმიერად აღებული სიმეტრიული ორობითი მატრიცები:

მოდული = 2

განზომილება = 16

ცვლადების რაოდენობა = $2^{16*8} = 2^{128}$

n=16, m=2 $2^{16\times16}$ – სიმრავლე, 128 – ცვლადების რიცხვი.

ორობითი მატრიცების გამოყენების დროს უფრო კარგი შედეგი მივიღეთ, ფაქტიურად გამეორება შეწყდა და შესაბამისად შეიქმნა მატრიცათა სიმრავლე.

როცა m=10 – მატრიცაში შემავალი ელემენტები (mod)

n=30 – მატრიცის განზომილება

$N=m^n=10^{30}$ – მატრიცათა სიმრავლე.

აქედან ნახევარი არის ჰორიზონტალურად სიმეტრიული და ნახევარი ვერტიკალურად სიმეტრიული მატრიცები. ე.ი. $m^n/2$ – არის სიმეტრიული ჰორიზონტალურად და $m^n/2$ – არის სიმეტრიული ვერტიკალურად. გარდა ამისა ისიც ცნობილია, რომ ერთ მატრიცაში ცვლადების რიცხვია 30*15=450, ეს საკმაოდ დიდი რიცხვია. ძებნის, ანუ სიმრავლიდან ამორჩევის ხანგრძლივობის დრო

$$t=m^n\times N\times T, \qquad (3.14)$$

N – ოპერაციათა ჩატარების რიცხვი,

T – ე.გ.მ.-ის დრო,

t – ეს არის საკმაოდ დიდი რიცხვი და მაღალი მედეგობით ხასიათდება.

აქედან გამომდინარე, თუ შევქმნით ასეთ 10^{30} რიცხვის ტოლ სიმრავლეს ნებისმიერი შემთხვევით აღებული რიცხვების შემცველი და ამავდროულად სიმეტრიული მატრიცებიდან, მივიღებთ სიმრავლის საკმაოდ დიდი რიცხვს, რაც ზემოთ უკვე კარგად ავღნიშნეთ, რომელიც გამოირჩევა დიდი მედეგობით, საკმაოდ დიდი დროის ფაქტორით, საიმედო და შედეგიანი იქნება მისი გამოყენება კრიპტოგრაფიაში.

ამ შემთხვევაში რადგან განვიხილეთ სიმეტრიული მატრიცები მივიღეთ ასეთი შედეგი: ყოველი მეორე ანუ ყოველი კენტი იყო y ღერძის სიმეტრიული, ხოლო ყოველი ლუწი x ღერძის სიმეტრიული, იმას არა აქვს არსებითი მნიშვნელობა, რომელი იყო y ღერძის სიმეტრიული და რომელი x ღერძის სიმეტრიული, მთავარი ფაქტორი არის ის რომ სიმრავლის ნახევარი აღმოჩნდა y ღერძის სიმეტრიული, მეორე ნახევარი კი x ღერძის სიმეტრიული. ე.ი. სიმრავლის ნახევარი - $m^n/2$ არის y

ღერძის სიმეტრიული. ხოლო მეორე ნახევარი - $m^n/2$ არის x ღერძის სიმეტრიული. თუმცა ეს ჯამში სიმრავლეს რიცხობრივად არ ცვლის.

მატრიცაში შემავალი ელემენტების რიცხვი არის n^2 (ზოგადად). ხოლო აქედან უცნობია – $n^2/2$ (ჩვენს შემთხვევაში), რადგან განვიხილეთ სიმეტრიული მატრიცები.

ე.ი. თუ ერთ ვექტორს გავამრავლებთ მატრიცაზე და მივიღებთ რაღაც ვექტორს, გვექნება 30 განტოლება და 450 უცნობი. ასეთი მატრიცების ამოხსნა ცალსახად შეუძლებელია.

ასეთი განზომილების მატრიცები არის საიმედო და გამოირჩევა მაღალი მედეგობით [48-56].

3.4. ნებისმიერი მოდულის მქონე სიმეტრიული მატრიცები

განვიხილოთ სიმეტრიული მატრიცები, ოღონდ სიმრავლე მიახლოებული უნდა იყოს ზემოდან 10^{30} რიცხვს.

თავდაპირველად განვიხილოთ ასეთი მაგალითი:

1) ჯერ განვიხილოთ ასეთი მაგალითი:

განზომილება n=8

მოდული d=11

სიმრავლე $N=11^{64}$, აქედან ნახევარი ცნობილია.

ამიტომ ცვლადების რაოდენობა არის 32

სიმრავლე არის საკმაოდ დიდი რიცხვია $>10^{30}$

$A_1=$

5	7	4	3	3	4	7	5
8	1	2	4	4	2	1	8
9	5	3	4	4	3	5	9
1	8	7	5	5	7	8	1
1	10	4	6	6	4	10	1
9	5	2	8	8	2	5	9
1	3	5	7	7	5	3	1
5	2	8	6	6	8	2	5

A_2=

1	3	7	8	4	7	1	4
7	8	3	1	7	5	7	1
2	7	2	8	8	1	5	0
3	1	6	6	3	8	9	9
3	1	6	6	3	8	9	9
2	7	2	8	8	1	5	0
7	8	3	1	7	5	7	1
1	3	7	8	4	7	1	4

A_3=

7	3	0	7	7	0	3	7
7	8	9	3	3	9	8	7
7	5	2	6	6	2	5	7
8	1	8	2	2	8	1	8
6	5	4	7	7	4	5	6
5	3	5	0	0	5	3	5
1	5	5	3	3	5	5	1
2	9	4	9	9	4	9	2

A_4=

5	7	1	4	0	9	1	4
5	8	1	5	1	9	5	7
4	9	4	6	6	7	5	0
3	1	8	0	3	8	3	1
3	1	8	0	3	8	3	1
4	9	4	6	6	7	5	0
5	8	1	5	1	9	5	7
5	7	1	4	0	9	1	4

A_5=

7	3	0	3	3	0	3	7
1	4	1	7	7	1	4	1
9	3	8	6	6	8	3	9
6	3	2	2	2	2	3	6
0	1	6	9	9	6	1	0
5	3	5	8	8	5	3	5
1	5	5	3	3	5	5	1
6	5	6	7	7	6	5	6

A_6=

5	7	1	4	0	9	1	4
5	8	1	5	1	9	5	7
4	9	4	6	6	7	5	0
3	1	8	0	3	8	3	1
3	1	8	0	3	8	3	1
4	9	4	6	6	7	5	0
5	8	1	5	1	9	5	7
5	7	1	4	0	9	1	4

მალე დაიწყო მატრიცებმა გამეორება.

2) ახლა განვიხილოთ ასეთი მაგალითი:

განზომილება n=10

მოდული d=5

სიმრავლე $N=5^{100}$

მაგრამ ცვლადების რაოდენობა არის 5^{50}

ეს კი არის საკმაოდ დიდი რიცხვი, $>10^{30}$

იხ. დანართი 1. გვ. 87.

3) შემდეგი მაგალითი:

მოდული = 2

განზომილება = 16

ცვლადების რაოდენობა = $2^{16*8=128}$.

იხ. დანართი 2. გვ. 90.

ნებისმიერი სახის მატრიცების დროს, გამეორება გვიან, მაგრამ მაინც დაფიქსირდა.

მატრიცათა გამეორება ფაქტიურად არ დაფიქსირდა და ამავდროულად, სიმრავლე არის $2^{16\times8}$ რაც არის ძალიან დიდი რიცხვი. როგორც ზემოთ უკვე ავღნიშნეთ კრიპტოგრაფიაში 2^{100} ანუ დაახლოებით 10^{30} არის ის სიმრავლე, რომლის გატეხვა, რეალურ დროში, შეუძლებელია.

3.5. შემთხვევითი მატრიცები

$A_1=$

1	2	4	3
1	4	2	3
4	2	3	1
2	4	0	3

ეს არის ნებისმიერად "შემთხვევით" აღებული მატრიცა, სადაც განზომილება n=4, მოდული m=5 სიმრავლე $N= m^{n*n}=5^{16}$

$A_2=$

0	4	0	2
0	4	1	2
0	3	4	1
2	1	4	2

$A_3=$

4	4	2	4
3	1	0	1
2	1	3	0
2	3	2	4

$A_4=$

0	2	2	4
4	1	2	0
2	3	3	3
1	2	4	2

$A_5=$

1	3	1	3
1	0	2	0
1	1	1	1
4	2	3	0

$A_6=$

2	3	2	4
0	0	1	0
2	3	2	1
4	0	4	0

$A_7=$

4	2	2	1
2	3	2	4
2	2	0	1
0	1	0	0

$A_8=$

4	3	2	2
4	1	1	3
2	0	3	2
4	1	0	4

$A_9=$

0	4	2	1
2	1	3	2
2	2	3	4
4	0	3	2

$A_{10}=$

1	1	1	4
3	0	1	2
1	2	1	3
3	0	1	0

$A_{11}=$

2	0	2	4
3	0	3	0
2	1	2	4
4	0	1	0

$A_{12}=$

4	2	2	0
2	3	2	1
2	2	0	0
1	4	1	0

$A_{13}=$

4	4	2	4
3	1	0	1
2	1	3	0
2	3	2	4

$A_{14}=$

0	2	2	4
4	1	2	0
2	3	3	3
1	2	4	2

$A_{15}=$

1	3	1	3
1	0	2	0
1	1	1	1
4	2	3	0

განვიხილოთ კიდევ სხვა სახის მატრიცები:

$A_1=$

3	0	4	1
0	2	4	1
3	4	2	0
4	1	3	2

$A_2=$

0	1	0	4
2	1	1	1
3	4	2	2
0	4	2	4

$A_3=$

2	0	4	4
2	1	3	3
4	0	2	1
2	0	3	4

$A_4=$

3	4	3	4
0	1	0	0
3	1	3	1
3	1	2	2

$A_5=$

0	0	1	1
3	1	2	2
1	0	0	4
3	0	2	3

$A_6=$

4	1	2	1
0	1	0	0
2	4	4	4
2	4	3	0

$A_7=$

2	0	4	4
2	1	3	3
4	0	2	1
2	0	3	4

$A_8=$

3	4	3	4
0	1	0	0
3	1	3	1
3	1	2	2

$A_9=$

0	0	1	1
3	1	2	2
1	0	0	4
3	0	2	3

$A_{10}=$

4	1	2	1
0	1	0	0
2	4	4	4
2	4	3	0

განვიხილოთ შემდეგი სახის მატრიცები:

$A_1=$

4	1	2	1
0	1	0	0
2	4	4	4
2	4	3	0

$A_2=$

2	0	4	4
2	1	3	3
4	0	2	1
2	0	3	4

$A_3=$

3	4	3	4
0	1	0	0
3	1	3	1
3	1	2	2

$A_4=$

0	0	1	1
3	1	2	2
1	0	0	4
3	0	2	3

$A_5=$

4	1	2	1
0	1	0	0
2	4	4	4
2	4	3	0

განვიხილოთ კიდევ სხვა სახის მატრიცა:

$A_1=$

1	4	0	2
3	3	2	1
0	2	1	4
3	4	1	1

$A_2=$

4	0	3	3
4	4	4	0
0	4	4	0
3	3	0	0

$A_3=$

0	2	1	4
1	2	2	2
4	4	2	1
2	2	0	4

$A_4=$

4	4	4	0
1	3	1	1
1	4	1	1
1	3	0	3

$A_5=$

4	4	0	0
4	0	3	2
4	3	4	2
3	2	3	2

$A_6=$

2	4	0	3
1	4	2	0
2	3	1	4
3	0	3	4

$A_7=$

2	0	1	4
4	1	3	1
2	0	4	0
3	1	1	2

$A_8=$

3	1	2	3
4	2	0	3
0	0	3	2
1	4	3	2

$A_9=$

1	3	2	1
2	0	3	2
1	2	0	2
2	4	0	0

$A_{10}=$

1	4	4	0
1	0	1	1
1	4	3	1
1	3	0	0

$A_{11}=$

4	3	4	4
0	1	4	4
0	2	2	2
3	1	2	3

$A_{12}=$

3	2	1	1
2	3	3	2
4	0	1	1
3	4	3	4

$A_{13}=$

0	0	4	1
1	1	2	4
3	0	3	0
2	4	4	0

$A_{14}=$

4	0	4	1
4	2	0	4
1	3	1	3
0	0	3	3

$A_{15}=$

0	4	2	3
2	4	4	4
3	3	4	2
4	4	0	3

$A_{16}=$

1	1	1	0
4	2	4	4
4	1	4	4
4	2	0	2

$A_{17}=$

4	4	0	0
4	0	3	2
4	3	4	2
3	2	3	2

მივიღეთ სრულიად განსხვავებული შედეგები.

პატარა განზომილების მატრიცებში გამეორება ხდება ძალიან მალე, რაც არის არასაიმედო ანუ მედეგობა არის მინიმალური.

მაშასადამე განხილული მაგალითი გვაძლევს ასეთ შედეგს:

მოდული p=10,

მატრიცაში შემავალი ელემენტები ანუ modp=m=10,

მატრიცის განზომილება n=30,

ოპერაციათა რაოდენობა = N,

ე.გ.მ. დრო = t,

$$T\approx m^n\times N\times t.$$

მატრიცის სიმრავლე = m^n (ზოგადად).

ყოველი მეორე ანუ ყოველი კენტი იყო x ღერძის სიმეტრიული, ხოლო ყოველი ლუწი y ღერძის სიმეტრიული, იმას არა აქვს არსებითი მნიშვნელობა რომელი იყო x ღერძის სიმეტრიული და რომელი y ღერძის სიმეტრიული, მთავარი ფაქტორი არის ის რომ სიმრავლის ნახევარი აღმოჩნდა x ღერძის სიმეტრიული, მეორე ნახევარი კი y ღერძის

სიმეტრიული. ე.ი. სიმრავლის ნახევარი - $m^n/2$ არის x ღერძის სიმეტრიული. ხოლო მეორე ნახევარი - $m^n/2$ არის y ღერძის სიმეტრიული. თუმცა ეს ჯამში სიმრავლეს რიცხობრივად არ ცვლის.

მატრიცაში შემავალი ელემენტების სიმრავლე არის n^2 (ზოგადად). ხოლო აქედან უცნობია – $n^2/2$ (ჩემს შემთხვევაში).

ე.ი. თუ ერთ ვექტორს გავამრავლებთ მატრიცაზე და მივიღებთ რაღაც ვექტორს, გვექნება 30 განტოლება და 450 უცნობი. ასეთი მატრიცების ამოხსნა ცალსახად შეუძლებელია. ასე რომ ჩვენ ვთვლით, რომ ასეთი განზომილების მატრიცები არის საიმედო და გამოირჩევა მაღალი მედეგობით.

თუკი არ ავიღებთ სიმეტრიულ მატრიცებს, მაგრამ ავიღებთ ისევ ორობითს, შედეგი არის უკეთესი, რადგან მატრიცათა სიმრავლე იქნება $2^{16\times16}$, ეს კი გაცილებით მეტია ვიდრე 2^{100}. შესაბამისად გაიზარდა მატრიცაში შემავალი ელემენტების რიცხვი 16×16, ხოლო განტოლებათა რაოდენობაა 16 [55-61].

3.6. მატრიცათა ველი

მატრიცათა სიმრავლე არის თუ არა მატრიცათა ველი.

1) ვთქვათ განზომილება არის 4, მოდული არის 5, ვნახოთ როგორ მატრიცებს მივიღებთ, ჯერ განვიხილოთ ისევ სიმეტრიული მატრიცები. A

1	3	3	1
2	1	1	2
3	2	2	3
3	1	1	3

A^2

4	3	2	2
3	1	3	0
3	1	3	0
4	3	2	2

A^4

4	4	4	4
3	3	3	3
2	3	3	2
2	1	1	2

A^8

4	3	2	2
4	3	3	1
4	3	3	1
4	3	2	2

A^{16}

4	4	4	4
3	3	3	3
2	3	3	2
2	1	1	2

გამეორება დაიწყო მეხუთე მატრიციდან, ახლა კი ვნახოთ ეს პატარა სიმრავლე არის თუ არა ველი.

ზემოთ მოცემულია შემდეგი მატრიცები: Á, $Á^2$, $Á^4$, $Á^8$, $Á^{16}$. ამ მატრიცებს შორის არის: $Á^3$, $Á^5$, $Á^6$, $Á^7$, $Á^9$, $Á^{10}$, $Á^{11}$, $Á^{12}$, $Á^{13}$, $Á^{14}$, $Á^{15}$. ეხლა უნდა ვიპოვოთ ეს მატრიცები. ჩამოვწეროთ თანმიმდევრობით:

$Á^3 = Á * Á^2$

1	2	1	0
2	4	2	0
2	4	4	3
4	3	2	2

$Á^5 = Á^4 * Á$

1	2	3	3
3	1	2	1
3	1	2	1
1	2	3	3

$Á^6 = Á^2 * Á^4$

3	1	1	3
3	4	4	3
3	4	4	3
3	1	1	3

$Á^7 = Á * Á^2 * Á^4$

1	2	1	0
2	4	2	0
2	4	4	3
4	3	2	2

×

4	4	4	4
3	3	3	3
2	3	3	2
2	1	1	2

2	4	4	3
3	1	0	3
3	1	0	3
2	4	4	3

$Á^9 = Á * Á^8$

2	4	0	2
4	3	0	4
2	4	4	3
0	0	1	4

$Á^{10} = Á^2 * Á^8$

4	3	3	4
3	1	1	3
2	3	3	2
2	0	0	2

$Á^{11} = Á * Á^2 * Á^8$

1	2	1	0
2	4	2	0
2	4	4	3
4	3	2	2

×

4	3	2	2
4	3	3	1
4	3	3	1
4	3	2	2

1	2	2	4
2	4	4	3
1	2	4	2
0	0	3	2

$Á^{12} = Á^{4} * Á^{8}$

4	3	0	4
3	1	0	3
0	0	1	4
4	3	4	0

$Á^{13} = Á * Á^{4} * Á^{8}$

1	2	3	3
3	1	2	1
3	1	2	1
1	2	3	3

×

4	3	2	2
4	3	3	1
4	3	3	1
4	3	2	2

1	3	3	1
2	1	1	2
3	2	2	3
3	1	1	3

$Á^{14} = Á^{2} * Á^{4} * Á^{8}$

3	1	1	3
3	4	4	3
3	4	4	3
3	1	1	3

×

4	3	2	2
4	3	3	1
4	3	3	1
4	3	2	2

2	1	1	2
4	2	2	4
3	1	1	3
4	0	0	4

$Á^{15} = Á * Á^{2} * Á^{4} * Á^{8}$

2	4	4	3
3	1	0	3
3	1	0	3
2	4	4	3

×

4	3	2	2
4	3	3	1
4	3	3	1
4	3	2	2

2	3	3	2
4	1	1	4
4	0	0	4
3	3	3	3

მაშასადამე მივიღეთ შემდეგი სახის მატრიცათა სიმრავლე:
$Á, Á^2, Á^3, Á^4, Á^5, Á^6, Á^7, Á^8, Á^9, Á^{10}, Á^{11}, Á^{12}, Á^{13}, Á^{14}, Á^{15}, Á^{16}$.

1	3	3	1
2	1	1	2
3	2	2	3
3	1	1	3

4	3	2	2
3	1	3	0
3	1	3	0
4	3	2	2

1	2	1	0
2	4	2	0
2	4	4	3
4	3	2	2

4	4	4	4
3	3	3	3
2	3	3	2
2	1	1	2

1	2	3	3
3	1	2	1
3	1	2	1
1	2	3	3

3	1	1	3
3	4	4	3
3	4	4	3
3	1	1	3

2	4	4	3
3	1	0	3
3	1	0	3
2	4	4	3

4	3	2	2
4	3	3	1
4	3	3	1
4	3	2	2

2	4	0	2
4	3	0	4
2	4	4	3
0	0	1	4

4	3	3	4
3	1	1	3
2	3	3	2
2	0	0	2

1	2	2	4
2	4	4	3
1	2	4	2
0	0	3	2

4	3	0	4
3	1	0	3
0	0	1	4
4	3	4	0

1	3	3	1
2	1	1	2
3	2	2	3
3	1	1	3

2	1	1	2
4	2	2	4
3	1	1	3
4	0	0	4

2	3	3	2
4	1	1	4
4	0	0	4
3	3	3	3

4	4	4	4
3	3	3	3
2	3	3	2
2	1	1	2

გადამოწმების შედეგად მივიღებთ, რომ ასეთი სიმეტრიული მატრიცები (რომლებიც სიმეტრიულია X ან Y ღერძის მიმართ) არ გვაძლევს მატრიცათა ველს.

ახლა კი განვიხილოთ ნებისმიერი სახის მატრიცები.

1) განზომილება იყოს 4, მოდული 5.

A

2	4	2	1
3	4	1	1
2	3	3	4
2	1	2	4

A^2

2	2	2	4
1	2	3	2
1	0	4	4
3	0	3	2

A^4

0	3	3	0
3	1	2	1
0	1	0	4
3	4	3	3

A^8

4	1	0	1
1	1	2	3
1	4	4	1
0	2	3	0

A^{16}

2	2	2	0
2	1	3	4
0	4	2	1
2	1	2	4

$(A^{16})^2$

3	4	0	4
4	1	3	2
4	1	3	4
0	3	2	2

$(A^{16})^4$

0	3	3	0
3	1	2	1
0	1	0	4
3	4	3	3

მატრიცამ დაიწყო გამეორება, ამიტომ კვადრატში აყვანას შევწყვიტოთ და ეხლა კი ვიპოვოთ დანარჩენი მატრიცები. ესენია: $Á^3$, $Á^5$, $Á^6$, $Á^7$, $Á^9$, $Á^{10}$, $Á^{11}$, $Á^{12}$, $Á^{13}$, $Á^{14}$, $Á^{15}$, $Á^{17}$, $Á^{18}$, $Á^{19}$, $Á^{20}$ და ა.შ.

$Á^3$

3	4	2	4
2	4	0	1
2	0	2	2
1	1	4	1

$Á^5$

0	0	1	0
1	3	3	0
2	0	4	0
0	1	2	1

$Á^6$

3	2	2	1
1	1	3	0
2	3	0	0
2	0	3	3

$Á^7$

4	0	1	1
1	4	1	2
4	2	2	3
4	2	4	0

$Á^{9}$

4	2	4	1
1	3	0	4
4	0	0	2
1	1	4	2

$Á^{10}$

2	4	3	0
0	4	0	4
4	2	3	3
0	0	0	1

$Á^{11}$

3	2	0	4
3	3	4	0
3	1	4	1
2	4	4	3

$Á^{12}$

1	0	1	4
0	4	4	0
3	3	4	4
2	3	3	3

$Á^{13}$

1	0	2	3
4	1	3	1
4	3	1	3
1	3	1	0

$Á^{14}$

1	3	1	1
0	4	0	0
0	4	1	1
1	2	1	0

$Á^{15}$

2	4	0	2
0	3	0	2
2	3	1	0
0	4	2	4

და ა. შ. მივიღეთ ასეთი მატრიცათა ბაზა:
$Á, Á^2, Á^3, Á^4, Á^5, Á^6, Á^7, Á^8, Á^9, Á^{10}, Á^{11}, Á^{12}, Á^{13}, Á^{14}, Á^{15}, Á^{16}$.

2	4	2	1
3	4	1	1
2	3	3	4
2	1	2	4

2	2	2	4
1	2	3	2
1	0	4	4
3	0	3	2

3	4	2	4
2	4	0	1
2	0	2	2
1	1	4	1

0	3	3	0
3	1	2	1
0	1	0	4
3	4	3	3

0	0	1	0
1	3	3	0
2	0	4	0
0	1	2	1

3	2	2	1
1	1	3	0
2	3	0	0
2	0	3	3

4	0	1	1
1	4	1	2
4	2	2	3
4	2	4	0

4	1	0	1
1	1	2	3
1	4	4	1
0	2	3	0

4	2	4	1
1	3	0	4
4	0	0	2
1	1	4	2

2	4	3	0
0	4	0	4
4	2	3	3
0	0	0	1

3	2	0	4
3	3	4	0
3	1	4	1
2	4	4	3

1	0	1	4
0	4	4	0
3	3	4	4
2	3	3	3

1	0	2	3
4	1	3	1
4	3	1	3
1	3	1	0

1	3	1	1
0	4	0	0
0	4	1	1
1	2	1	0

2	4	0	2
0	3	0	2
2	3	1	0
0	4	2	4

2	2	2	0
2	1	3	4
0	4	2	1
2	1	2	4

გადამოწმების შედეგად მივიღებთ, რომ ასეთი მატრიცები არ გვაძლევს მატრიცათა ველს. ერთმანეთზე გამრავლების შედეგად არ მიიღება ისეთი მატრიცები, რომლებიც იქნება ამავე სიმრავლეში, ე.ი. არ არის ჩაკეტილი და მაშასადამე არ არის ველი.

2) ახლა განვიხილოთ ისეთი მატრიცები, რომლებიც სიმეტრიული იქნება დიაგონალის მიმართ.

განზომილება იყოს 2, მოდული 7.

A_1=

2	4
4	2

A_2=

6	2
2	6

A_3=

5	3
3	5

A_4=

6	2
2	6

უკვე დაიწყო მატრიცამ გამეორება, ამიტომ ეხლა ავაგოთ ამ სიმრავლეში მოთავსებული დანარჩენი მატრიცები: $Á^3$, $Á^5$, $Á^6$, $Á^7$

$Á^3 = Á * Á^2$

6	0
0	6

$Á^5 = Á * Á^4$

1	5
5	1

$Á^6 = Á^2 * Á^4$

1	0
0	1

$Á^7 = Á * Á^2 * Á^4$

2	4
4	2

მივიღეთ მატრიცათა სიმრავლე: $Á, Á^2, Á^3, Á^4\ Á^5, Á^6, Á^7, Á^8$:

2	4	6	2	6	0	5	3	1	5	1	0	2	4	6	2
4	2	2	6	0	6	3	5	5	1	0	1	4	2	2	6

შედეგი: დიაგონალის მიმართ სიმეტრიული მატრიცები გვაძლევს მატრიცათა ველს.

2) შემდეგ გავზარდოთ განზომილება:

განზომილება იყოს 4 მოდული 7

$A_1=$

1	4	5	2
2	1	4	5
5	2	1	4
4	5	2	1

$A_2=$

0	2	2	0
0	0	2	2
2	0	0	2
2	2	0	0

$A_3=$

4	1	4	0
0	4	1	4
4	0	4	1
1	4	0	4

$A_4=$

4	1	5	1
1	4	1	5
5	1	4	1
1	5	1	4

$A_5=$

1	4	0	4
4	1	4	0
0	4	1	4
4	0	4	1

$A_6=$

5	1	4	1
1	5	1	4
4	1	5	1
1	4	1	5

$A_7=$

1	4	0	4
4	1	4	0
0	4	1	4
4	0	4	1

უკვე დაიწყო გამეორება, ასე რომ ეხლა უნდა ვიპოვოთ დანარჩენი მატრიცები.

$Á^3$, $Á^5$, $Á^6$, $Á^7$, $Á^9$, $Á^{10}$, $Á^{11}$, $Á^{12}$, $Á^{13}$, $Á^{14}$, $Á^{15}$, $Á^{17}$, $Á^{18}$, $Á^{19}$,$Á^{20}$, $Á^{21}$, $Á^{22}$, $Á^{23}$,$Á^{24}$, $Á^{25}$, $Á^{26}$, $Á^{27}$, $Á^{28}$, $Á^{29}$, $Á^{30}$, $Á^{31}$, $Á^{33}$..... $Á^{63,}$ $Á^{64}$.

$Á^3$

0	4	3	6
6	0	4	3
3	6	0	4
4	3	6	0

$Á^5$

5	1	0	4
4	5	1	0
0	4	5	1
1	0	4	5

$Á^6$

1	3	3	1
1	1	3	3
3	1	1	3
3	3	1	1

$Á^7$

4	1	2	5
5	4	1	2
2	5	4	1
1	2	5	4

$Á^9$

0	6	3	4
4	0	6	3
3	4	0	6
6	3	4	0

$Á^{10}$

5	5	3	3
3	5	5	3
3	3	5	5
5	3	3	5

$Á^{11}$

4	5	1	0
0	4	5	1
1	0	4	5
5	1	0	4

$Á^{12}$

2	6	2	5
5	2	6	2
2	5	2	6
6	2	5	2

$Á^{13}$

4	5	2	1
1	4	5	2
2	1	4	5
5	2	1	4

$Á^{14}$

2	2	0	0
0	2	2	0
0	0	2	2
2	0	0	2

$Á^{15}$

4	3	6	0
0	4	3	6
6	0	4	3
3	6	0	4

$Á, Á^{2}, Á^{3}, Á^{4}, Á^{5}, Á^{6}, Á^{7}, Á^{8}, Á^{9}, Á^{10}, Á^{11}, Á^{12}, Á^{13}, Á^{14}, Á^{15}, Á^{16}$:

1	4	5	2
2	1	4	5
5	2	1	4
4	5	2	1

0	2	2	0
0	0	2	2
2	0	0	2
2	2	0	0

0	4	3	6
6	0	4	3
3	6	0	4
4	3	6	0

4	1	4	0
0	4	1	4
4	0	4	1
1	4	0	4

5	1	0	4
4	5	1	0
0	4	5	1
1	0	4	5

1	3	3	1
1	1	3	3
3	1	1	3
3	3	1	1

4	1	2	5
5	4	1	2
2	5	4	1
1	2	5	4

4	1	5	1
1	4	1	5
5	1	4	1
1	5	1	4

0	6	3	4
4	0	6	3
3	4	0	6
6	3	4	0

5	5	3	3
3	5	5	3
3	3	5	5
5	3	3	5

4	5	1	0
0	4	5	1
1	0	4	5
5	1	0	4

2	6	2	5
5	2	6	2
2	5	2	6
6	2	5	2

4	5	2	1
1	4	5	2
2	1	4	5
5	2	1	4

2	2	0	0
0	2	2	0
0	0	2	2
2	0	0	2

4	3	6	0
0	4	3	6
6	0	4	3
3	6	0	4

1	4	0	4
4	1	4	0
0	4	1	4
4	0	4	1

მატრიცათა სიმრავლემ მოგვცა მატრიცათა ველი.

მაშასადამე სიმეტრიული მატრიცები გვაძლევს ასეთ შედეგებს:

1) როდესაც ავიღეთ X ან Y ღერძის მიმართ სიმეტრიული მატრიცები (მაგალითი ზემოთ არის მოყვანილი), ვერ მივიღეთ ჩაკეტილი სიმრავლე. ე.ი. არ შეიქმნა მატრიცათა ველი.

2) როდესაც განვიხილეთ დიაგონალის მიმართ სიმეტრიული მატრიცები, მაგალითი ზემოთ არის მოყვანილი, ორ განზომილებიანის შემთხვევაში მივიღეთ მატრიცათა ველი, და ამავდროულად ასეთი მატრიცები არის კომუტატიურიც და გამოიყენება ჩვენს მიერ განხილულ მეთოდში.

ე.ი. 1) თუ ავიღებთ ნებისმიერ მატრიცებს და შევადგენთ მატრიცათა სიმრავლეს, მატრიცათა ველი არ მიიღება.

2) თუ ავიღებთ სიმეტრიულ მატრიცებს x ან y ღერძების მიმართ, მატრიცათა ველი არც მაშინ არ მიიღება.

3) და თუ ავიღებთ სიმეტრიულ მატრიცებს დიაგონალის მიმართ და შევადგენთ მატრიცათა სიმრავლეს, მაშინ მატრიცათა ველი მიიღება, მაგრამ სიმრავლის ნახევარი ცნობილია და ნახევარი უცნობი [62-66, 68, 73, 75, 77, 79, 82-85].

3.7. შიფრაციის დროისა და მატრიცათა სიმრავლის დამოკიდებულება

შეიქმნა ორობითი მატრიცათა სიმრავლე, რომელიც შეგვიძლია გამოვიყენოთ ჩვენს მიერ განხილულ მეთოდებში.

მატრიცათა სიმრავლიდან ამორჩევის დრო ჩვენთვის უკვე ცნობილია $t = M^{n\times n} \cdot N \cdot T$, სადაც $M^{n\times n}$ არის მატრიცათა სიმრავლე, N – ოპერაციათა ჩატარების რიცხვი, T – ე.გ.მ.-ის დრო.

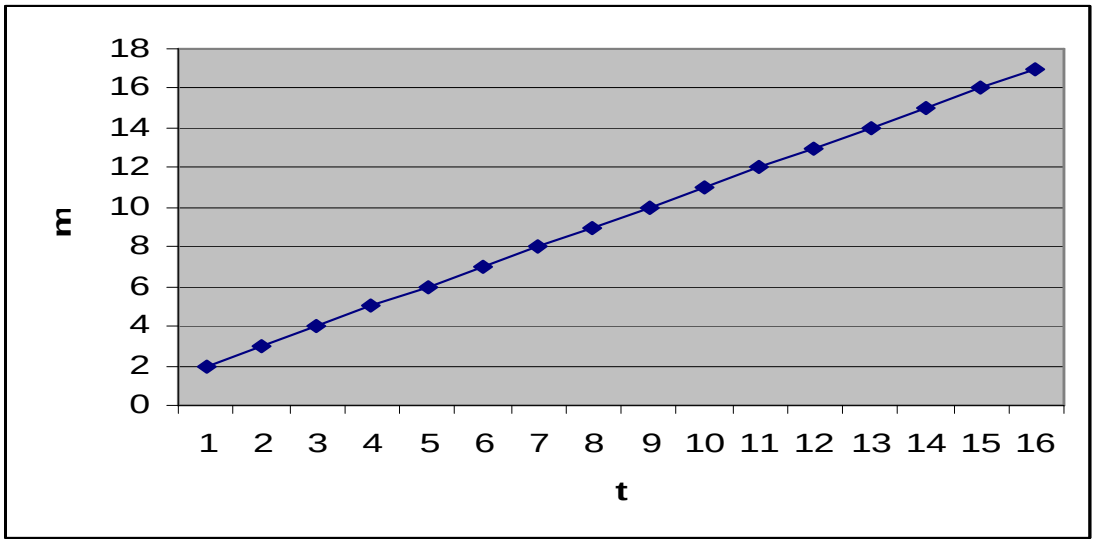
ავაგოთ სხვადასხვა დამოკიდებულების გრაფიკები, მოცემული კონკრეტული შემთხვევისათვის, იხ. ცხრილი 4. განზომილების, მოდულის, სიმრავლისა და შიფრაციის დროის დამოკიდებულება, როცა მოდული m=2, განზომილება n=2, 3, 4, ...

m	n	n*n	m^(n*n)	t	m^(n*n)/2
2	2	4	16	128	8
2	3	9	512	13824	256
2	4	16	65536	4194304	32768
2	5	25	33554432	4,19E+09	16777216
2	6	36	68719476736	1,48E+13	34359738368
2	7	49	5,63E+14	1,93E+17	2,81475E+14
2	8	64	1,84E+19	9,44E+21	9,22335E+18
2	9	81	2,42E+24	1,76E+27	1,20893E+24
2	10	100	1,27E+30	1,27E+33	6,33825E+29
2	11	121	2,66E+36	3,54E+39	1,32923E+36
2	12	144	2,23E+43	3,85E+46	1,11504E+43
2	13	169	7,48E+50	1,64E+54	3,74145E+50
2	14	196	1,00E+59	2,76E+62	5,0217E+58
2	15	225	5,39E+67	1,82E+71	2,696E+67
2	16	256	1,16E+77	4,74E+80	5,7896E+76
2	17	289	9,95E+86	4,89E+90	4,97323E+86

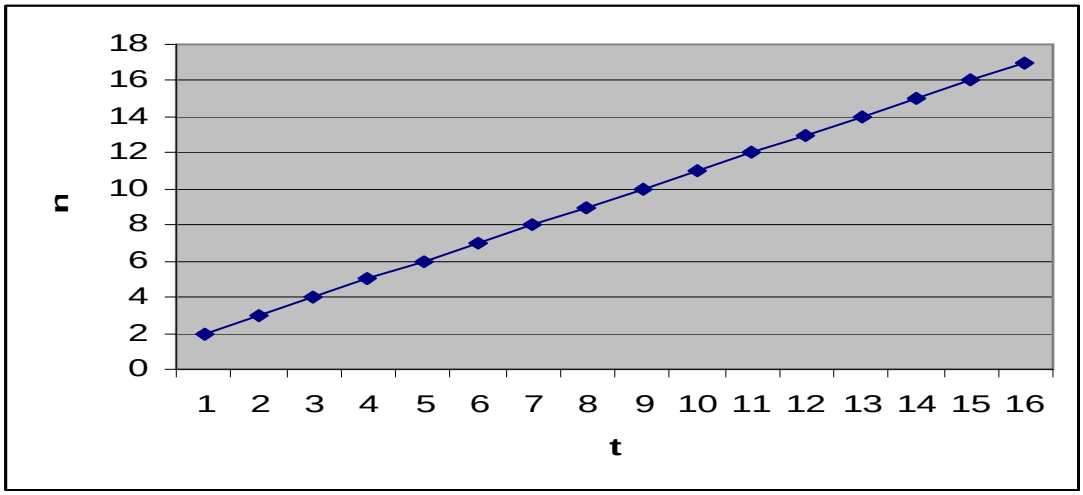
ცხრილი 4.

ნათლად ჩანს, რომ განზომილებისა და მოდულის ზრდასთან ერთად საგრძნობლად იზრდება მატრიცათა სიმრავლე, იხ. ნახ. 7. m მოდულისა და M^{n*n} მატრიცათა სიმრავლის დამოკიდებულება. ასევე იზრდება მატრიცათა სიმრავლიდან ამორჩევის დრო, იხ. ნახ. 3. t დროის და m მოდულის დამოკიდებულება, რაც კარგ შედეგს იძლევა და ამოცანა ხასიათდება მაღალი მედეგობით.

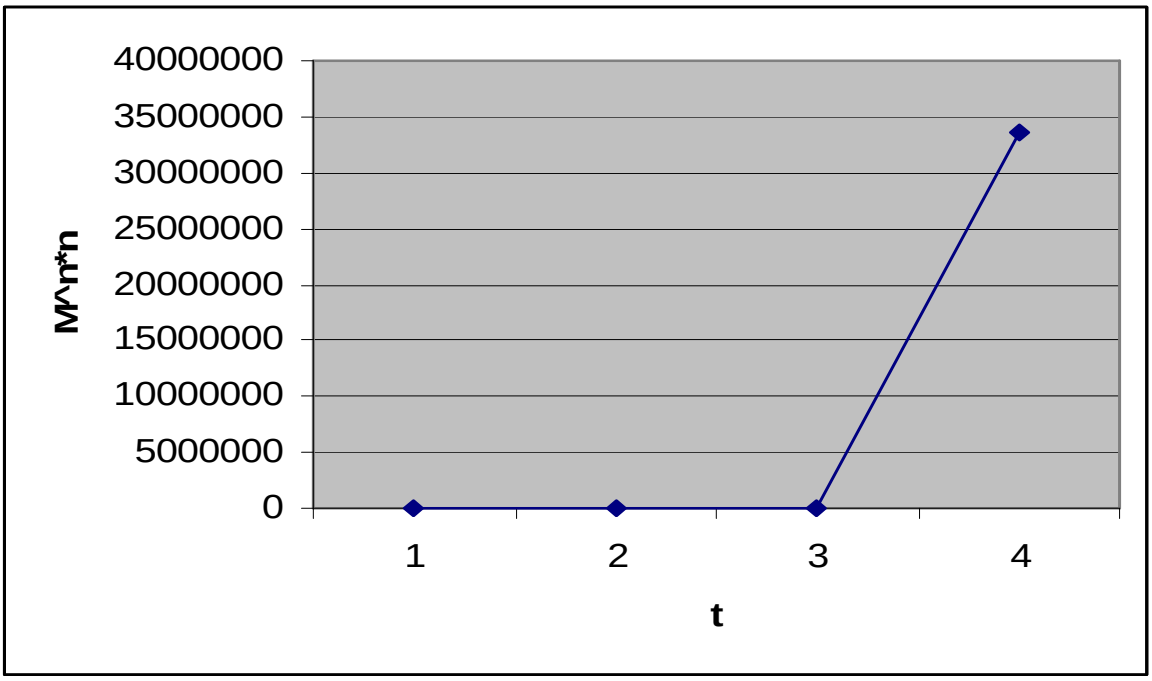
შესაბამისად, განზომილების ზრდასთან ერთად საგრძნობლად იზრდება მატრიცათა სიმრავლიდან ამორჩევის ხანგრძლივობა, იხ. ნახ. 4. t დროის და n განზომილების დამოკიდებულება, იხ. ნახ. 5. m^{n*n} სიმრავლისა და t დროის დამოკიდებულება, იხ. ნახ. 6. t დროის და $m^{(n*n)/2}$ სიმრავლის დამოკიდებულება.



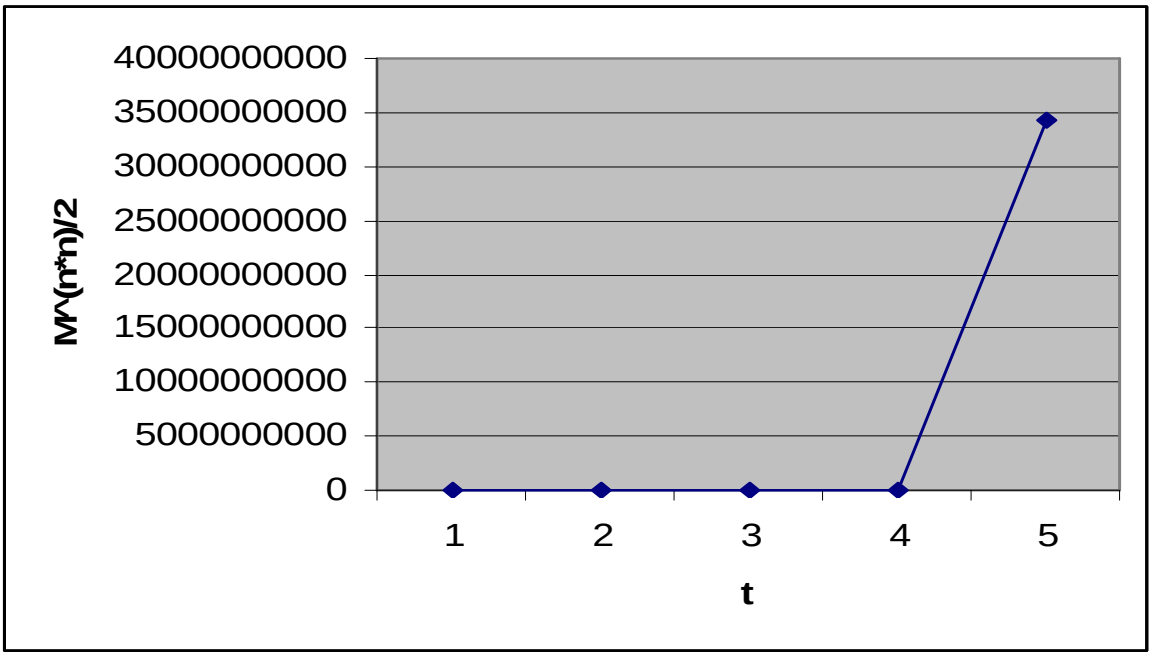
ნახ. 3.



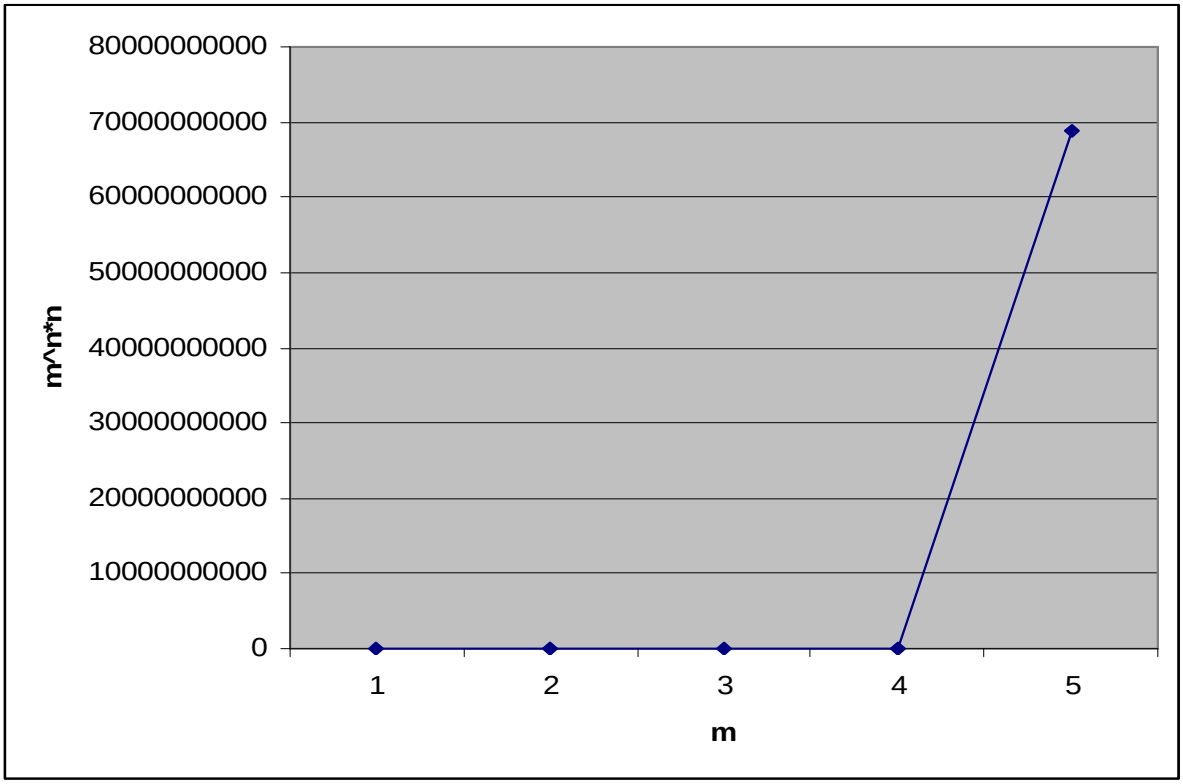
ნახ. 4.


40000000
35000000
30000000
25000000
20000000
15000000
10000000
5000000
0
M^n*n
1
2
3
4
t

ნახ. 5.


40000000000
35000000000
30000000000
25000000000
20000000000
15000000000
10000000000
5000000000
0
M^(n*n)/2
1
2
3
4
5
t

ნახ. 6.



ნახ. 7.

3.8. მატრიცული მეთოდის გატეხვის მცდელობა

ზემოთ არის აღნიშნული, თუ როგორ ხდება ჯერ გასაღების გაცვლა, როგორც სიმეტრიულ ასევე ასიმეტრიულ მეთოდებში; შემდგომ კი ინფორმაციის დაშიფვრა, გადაცემა და მიმღები მხარის მიერ გა-შიფვრა.

როგორ შეიძლება ამ პროცედურის დროს და სად არის შესაძ-ლებელი, რომ არაკანონიერმა მომხმარებელმა შემდგომში "ჰაკერმა" მოახერხოს დაშიფრული ინფორმაციის ხელში ჩაგდება და შესაბამისად გაშიფვრა.

ვთქვათ, ჰაკერმა ჩაიგდო ხელში n^2 სიგრძის დაშიფრული ინფორმაცია, სადაც n არის განზომილება. აქედან გამომდინარე შეგვიძლია ვთქვათ, რომ ჰაკერმა ჩაიგდო ხელში სრული ინფორმაცია.

ისმის კითხვა: შეძლებს თუ არა ამ დროს იგი ინფორმაციის გაშიფვრას და შესაბამისად საწყისი ინფორმაციის მიღებას?

ჩვენს მიერ განხილულ მეთოდში გამოყენებულია მატრიცათა სიმრავლე, რომელიც ყველასათვის ცნობილია, მათ შორის ჰაკერისთვისაც ცნობილია.

მატრიცათა სიმრავლე არის $m^{n\times n}$, სადაც m არის მატრიცაში შემავალი ელემენების რიცხვითი მნიშვნელობა, n – განზომილება.

როგორც უკვე ზემოთ ავღნიშნეთ და მოვიყვანეთ მაგალითები, ნათლად ჩანს, რომ თუკი ავიღებთ ორობით მატრიცათა სიმრავლეს, სადაც სიმრავლის რაოდენობა იქნება 2^{100}, რომელიც არის დაახლოებით 10^{30} რიცხვის ტოლი, ეს რიცხვი კი კრიპტოგრაფიაში არის ქვედა ზღვარი. ამ სიმრავლიდან კი, რეალურ დროში, იმ ორი კონკრეტული მატრიცის ამორჩევა შეუძლებელია [1, 8, 15, 31, 56, 64, 77].

ე.ი. გატეხვა შეუძლებელია.

მაგრამ კიდევ ისმის კითხვა: შესაძლებელია რომ ჰაკერმა, თუკი ის სრულ ინფორმაციას ჩაიგდებს ხელში, მთლიანად შეცვალოს იგი და აბსოლუტურად სხვა ინფორმაცია გაუგზავნოს მიმღებს?

როგორ მიხვდება მიმღები, ანუ როგორ უნდა გადაამოწმოს მიმღებმა, მიღებული ინფორმაციის ნამდვილობა?

თუ ჰაკერი გასაღების გაცვლის პროცესში ჩაიგდებს გადაცემულ სიმრავლეს სრულად, მას შეუძლია შეცვალოს, ანუ აიღოს სხვა მატრიცა, რომელსაც გაამრავლებს ცნობილ ვექტორზე და გაუგზავნის მიმღებს, მიმღები ამ ეტაპზე ვერაფერს ვერ მიხვდება, იგი მიიღებს გასაღებს და გააგრძელებს პროცედურას. ანუ ისიც გამოაგზავნის ვექტორის ნამრავლს მატრიცაზე და მას ჩაიჭერს ისევ ჰაკერი. ე.ი. ჰაკერი და მიმღები მიიღებენ ერთიდაიგივე გასაღებს, ხოლო მეორე მომხმარებელი კი სხვა გასაღებს. ამ შემთხვევაში გასაღები ჰაკერის ხელში იქნება და ვერაფერს შევცვლით. ანუ ჰაკერი იმუშავებს გადამცემსა და მიმღებს შორის.

მაგრამ ასე რომ არ მოხდეს, ჩვენ თავი დავიცავით და შევქმენით მეთოდი სადაც ვექტორის გადაცემა ხდება დახურული არხით და შემდგომ ხდება გასაღების მიღება. ამით განზომილება უცნობი გახდა ჰაკერისათვის, შესაბამისად მან თუნდაც რომ ჩაიჭიროს ინფორმაცია, იგი ვერ მოახერხებს მის გაშიფვრას, რადგან ვერ დაყოფს ბლოკებად. ასევე რადგან არ იცის განზომილება, შესაბამისად მისთვის უცნობია, რა განზომილების მატრიცა გამოიყენოს, ეს კი აუცილებელია ინფორმაციის როგორც დაშიფვრისათვის, ასევე გაშიფვრისათვის. ასევე ვექტორთა სიმრავლეა n!, ეს ძალიან დიდი რიცხვია, რეალურ დროში, კონკრეტულ ვექტორს ვერ ამოარჩევს, შემდეგ კი გარკვეული დროის მერე მოხდება ვექტორის შეცვლა და რა თქმა უნდა, მომხმარებლები თავის საიდუმლო მატრიცებსაც ცვლიან.

... და კიდევ, რადგან უკვე გამოვიყენეთ დახურული არხი, შესაძლებელია რომ ვექტორთან ერთად საიდუმლოდ გადავცეთ მატრიცაც, ამით გასაღების გენერაციის დროც გაიზრდება და ჰაკერი მის ჩაჭერას ვეღარც კი მოახერხებს. გასაღების გენერაცია ხდება მილიწამებში.

მაგრამ, ვთქვათ ჰაკერმა მთლიანად შეცვალა ინფორმაცია, როგორ ამოწმებს მას მიმღები?

მიმღებმა ინფორმაციის ნამდვილობა რომ შეამოწმოს, უკუ პროცესი უნდა გაიაროს, როგორც მივიდა გასაღების მიღებამდე და უნდა მიიღოს იგივე ვექტორი, ეს ხდება წამებში და თუ ვერ მიიღებს ესეიგი ინფორმაცია შეცვლილია.

აქვე უნდა აღინიშნოს, რომ ამ მეთოდის გამოყენებით უმჯობესია მცირე ზომის ინფორმაციის გადაცემა, რადგან თუ დიდი ზომის ინფორმაციას დავშიფრავთ ამ მეთოდით, იქიდან შედარებით მარტივი იქნება n^2 სიმრავლის ამორჩევა. მაგრამ თუ ვექტორს გადავცემთ საიდუმლოდ, მაშინ ინფორმაციის სიგრძე შეგვიძლია გავზარდოთ.

III თავის დასკვნა

ჩვენი მიზანი იყო მიღებული ახალი მეთოდებისათვის, რომლებიც განხილულ იქნა მეორე თავში, შეგვექმნა მატრიცათა სიმრავლე, რომელსაც გამოვიყენებდით აღნიშნულ მეთოდებში.

მესამე თავში განხილულ იქნა სხვადასხვა სახის მატრიცები, როგორიცაა: ორობითი, ათობითი, სიმეტრიული, შემთხვევითი, ნებისმიერი, სიმეტრიული დიაგონალის მიმართ და ა.შ.

მოყვანილ და განხილულ იქნა რამოდენიმე მაგალითი, სხვადასხვა განზომილების და მოდულის მქონე მატრიცებისათვის.

თუკი ავიღებთ სიმეტრიულ ორობით მატრიცებს დიაგონალის მიმართ, მატრიცების გამეორების ფაქტი, საერთოდ არ ფიქსირდება. შეიქმნა **მატრიცათა სიმრავლე** და თანაც მატრიცათა ველი. სწორედ ეს სიმრავლე გამოიყენება მიღებულ ახალ ორიგინალურ მეთოდებში, ინფორმაციის დასაიდუმლოებისათვის. აქვე უნდა აღინიშნოს, რომ მატრიცები უნდა იყოს **კომუტატიური**.

თუ ავიღებთ 10 განზომილებიან ორობით მატრიცებს, მატრიცათა სიმრავლე შეადგენს 2^{100} რიცხვს, ეს კი დაახლოებით არის 10^{30}. აღნიშნული რიცხვი კი კრიპტოგრაფიაში არის ქვედა ზღვარი, ანუ ამ სიმრავლიდან მატრიცათა ამორჩევა, რეალურ დროში, შეუძლებელია.

საბოლოო დასკვნა

განხილულ და გამოყენებულ იქნა **კრიპტოგრაფიის** სიმეტრიული – დახურული და ასიმეტრიული – ღია სისტემები. სიმეტრიულს მიეკუთნება – ცეზარის, ვიჟინერის და ვერნამის, ასიმეტრიულს კი – დიფი-ჰელმანის, რაივესტ-შამირ-ეიდელმანის და ელგამალის მეთოდები და ალგორითმები.

ჩვენს მიერ განხილულ და აღწერილ იქნა თითოეული მეთოდი, ხოლო გამოყენებულ იქნა, კერძოდ დიფი-ჰელმანის ალგორითმი.

შემუშავებულ იქნა ახალი მეთოდები:

1. დიფი-ჰელმანის მეთოდის გამოყენებით მიღებულ იქნა ახალი მეთოდი, ოღონდ დიფი-ჰელმანის ახარისხება **შეცვლილი იქნა მატრიცაზე გამრავლებით**. ახარისხებას უფრო მეტი დრო სჭირდება (მამრავლებად დაშლა), ვიდრე მატრიცაზე გამრავლებას. აღნიშნულით შიფრაციის სიჩქარე გაიზარდა, შემცირდა გასაღების გენერაციის დრო, ანუ გასაღების მიღება ხდება უფრო სწრაფად, ვიდრე ეს ხდებოდა დიფი-ჰელმანის მეთოდში.

2. მოვახდინეთ მეთოდთა **სინთეზი**. გამოყენებულ იქნა როგორც სიმეტრიული, ასევე ასიმეტრიული მეთოდი. ვექტორის გადაცემა განვახორციელეთ დახურული არხით და შემდგომ კი, ყველა პროცედურა შევასრულეთ ღია არხით. ამ მეთოდმა მოგვცა, ის რომ შიფრაციის სიჩქარე უმნიშვნელოდ შემცირდა, რაც გამოიწვია კურიერის არსებობამ, მაგრამ სამაგიეროდ, კიდევ უფრო გაიზარდა მედეგობა. განზომილება გახდა უცნობი, რის გამოც არაკანონიერი მომხმარებელი ვერ შეძლებს ინფორმაციის დაყოფას ბლოკებად, შესაბამისად ვერ მიხვდება რა განზომილების მატრიცა უნდა გამოიყენოს, რაც ინფორმაციის გაშიფვრისათვის მთავარი ეტაპია.

3. ერთდროულად მოვახდინეთ დახურული არხით, ანუ კურიერით, **ვექტორის და მატრიცის გადაცემა**. მიმღები მილიწამებში აფიქსირებს კომუტატიურ მატრიცას და შესაბამისად გასაღებსაც. ანუ გასაღების გენერაციის დრო კიდევ უფრო შემცირდა, ანუ მილიწამებში მიი-

ღება, შიფრაციის სიჩქარე კი საბოლოო ჯამში კიდევ უფრო გაიზარდა, მაგრამ ეს არ მომხდარა საიმედოობის ხარჯზე.

4. დავამტკიცეთ რომ, აღნიშნულ მეთოდებში გამოიყენება **კომუტატიური მატრიცები** ანუ $A_1A_2=A_2A_1$.

5. დავადგინეთ **მატრიცათა სიმრავლე**. მიუხედავად იმისა, რომ წინასწარ ცნობილია მატრიცათა განზომილება, მოდული და სიმრავლე, მაინც შეუძლებელია ამ მეთოდის გატეხვა, რადგან მატრიცათა სიმრავლე შეადგენს ძალიან დიდ რიცხვს – M^{m*n}. რადგან ვიყენებთ კომუტატიურ-კვადრატულ მატრიცებს, როცა m=6 და n=6, მაშინ ათობითში – სიმრავლე იქნება 10^{36}, რაც დაახლოებით ორობითში შეადგენს 2^{100}-ის ტოლ სიმრავლეს. აღნიშნული კი კრიპტოგრაფიაში წარმოადგენს ქვედა ზღვარს, რაც იმას ნიშნავს რომ, რეალურ დროში, ამ სიმრავლიდან მატრიცის ამორჩევა არის შეუძლებელი.

6. მატრიცათა სიმრავლე არის მატრიცათა ველი, ანუ ჩაკეტილი სიმრავლე. ორი მატრიცის გამრავლებით მიიღება ისეთი მესამე მატრიცა, რომელიც მოთავსებულია ამავე მატრიცათა სიმრავლეში.

... და ბოლოს, მიღებული ახალი მეთოდები, მიეკუთვნება ასიმეტრიულ მეთოდს და გამოირჩევა **მაღალი მედეგობით**. **კრიპტოსირთულეს** წარმოადგენს მატრიცათა სიმრავლიდან ამორჩევის სირთულე, რასაც ემყარება მიღებული მეთოდების საიმედოობა.

დანართი 1.

A_1=

1	2	4	3	4	4	3	4	2	1
2	4	3	1	4	4	1	3	4	2
2	4	4	1	1	1	1	4	4	2
3	3	2	4	1	1	4	2	3	3
2	4	3	3	1	1	3	3	4	2
4	3	4	2	1	1	2	4	3	4
1	1	2	4	3	3	4	2	1	1
2	1	4	3	1	1	3	4	1	2
2	2	4	3	1	1	3	4	2	2
1	1	2	3	4	4	3	2	1	1

A_2=

2	0	1	3	0	0	3	2	1	0
0	2	1	0	4	0	1	1	2	4
2	1	3	3	3	2	1	0	2	4
4	3	2	0	4	3	0	1	0	2
1	4	0	1	1	0	4	3	3	2
1	4	0	1	1	0	4	3	3	2
4	3	2	0	4	3	0	1	0	2
2	1	3	3	3	2	1	0	2	4
0	2	1	0	4	0	1	1	2	4
2	0	1	3	0	0	3	2	1	0

A_3 =

4	0	4	0	3	3	0	4	0	4
3	4	1	2	1	1	2	1	4	3
4	1	1	3	4	4	3	1	1	4
0	2	2	4	4	4	4	2	2	0
2	0	2	3	3	3	3	2	0	2
4	2	3	1	1	1	1	3	2	4
0	4	4	2	3	3	2	4	4	0
1	0	4	1	1	1	1	4	0	1
0	3	3	4	1	1	4	3	3	0
3	4	2	3	2	2	3	2	4	3

A_4=

1	4	1	3	4	4	3	1	4	1
4	0	0	0	0	0	0	0	0	4
1	4	0	4	4	4	4	0	4	1
4	2	1	3	1	1	3	1	2	4
4	2	4	4	1	1	4	4	2	4
3	1	1	0	1	1	0	1	1	3
2	0	1	1	0	0	1	1	0	2
0	4	4	3	2	2	3	4	4	0
4	0	2	2	0	0	2	2	0	4
1	3	0	2	1	1	2	0	3	1

$A_{5=}$

1	4	0	0	2	0	0	3	0	0
1	0	0	3	4	1	0	1	0	4
4	1	1	2	0	3	3	2	1	2
0	3	1	0	4	1	4	4	3	2
2	1	4	3	3	0	4	1	3	2
2	1	4	3	3	0	4	1	3	2
0	3	1	0	4	1	4	4	3	2
4	1	1	2	0	3	3	2	1	2
1	0	0	3	4	1	0	1	0	4
1	4	0	0	2	0	0	3	0	0

A_6=

2	2	3	0	0	0	0	3	2	2
4	3	3	3	2	2	3	3	3	4
1	2	1	2	1	1	2	1	2	1
0	4	4	4	3	3	4	4	4	0
4	4	1	4	0	0	4	1	4	4
4	1	4	4	0	0	4	4	1	4
1	4	4	0	0	0	0	4	4	1
0	2	2	4	0	0	4	2	2	0
2	3	3	0	0	0	0	3	3	2
1	4	4	3	0	0	3	4	4	1

A_7=

1	3	1	0	4	2	1	3	2	0
3	3	2	0	1	2	4	4	3	4
4	4	2	3	2	4	3	0	1	1
3	0	0	2	2	3	1	1	2	3
2	0	2	1	0	3	2	1	4	4
2	0	2	1	0	3	2	1	4	4
3	0	0	2	2	3	1	1	2	3
4	4	2	3	2	4	3	0	1	1
3	3	2	0	1	2	4	4	3	4
1	3	1	0	4	2	1	3	2	0

A_8=

3	0	2	3	3	3	3	2	0	3
3	4	3	0	2	2	0	3	4	3
3	1	2	2	1	1	2	2	1	3
0	2	2	0	1	1	0	2	2	0
3	1	4	2	4	4	2	4	1	3
0	2	1	4	3	3	4	1	2	0
3	2	0	3	4	4	3	0	2	3
2	1	0	1	4	4	1	0	1	2
1	4	0	1	3	3	1	0	4	1
2	4	0	0	0	0	0	0	4	2

A_9=

1	2	1	1	1	1	1	3	2	4
1	3	3	2	4	3	1	2	2	0
0	4	3	3	2	3	3	0	1	2
0	2	1	1	1	0	4	4	3	1
2	3	1	4	1	3	2	3	4	1
2	3	1	4	1	3	2	3	4	1
0	2	1	1	1	0	4	4	3	1
0	4	3	3	2	3	3	0	1	2
1	3	3	2	4	3	1	2	2	0
1	2	1	1	1	1	1	3	2	4

A_{10}=

4	3	3	3	0	0	3	3	3	4
4	0	1	2	4	4	2	1	0	4
2	1	4	1	3	3	1	4	1	2
1	4	3	4	4	4	4	3	4	1
2	3	0	2	2	2	2	0	3	2
4	1	1	3	3	3	3	1	1	4
4	1	2	4	0	0	4	2	1	4
3	0	2	0	1	1	0	2	0	3
3	2	4	3	0	0	3	4	2	3
2	0	0	1	4	4	1	0	0	2

A_{11}=

3	2	3	1	2	4	4	4	3	1
2	1	0	3	3	3	2	2	4	0
1	4	2	0	1	1	3	4	1	1
2	4	3	4	2	0	4	4	3	0
0	3	1	2	2	1	2	4	4	1
0	3	1	2	2	1	2	4	4	1
2	4	3	4	2	0	4	4	3	0
1	4	2	0	1	1	3	4	1	1
2	1	0	3	3	3	2	2	4	0
3	2	3	1	2	4	4	4	3	1

A_{12}=

0	3	0	0	0	0	0	0	3	0
4	0	4	4	3	3	4	4	0	4
3	1	3	2	1	1	2	3	1	3
1	4	3	3	2	2	3	3	4	1
1	2	3	3	1	1	3	3	2	1
3	1	3	0	1	1	0	3	1	3
1	3	1	3	4	4	3	1	3	1
2	4	1	0	3	3	0	1	4	2
2	1	2	1	3	3	1	2	1	2
3	0	2	4	1	1	4	2	0	3

$A_{13}=$

0	3	2	3	0	4	1	4	2	1
1	4	4	0	0	2	1	0	2	2
0	2	3	0	3	1	4	2	3	0
3	3	0	4	4	1	0	4	0	1
2	3	2	3	3	1	4	0	3	2
2	3	2	3	3	1	4	0	3	2
3	3	0	4	4	1	0	4	0	1
0	2	3	0	3	1	4	2	3	0
1	4	4	0	0	2	1	0	2	2
0	3	2	3	0	4	1	4	2	1

$A_{14}=$

3	4	2	3	1	1	3	2	4	3
3	3	3	3	1	1	3	3	3	3
0	0	3	3	3	3	3	3	0	0
3	3	1	1	3	3	1	1	3	3
1	0	1	4	4	4	4	1	0	1
1	2	4	0	1	1	0	4	2	1
4	3	2	3	2	2	3	2	3	4
0	3	2	4	2	2	4	2	3	0
3	1	4	1	4	4	1	4	1	3
4	2	1	4	1	1	4	1	2	4

$A_{15}=$

3	2	3	1	0	4	3	2	1	1
3	4	2	4	4	3	4	4	3	0
3	3	3	2	4	0	0	0	0	1
0	2	3	4	1	1	1	4	2	3
3	0	0	4	0	3	4	1	3	2
3	0	0	4	0	3	4	1	3	2
0	2	3	4	1	1	1	4	2	3
3	3	3	2	4	0	0	0	0	1
3	4	2	4	4	3	4	4	3	0
3	2	3	1	0	4	3	2	1	1

$A_{16}=$

1	4	1	3	4	4	3	1	4	1
4	0	0	0	0	0	0	0	0	4
1	4	0	4	4	4	4	0	4	1
4	2	1	3	1	1	3	1	2	4
4	2	4	4	1	1	4	4	2	4
3	1	1	0	1	1	0	1	1	3
2	0	1	1	0	0	1	1	0	2
0	4	4	3	2	2	3	4	4	0
4	0	2	2	0	0	2	2	0	4
1	3	0	2	1	1	2	0	3	1

$A_{17}=$

3	2	2	2	3	1	1	0	2	0
0	4	3	0	1	3	4	1	3	1
1	4	4	3	0	2	2	3	4	3
2	0	0	1	1	2	4	0	3	3
1	1	0	1	2	2	3	0	1	3
1	1	0	1	2	2	3	0	1	3
2	0	0	1	1	2	4	0	3	3
1	4	4	3	0	2	2	3	4	3
0	4	3	0	1	3	4	1	3	1
3	2	2	2	3	1	1	0	2	0

დანართი 2.

A_1=

0	1	1	0	0	0	1	1	0	1	1	1	1	0	1	0
1	0	0	0	1	1	0	1	0	1	0	1	1	0	1	0
1	1	0	0	1	1	1	0	1	0	1	0	1	0	1	0
0	0	0	1	0	1	0	1	1	0	0	1	1	0	1	0
1	1	1	1	1	1	0	1	1	0	1	0	1	0	1	0
0	0	0	0	1	1	1	0	1	0	1	1	0	0	0	1
1	0	1	0	1	0	1	1	0	0	0	1	0	0	1	0
0	0	1	1	1	0	1	0	1	0	1	1	1	0	1	0
1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	0
0	1	1	1	0	0	0	0	1	0	1	0	1	0	1	0
0	1	0	1	0	0	1	1	1	0	0	1	0	0	1	0
1	1	1	1	0	1	0	1	0	1	0	1	1	0	1	0
0	1	0	0	1	0	1	0	1	0	1	0	1	1	1	0
1	1	0	1	0	0	1	1	0	1	1	1	0	1	1	0
0	0	1	1	0	0	0	1	1	0	0	1	0	1	0	1
1	1	1	0	0	1	0	1	0	0	0	1	0	1	0	1

A_2=

1	1	1	1	1	0	1	0	1	0	1	0	0	1	0	0
0	0	0	0	1	0	1	1	1	1	1	0	0	0	0	0
0	1	0	1	0	0	1	0	0	1	0	0	1	1	1	1
1	1	0	1	0	0	0	0	1	0	1	1	1	1	1	1
1	0	0	0	1	0	0	1	0	0	0	1	1	1	1	0
0	0	1	1	1	0	0	0	1	1	1	0	0	0	0	0
1	0	0	0	1	0	0	1	0	0	1	1	1	1	0	1
0	1	1	0	1	0	0	1	1	1	0	0	1	1	1	0
0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	1
0	0	0	1	0	1	0	1	0	1	0	1	0	0	0	0
0	0	0	1	0	0	0	1	0	0	1	0	1	0	1	1
1	0	0	1	1	1	0	1	1	0	0	0	1	0	1	0
0	0	1	1	0	1	1	0	1	1	1	0	0	0	1	1
1	1	0	0	0	1	0	0	0	0	1	1	1	1	0	1
0	0	1	1	1	1	0	0	1	0	0	0	1	1	0	0
1	0	0	0	0	1	1	1	0	1	1	0	1	1	0	1

A_3=

1	0	0	1	1	0	0	1	0	0	0	0	1	1	1	1
0	1	0	1	1	0	1	1	1	0	0	1	0	0	1	1
0	0	0	0	0	1	1	0	0	0	1	0	1	1	1	0
1	1	0	1	0	1	0	1	1	0	0	0	1	1	1	1
0	1	1	0	1	1	0	0	1	1	0	1	1	0	0	0
0	0	1	0	1	0	1	0	1	0	1	0	0	1	1	1
1	0	1	0	1	1	0	0	0	0	0	1	0	1	0	0
0	1	0	0	0	1	0	1	0	1	1	1	0	1	1	0
1	1	0	0	1	1	0	0	0	0	0	0	1	1	1	0
1	1	0	0	1	1	0	1	0	1	1	1	1	1	0	0
1	1	0	0	0	1	0	1	1	0	0	0	0	0	1	0
1	0	0	1	0	0	0	0	1	0	1	1	0	1	0	1
0	0	1	0	0	0	1	0	1	1	1	1	0	1	0	0
1	0	1	0	0	0	0	1	1	0	0	1	0	0	1	0
1	0	0	1	0	1	1	1	0	1	0	1	0	1	1	1
0	1	0	1	0	0	1	0	0	1	1	1	1	1	1	0

A_4=

0	1	0	1	1	1	1	1	1	1	1	0	0	0	1	1
0	0	0	1	0	0	1	1	1	1	0	1	1	1	0	1
1	0	0	1	1	1	1	0	0	0	1	1	0	0	1	1
0	1	0	1	0	0	0	0	0	1	0	1	1	0	1	1
0	0	0	0	1	1	1	1	0	1	0	0	1	0	0	1
0	0	1	0	0	0	0	0	0	0	1	1	1	0	1	1
1	1	0	1	0	1	0	0	1	1	0	0	1	1	1	0
1	0	1	0	0	1	0	0	0	0	0	0	1	1	0	0
0	0	0	1	1	1	0	1	1	1	0	0	1	1	0	0
1	0	1	0	1	1	1	0	0	0	1	0	1	1	0	0
1	1	1	0	1	0	1	1	1	1	1	1	1	0	1	0
0	1	1	0	1	1	1	1	0	1	0	0	0	0	1	0
0	0	1	0	0	0	1	0	1	1	1	1	1	0	0	1
0	1	1	0	0	1	0	0	1	0	0	0	1	1	1	1
0	0	1	1	0	0	0	1	0	0	1	1	0	0	1	0
0	1	1	0	1	0	1	1	1	0	1	1	1	0	0	1

A_5=

0	1	0	1	1	0	1	1	0	1	1	0	0	1	1	0
0	0	0	1	1	1	0	0	0	0	1	0	1	0	0	1
0	1	1	1	0	1	0	1	1	0	1	1	0	1	1	0
1	1	0	1	1	0	1	0	0	1	0	0	1	0	1	0
1	1	1	1	0	0	0	0	1	0	0	0	1	1	0	1
1	0	0	0	0	0	0	1	1	1	0	1	1	1	1	0
1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0
0	0	0	0	1	0	1	1	0	1	0	0	1	0	0	1
1	0	0	1	0	1	0	1	1	1	1	1	0	1	0	1
0	1	0	0	1	1	1	0	0	1	0	1	1	1	1	1
1	0	1	0	1	1	0	0	1	1	1	1	0	1	0	1
0	0	1	1	0	1	0	1	1	0	0	1	1	0	1	0
0	1	0	1	0	1	0	1	0	0	1	1	1	0	0	1
1	1	1	0	1	0	0	1	0	0	1	0	1	1	1	0
1	0	1	1	0	0	1	0	1	0	0	0	0	0	1	0
0	1	0	1	1	0	0	1	1	0	1	0	0	1	0	0

A_6=

0	0	0	0	1	1	0	0	1	1	1	0	1	0	0	1
0	1	0	1	1	1	1	0	0	0	1	0	0	0	1	1
1	0	1	1	0	1	1	0	1	1	1	1	0	1	1	1
0	1	1	0	0	0	1	1	0	1	1	1	0	1	1	0
0	0	0	0	0	1	1	1	0	1	0	1	0	0	0	1
0	0	1	0	0	0	0	1	0	1	1	0	0	0	1	1
1	1	1	1	0	0	1	1	0	1	0	1	0	1	0	0
0	0	1	0	1	1	0	1	0	0	0	1	0	0	1	1
1	1	1	0	0	0	1	0	0	0	0	0	1	1	1	1
1	1	1	0	1	0	0	1	1	1	1	0	0	1	0	0
1	0	0	1	0	1	1	0	0	1	1	0	1	1	1	0
1	1	1	1	1	0	0	1	1	1	0	1	0	1	1	0
1	0	0	0	0	1	1	1	0	0	1	1	0	1	0	1
1	1	0	0	0	1	1	0	0	1	0	0	0	0	0	0
0	0	0	0	0	1	0	1	0	1	0	1	1	0	0	0
1	1	0	0	1	0	1	0	0	0	0	1	0	1	1	1

A_7=

0	1	0	1	1	0	1	1	1	1	0	0	0	0	1	0
0	0	1	0	1	0	0	0	0	0	1	1	1	1	0	1
1	1	1	1	1	1	0	0	0	0	0	0	0	1	0	0
1	1	0	1	0	0	0	0	1	1	0	1	1	0	1	1
1	0	0	1	1	1	1	1	1	0	1	0	1	1	1	0
1	0	1	0	1	0	1	0	0	1	1	1	0	0	0	1
0	0	1	0	1	1	1	1	0	0	0	1	1	0	1	1
0	1	0	1	1	1	1	1	1	1	0	0	0	1	1	0
1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0
0	0	0	1	0	0	1	1	1	0	0	0	0	0	1	0
0	0	0	0	0	1	1	0	0	1	0	1	1	0	1	0
0	1	0	0	1	0	1	0	1	1	1	1	1	1	1	1
0	0	0	0	0	0	1	1	0	1	1	1	0	1	0	0
0	0	0	0	1	0	1	1	0	0	0	0	1	0	1	1
1	1	1	0	1	0	1	1	1	1	0	1	0	0	1	1
0	0	1	0	0	1	0	1	1	0	0	1	1	1	1	0

A_8=

0	0	0	1	1	0	0	1	1	1	0	1	0	0	0	0
1	0	1	0	0	1	0	1	0	1	0	0	0	0	1	0
0	1	1	1	0	0	1	1	0	1	0	0	1	1	1	0
1	0	0	0	1	0	1	1	1	1	1	1	0	0	0	1
1	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0
0	1	0	1	1	0	1	0	0	1	0	0	1	0	1	1
1	1	0	1	1	0	1	1	0	1	0	0	0	1	1	0
0	1	1	1	0	0	0	1	0	0	1	1	0	0	1	1
0	0	1	0	0	0	1	0	1	0	0	1	1	0	1	0
0	1	1	0	0	1	1	1	0	0	0	1	1	1	1	0
0	1	1	1	1	0	0	1	0	0	1	0	1	0	1	1
1	1	1	0	1	1	0	0	1	0	0	1	1	0	1	1
1	0	0	0	0	0	0	0	1	1	1	1	0	1	1	1
0	0	1	0	0	1	0	0	0	0	1	1	0	0	0	1
1	0	0	0	1	0	0	0	1	1	1	0	0	1	0	1
1	0	0	1	0	0	1	1	1	0	1	0	1	1	1	1

A_9=

1	0	0	1	0	1	0	1	1	0	0	0	1	1	1	1
1	0	0	1	0	0	1	0	1	1	1	1	1	0	0	1
0	1	1	1	1	0	0	1	1	1	0	0	1	1	0	0
1	1	0	0	0	0	0	0	1	1	0	0	1	1	0	1
1	1	1	1	0	0	1	0	1	0	0	1	0	1	1	1
1	1	1	1	0	1	0	0	1	1	0	1	1	1	1	1
0	0	1	0	1	1	1	1	0	0	0	1	1	0	1	0
0	1	1	0	1	0	0	0	1	1	1	1	0	0	0	0
0	1	0	0	1	1	1	0	1	0	1	1	1	1	1	0
0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	1
0	1	0	0	1	0	1	1	1	1	0	1	0	1	0	1
1	1	1	1	0	1	1	1	1	0	1	0	1	1	0	0
1	0	1	0	1	0	0	0	0	0	1	1	1	0	1	1
1	0	0	0	0	1	0	1	1	1	0	0	1	1	1	0
0	1	1	0	1	1	1	0	0	0	0	1	1	0	1	0
1	0	0	1	0	0	1	0	0	1	0	1	1	1	0	1

A_{10}=

0	0	1	0	0	0	1	1	1	0	0	0	1	1	0	1
1	0	1	1	1	0	0	1	0	0	0	0	1	0	1	0
0	1	0	1	0	1	0	1	0	1	0	1	1	0	1	1
1	1	0	1	1	1	1	1	1	1	0	0	1	0	0	1
0	0	0	0	0	0	1	1	1	0	1	0	0	0	0	0
1	0	0	1	0	0	0	0	0	1	0	1	1	1	0	0
1	0	1	0	0	1	1	1	0	1	1	0	1	1	0	0
0	0	0	0	1	0	1	1	0	1	1	1	0	0	1	0
0	1	1	0	1	0	1	0	1	0	0	1	1	1	1	0
1	0	1	0	1	0	0	1	1	1	1	1	1	0	0	0
1	1	0	1	1	0	1	1	0	1	0	0	0	1	1	0
0	1	0	0	1	1	1	1	1	0	0	1	1	1	1	1
0	0	0	1	0	1	1	0	1	0	1	1	0	1	0	0
0	1	1	1	1	0	1	1	1	0	0	1	0	1	1	0
0	0	0	0	1	0	1	0	1	0	0	0	0	0	1	0
0	1	1	0	1	0	1	0	1	1	1	0	0	0	0	0

A_{11}=

1	1	0	1	0	0	0	1	0	0	0	1	0	1	1	0
1	1	1	0	0	1	1	1	1	0	1	0	1	0	0	1
1	0	1	1	0	1	0	1	1	1	0	1	1	1	1	0
1	1	0	0	1	1	1	1	0	1	1	0	0	0	0	1
1	0	1	1	1	0	0	0	0	1	1	1	1	0	1	0
1	1	1	1	1	1	1	0	0	1	0	1	1	0	1	0
1	1	0	1	0	1	0	1	0	1	0	1	0	1	1	0
0	1	1	1	1	1	1	0	0	1	0	0	1	0	0	0
1	0	0	0	1	0	0	1	1	0	1	1	0	1	0	1
1	0	1	1	1	0	0	1	1	0	1	0	0	1	0	0
1	0	0	1	0	0	0	1	0	0	1	1	1	0	1	1
1	1	1	1	0	0	0	1	1	0	1	0	0	1	1	1
1	1	1	1	0	0	1	1	1	1	1	1	1	0	0	1
0	0	1	1	1	0	0	1	1	1	1	0	0	0	0	1
0	1	0	1	1	0	0	0	0	1	0	0	0	1	0	0
1	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1

A_{12}=

1	0	1	1	1	1	1	0	1	0	0	1	0	0	0	1
1	0	0	1	0	1	0	1	1	1	1	0	1	0	0	1
0	1	1	1	1	1	0	0	0	0	1	0	0	0	0	0
1	1	1	1	0	1	1	0	0	0	0	0	0	1	1	0
0	1	1	0	0	1	0	0	0	1	1	1	0	1	0	0
0	1	1	0	1	0	1	1	1	1	1	1	1	1	0	1
1	0	0	1	0	0	0	0	1	0	1	1	0	0	0	1
0	1	1	1	0	1	1	0	1	0	0	0	0	1	0	1
1	0	0	0	0	1	0	0	1	1	0	0	0	1	1	0
1	1	0	0	0	0	0	0	1	1	1	0	1	0	1	1
0	0	0	0	0	0	1	1	1	1	0	1	1	1	1	0
0	1	0	1	0	1	1	1	0	1	0	1	0	0	1	0
0	0	0	1	0	1	1	1	1	0	1	0	1	0	0	1
0	0	1	1	0	1	1	1	1	1	0	1	0	1	1	1
0	1	0	1	1	0	1	0	0	0	1	1	1	1	1	1
0	0	1	0	0	0	0	1	0	0	0	1	0	1	1	1

A_{13}=

0	0	0	0	0	0	1	0	1	0	1	0	1	0	1	0
1	0	0	0	0	1	0	1	1	0	0	0	1	1	0	0
1	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0
1	0	1	1	0	1	1	1	1	0	0	0	0	1	1	1
1	0	0	0	0	1	1	0	1	0	1	0	1	1	1	0
0	1	0	1	0	0	0	1	1	0	1	0	0	0	0	0
0	0	1	1	0	1	0	1	0	0	1	1	1	0	0	0
0	1	1	0	1	1	0	1	1	0	0	0	1	0	0	1
0	1	1	1	1	0	1	1	1	0	0	1	0	0	1	0
0	0	0	1	0	1	1	0	0	0	0	0	1	1	1	0
0	1	0	1	0	0	0	0	1	0	0	1	1	1	1	0
1	1	1	0	0	1	1	1	1	0	1	1	1	0	1	0
1	0	1	1	0	0	1	0	1	1	1	0	1	1	0	1
0	1	0	1	1	1	1	0	1	0	1	1	1	1	0	0
1	0	0	0	0	1	0	1	1	1	0	1	1	1	0	0
1	1	0	1	0	0	1	0	0	0	1	1	0	1	0	0

A_{14}=

1	1	0	0	1	0	0	0	1	0	0	0	1	1	0	1
1	0	1	1	1	1	0	1	0	1	0	0	1	1	1	1
1	1	1	0	1	1	0	1	1	1	0	1	0	1	0	1
1	0	0	0	1	1	0	1	0	0	1	0	1	1	1	0
1	1	0	0	0	0	0	1	1	1	0	1	1	0	1	1
0	0	1	1	1	1	1	1	1	0	1	1	0	0	0	1
1	0	1	1	1	0	1	1	1	0	0	1	0	0	0	0
1	1	0	0	0	0	0	0	1	0	1	1	1	0	0	0
0	0	0	1	1	1	0	0	1	1	1	1	0	1	1	0
0	1	1	1	0	0	1	1	1	0	0	0	1	1	1	0
1	0	1	0	0	0	0	0	1	1	0	1	1	0	1	0
1	0	1	1	0	0	0	1	1	0	1	0	0	1	1	0
0	0	0	0	0	1	1	1	1	0	1	1	1	1	0	0
0	0	1	0	1	1	1	1	1	1	0	1	1	0	1	0
0	0	1	1	1	1	1	0	0	1	1	0	1	1	0	0
1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1

A_{15}=

1	0	0	1	1	1	1	0	1	0	0	0	0	0	1	0
0	1	1	1	1	1	0	1	0	0	1	1	1	0	1	1
0	0	0	1	1	1	1	1	1	0	1	1	1	1	0	0
0	1	1	0	1	0	1	1	1	0	0	0	0	0	1	1
0	1	0	1	1	1	1	1	0	0	1	1	0	0	1	1
0	0	1	0	0	0	1	1	1	1	0	1	0	1	1	1
0	0	1	1	0	0	1	1	1	1	0	1	0	0	1	1
0	1	1	0	0	0	1	1	0	0	0	1	1	1	0	1
1	0	1	1	0	0	1	1	1	0	0	0	0	1	0	0
0	0	1	0	1	0	1	1	1	1	1	1	1	0	0	0
0	1	0	0	1	1	0	1	1	1	0	0	1	0	1	0
0	0	0	0	1	1	1	1	1	0	1	1	1	1	1	1
1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0
0	0	0	1	1	0	1	1	1	0	1	1	1	0	0	0
0	0	0	1	0	1	0	0	1	0	1	0	0	0	1	1
1	0	1	1	0	1	1	0	0	0	0	0	1	1	1	1

A_{16}=

1	0	0	0	1	0	0	1	0	0	1	1	1	0	0	1
0	1	0	1	1	1	0	0	0	1	1	1	1	0	0	1
1	1	1	1	0	1	0	1	0	0	0	1	1	0	0	0
0	0	1	1	1	0	1	1	1	1	0	1	0	0	1	1
1	0	1	1	1	0	0	0	0	1	1	0	1	0	0	0
0	1	1	1	0	0	0	1	0	0	0	1	1	1	1	0
1	1	0	0	1	0	0	1	1	1	0	0	1	0	0	1
1	0	1	0	0	1	1	0	0	0	0	0	0	1	0	1
0	0	1	0	0	1	1	0	0	0	0	1	1	1	1	1
0	0	1	1	1	0	0	1	1	1	0	1	0	0	0	0
0	1	1	0	0	1	0	0	0	0	0	0	1	0	1	1
1	0	0	1	0	0	1	0	0	0	1	0	1	0	1	0
1	0	0	0	1	0	1	1	1	1	0	1	1	1	0	1
1	0	1	0	0	1	1	0	1	1	1	0	0	0	1	0
1	0	0	1	1	0	1	1	1	0	1	1	0	1	1	0
0	0	0	0	1	1	0	0	1	0	0	1	1	1	0	1

A_{17}=

1	1	1	0	0	0	0	0	0	0	1	0	1	0	1	0
1	1	1	0	0	0	1	1	1	1	1	0	1	0	0	1
1	1	0	0	1	0	0	1	1	0	0	0	1	1	0	0
0	0	1	0	0	1	1	0	0	1	0	0	1	0	0	1
1	1	0	0	1	1	1	0	0	1	0	0	1	1	0	0
0	0	1	0	0	1	1	0	1	1	1	0	1	0	1	0
1	1	0	1	0	0	1	1	0	0	0	1	1	0	0	0
0	0	1	1	1	0	1	0	1	1	0	1	0	0	0	0
1	1	0	1	1	1	0	0	1	0	1	1	0	0	1	0
0	1	1	0	0	0	0	0	1	1	0	1	1	0	0	1
1	1	1	1	0	0	1	0	1	0	0	0	0	0	1	1
0	1	0	0	1	0	1	1	1	0	0	1	0	1	1	1
1	0	0	0	1	1	1	0	0	0	1	1	0	1	1	1
0	0	1	0	1	0	1	1	0	0	0	1	1	0	0	1
0	0	1	0	0	0	1	0	0	1	0	1	1	0	0	0
0	0	1	0	0	0	1	0	0	1	0	1	1	0	0	0

A_{18}=

1	1	1	1	1	1	0	0	1	0	1	0	0	0	1	1
0	1	0	1	1	1	0	0	0	1	1	1	1	0	0	0
1	1	0	0	1	1	0	0	1	0	1	1	0	1	1	1
1	0	0	1	1	1	0	0	0	1	0	1	0	0	1	1
0	0	1	0	1	1	1	0	1	0	0	1	1	1	1	1
1	0	1	0	1	1	0	1	0	0	0	0	0	0	1	1
1	1	1	1	0	0	0	0	0	1	1	0	0	1	1	1
0	1	0	0	1	0	1	1	0	1	1	0	1	1	1	1
1	0	1	1	1	1	1	0	1	1	1	0	1	1	1	1
1	1	1	0	0	0	1	1	0	0	0	1	0	0	1	1
1	0	0	0	0	1	1	1	0	1	1	0	0	1	1	1
1	1	0	1	0	0	0	0	0	0	0	1	1	0	0	0
1	1	0	0	1	0	0	1	1	1	1	0	1	1	1	1
0	0	0	0	0	0	0	1	0	1	1	0	0	0	1	1
1	0	1	0	1	0	1	0	1	1	0	0	0	0	0	0
1	0	1	0	0	1	0	1	0	0	0	1	1	0	1	1

A_{19}=

0	0	1	1	0	1	1	0	1	0	1	0	1	0	1	1
1	0	1	1	0	1	0	1	1	0	0	0	1	0	0	1
0	1	0	0	0	1	0	1	0	0	0	1	0	1	1	0
0	1	0	1	1	1	1	0	0	0	0	0	1	0	1	0
0	1	0	1	0	0	1	1	0	1	0	0	1	0	0	0
1	1	1	1	1	1	0	0	0	0	0	1	0	0	0	0
0	1	0	1	1	1	1	1	1	0	0	0	0	0	1	0
1	0	0	1	0	1	0	0	0	0	0	1	0	0	1	0
1	0	0	1	1	0	1	1	0	1	0	0	1	1	0	0
1	0	1	0	1	0	1	1	1	0	1	1	1	1	0	1
1	1	1	1	1	1	1	0	1	1	1	1	1	0	0	0
1	1	0	1	0	1	1	0	1	0	0	1	0	0	1	1
0	0	1	1	1	1	0	1	0	0	0	1	0	0	0	0
0	1	1	1	1	1	0	1	0	1	1	1	1	0	0	1
0	0	1	0	0	0	1	0	0	1	0	1	1	0	0	0
0	0	1	0	0	0	1	0	0	1	0	1	1	0	0	0

A_{20}=

1	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0
1	1	1	0	0	1	0	1	0	0	1	0	1	0	1	1
1	1	1	1	1	1	0	0	0	0	0	1	1	1	0	0
0	0	1	0	1	0	1	0	1	1	0	1	1	0	1	1
0	0	0	0	0	0	0	0	1	1	1	0	0	1	1	1
0	0	1	1	1	0	1	0	0	0	1	0	1	0	0	0
0	1	1	1	1	0	0	1	1	0	0	1	1	1	1	1
0	1	0	0	0	1	0	0	1	0	1	1	0	1	0	0
0	1	0	0	1	1	0	0	1	0	0	0	1	0	1	1
0	1	1	1	0	1	0	0	0	0	1	1	1	0	0	0
1	1	1	0	1	1	0	1	1	1	1	1	0	0	1	1
0	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0
1	1	0	1	1	0	0	0	1	1	1	0	0	1	1	1
0	0	0	0	1	1	1	0	1	0	1	1	1	0	0	0
1	0	0	0	1	0	1	1	0	1	1	0	0	0	1	1
0	1	1	1	0	1	1	0	1	1	0	1	1	1	0	0

A_{21}=

1	0	0	1	0	1	0	0	1	0	1	0	0	0	1	1
1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0
0	1	0	0	1	0	0	1	1	1	0	1	1	1	0	0
0	0	1	1	0	1	1	1	1	1	0	1	0	1	1	1
1	0	1	0	0	1	1	1	0	0	1	0	0	0	0	0
0	0	1	1	1	0	1	1	1	0	1	1	1	1	1	0
1	1	1	0	1	1	0	0	1	0	1	0	0	1	0	1
1	1	1	0	0	0	0	0	0	0	1	0	1	0	1	0
0	0	0	1	0	1	1	1	0	1	1	0	0	1	1	1
0	0	1	0	1	0	1	1	0	1	0	1	1	1	0	0
0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1
0	0	1	0	0	0	1	0	1	1	1	1	1	0	1	1
1	1	0	1	0	1	0	0	0	0	1	0	1	1	0	0
0	0	0	0	1	0	0	1	1	1	1	1	0	0	0	0
1	0	0	1	1	1	0	1	1	0	1	1	0	1	0	1
1	0	0	1	1	1	0	1	1	0	1	1	0	1	0	1

A_{22}=

1	1	0	0	1	0	1	1	0	0	0	0	1	0	1	1
0	0	1	1	1	0	0	1	0	0	1	1	0	1	1	1
1	1	0	0	0	0	1	1	0	1	1	0	1	1	0	0
0	1	0	1	0	1	1	0	0	1	0	0	0	1	0	0
1	0	0	1	1	1	1	1	0	0	0	1	0	1	0	0
0	1	1	1	1	0	0	1	1	1	0	0	0	1	1	1
1	0	0	1	1	0	1	0	1	1	1	1	0	0	1	1
1	1	1	0	0	1	0	0	0	0	1	1	0	1	1	1
0	1	0	0	1	0	1	1	1	0	0	0	1	0	0	0
0	0	0	0	1	1	1	1	1	0	1	0	0	1	0	0
0	0	0	0	1	0	0	1	1	0	0	1	1	1	0	0
1	0	1	0	1	1	0	0	1	0	0	0	0	1	1	1
1	1	0	1	1	0	0	0	1	1	1	0	0	1	1	1
1	0	1	0	1	1	1	0	0	0	1	1	1	0	1	1
1	0	1	1	0	1	0	0	0	0	0	1	0	0	1	1
1	1	0	1	1	0	1	1	0	0	0	1	1	1	1	1

A_{23}=

1	1	1	0	0	0	0	0	0	0	1	0	1	0	1	1
0	0	1	0	0	1	0	0	1	1	1	1	0	1	1	1
1	0	1	1	0	0	0	1	0	1	1	1	1	1	1	1
0	0	1	0	0	1	1	0	0	1	0	0	1	0	0	1
0	1	1	1	0	0	0	1	1	0	1	0	0	0	0	0
1	0	1	1	1	0	1	1	0	1	0	1	1	1	1	0
0	1	0	0	1	1	1	0	1	0	1	0	1	1	0	0
0	0	0	1	1	0	0	0	1	0	0	0	1	0	0	0
0	0	0	1	1	0	1	1	1	0	1	0	1	1	0	1
0	0	0	1	1	0	0	0	0	0	1	0	1	0	1	1
0	1	0	0	1	1	0	1	0	1	1	0	1	1	1	1
0	0	1	1	0	0	1	1	0	1	1	0	0	1	0	1
0	0	1	1	0	0	0	1	1	1	0	1	1	0	1	1
1	1	1	0	1	1	0	0	0	0	0	0	0	1	1	1
1	1	0	0	0	1	1	1	0	0	0	1	1	1	1	1
1	1	0	0	0	1	1	1	0	0	0	1	1	1	1	1

A_{24}=

0	1	1	0	1	1	0	0	1	0	0	0	1	0	1	1
0	0	1	1	1	0	0	1	0	0	1	1	0	1	1	1
0	0	0	1	1	1	1	1	0	1	1	1	0	0	0	0
0	1	1	0	1	0	0	1	0	0	1	1	0	1	0	0
1	1	0	1	1	0	1	1	1	1	1	1	1	0	0	0
0	0	1	1	1	1	0	1	0	0	1	0	1	0	1	1
0	1	0	0	0	1	1	0	1	1	1	0	1	1	1	1
1	1	0	1	1	0	1	1	0	1	0	0	0	1	1	1
0	1	0	0	1	0	1	1	1	0	0	0	1	0	0	0
0	0	1	1	0	0	0	0	1	1	0	1	0	1	0	0
0	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0
1	0	0	1	0	0	1	1	1	1	1	1	0	1	1	1
0	1	1	1	1	1	1	1	0	1	1	0	0	1	1	1
1	0	0	1	0	0	0	1	0	1	0	0	1	0	1	1
1	1	0	0	1	1	1	1	1	0	0	0	1	1	1	1
1	0	0	1	1	1	1	1	1	1	1	1	0	0	1	1

A_{25}=

1	0	1	0	1	0	1	1	0	0	0	1	1	1	1	1
0	1	1	1	0	0	1	0	1	0	0	1	0	1	1	0
1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	1
0	1	0	1	1	1	1	0	0	0	0	0	1	0	1	1
0	0	0	0	1	0	0	1	1	1	1	0	0	0	1	0
1	1	0	1	1	1	1	0	0	1	0	0	1	0	0	1
0	1	1	1	1	1	0	1	1	1	0	1	1	0	1	0
0	0	1	0	1	0	1	1	1	1	1	1	1	1	1	0
0	0	0	0	0	1	1	0	1	1	1	1	1	0	0	0
0	0	1	1	0	1	1	0	0	0	0	0	1	0	0	0
0	1	1	0	0	0	1	1	0	1	0	0	1	1	0	0
0	1	0	0	1	0	1	1	0	0	1	0	0	1	1	1
0	1	1	0	0	1	1	1	1	0	1	1	1	0	1	0
1	0	1	1	1	0	1	0	0	1	1	0	0	1	1	0
1	1	0	0	0	1	1	1	0	0	0	1	1	1	1	1
1	1	0	0	0	1	1	1	0	0	0	1	1	1	1	1

A_{26}=

1	0	1	1	0	0	0	0	1	0	0	1	0	1	1	1
1	0	0	1	1	1	1	0	1	0	1	1	0	1	1	1
1	1	1	1	1	1	0	0	0	0	0	1	1	1	0	0
0	0	1	0	1	1	0	1	1	1	0	1	1	0	0	0
0	0	0	0	0	1	1	1	1	1	1	0	0	1	0	0
0	1	0	0	0	1	1	0	1	0	1	1	0	1	1	1
0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	1
0	0	1	1	1	0	0	0	0	0	1	0	1	0	1	1
0	1	0	0	1	0	1	1	1	0	0	0	1	0	0	0
0	1	1	1	0	1	0	0	0	0	1	1	1	0	0	0
1	1	1	0	1	0	1	0	1	1	1	1	0	0	0	0
0	1	1	1	0	0	0	0	1	0	0	1	1	0	1	1
1	0	1	0	0	0	1	1	0	1	1	1	1	0	1	1
0	1	1	1	0	0	1	0	0	0	1	0	0	1	1	1
1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	0	0	1	0	0	0	1	1	0	1	1	1	1

A_{27}=

0	0	0	0	1	0	0	1	0	0	0	1	0	1	1	1
0	1	0	1	1	1	0	0	1	0	1	1	0	1	0	1
1	1	0	1	0	1	0	0	0	1	1	0	1	0	0	0
1	0	1	0	1	0	1	0	0	1	1	0	0	0	1	0
1	1	1	1	1	1	0	1	1	0	0	0	1	0	1	1
1	0	1	0	0	1	1	0	0	0	0	0	1	0	1	1
0	0	1	0	1	0	1	1	1	0	1	1	1	0	1	1
0	1	1	1	1	1	0	1	1	0	0	1	1	1	1	1
1	0	0	0	1	0	1	0	1	1	0	1	0	0	1	1
1	1	1	0	1	1	0	0	0	1	0	0	0	0	1	0
1	0	1	1	1	0	0	1	0	0	0	0	0	1	1	0
1	0	1	1	1	1	1	1	0	1	0	0	1	1	1	0
0	1	0	0	1	0	0	1	1	0	0	1	1	0	0	1
1	0	0	1	0	1	0	0	0	1	0	0	0	1	0	1
1	1	0	0	0	1	1	1	0	0	0	1	1	1	1	1
1	1	0	0	0	1	1	1	0	0	0	1	1	1	1	1

A_{28}=

1	1	0	0	1	0	1	1	0	0	0	0	1	0	1	1
0	0	1	1	1	0	0	1	0	0	1	1	0	1	1	1
1	1	0	0	0	0	1	1	0	1	1	0	1	1	0	0
0	1	0	1	0	1	1	0	0	1	0	0	0	1	0	0
1	0	0	1	1	1	1	1	0	0	0	1	0	1	0	0
0	1	1	1	1	0	0	1	1	1	0	0	0	1	1	1
1	0	0	1	1	0	1	0	1	1	1	1	0	0	1	1
1	1	1	0	0	1	0	0	0	0	1	1	0	1	1	1
0	1	0	0	1	0	1	1	1	0	0	0	1	0	0	0
0	0	0	0	1	1	1	1	1	0	1	0	0	1	0	0
0	0	0	0	1	0	0	1	1	0	0	1	1	1	0	0
1	0	1	0	1	1	0	0	1	0	0	0	0	1	1	1
1	1	0	1	1	0	0	0	1	1	1	0	0	1	1	1
1	0	1	0	1	1	1	0	0	0	1	1	1	0	1	1
1	0	1	1	0	1	0	0	0	0	0	1	0	0	1	1
1	1	0	1	1	0	1	1	0	0	0	1	1	1	1	1

A_{29}=

1	1	1	0	0	0	0	0	0	0	1	0	1	0	1	1
0	0	1	0	0	1	0	0	1	1	1	1	0	1	1	1
1	0	1	1	0	0	0	1	0	1	1	1	1	1	1	1
0	0	1	0	0	1	1	0	0	1	0	0	1	0	0	1
0	1	1	1	0	0	0	1	1	0	1	0	0	0	0	0
1	0	1	1	1	0	1	1	0	1	0	1	1	1	1	0
0	1	0	0	1	1	1	0	1	0	1	0	1	1	0	0
0	0	0	1	1	0	0	0	1	0	0	0	1	0	0	0
0	0	0	1	1	0	1	1	1	0	1	0	1	1	0	1
0	0	0	1	1	0	0	0	0	0	1	0	1	0	1	1
0	1	0	0	1	1	0	1	0	1	1	0	1	1	1	1
0	0	1	1	0	0	1	1	0	1	1	0	0	1	0	1
0	0	1	1	0	0	0	1	1	1	0	1	1	0	1	1
1	1	1	0	1	1	0	0	0	0	0	0	0	1	1	1
1	1	0	0	0	1	1	1	0	0	0	1	1	1	1	1
1	1	0	0	0	1	1	1	0	0	0	1	1	1	1	1

A_{30}=

0	1	1	0	1	1	0	0	1	0	0	0	1	0	1	1
0	0	1	1	1	0	0	1	0	0	1	1	0	1	1	1
0	0	0	1	1	1	1	1	0	1	1	1	0	0	0	0
0	1	1	0	1	0	0	1	0	0	1	1	0	1	0	0
1	1	0	1	1	0	1	1	1	1	1	1	1	0	0	0
0	0	1	1	1	1	0	1	0	0	1	0	1	0	1	1
0	1	0	0	0	1	1	0	1	1	1	0	1	1	1	1
1	1	0	1	1	0	1	1	0	1	0	0	0	1	1	1
0	1	0	0	1	0	1	1	1	0	0	0	1	0	0	0
0	0	1	1	0	0	0	0	1	1	0	1	0	1	0	0
0	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0
1	0	0	1	0	0	1	1	1	1	1	1	0	1	1	1
0	1	1	1	1	1	1	1	0	1	1	0	0	1	1	1
1	0	0	1	0	0	0	1	0	1	0	0	1	0	1	1
1	1	0	0	1	1	1	1	1	0	0	0	1	1	1	1
1	0	0	1	1	1	1	1	1	1	1	1	0	0	1	1

$A_{31}=$

1	0	1	0	1	0	1	1	0	0	0	1	1	1	1	1
0	1	1	1	0	0	1	0	1	0	0	1	0	1	1	0
1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	1
0	1	0	1	1	1	1	0	0	0	0	0	1	0	1	1
0	0	0	0	1	0	0	1	1	1	1	0	0	0	1	0
1	1	0	1	1	1	1	0	0	1	0	0	1	0	0	1
0	1	1	1	1	1	0	1	1	1	0	1	1	0	1	0
0	0	1	0	1	0	1	1	1	1	1	1	1	1	1	0
0	0	0	0	0	1	1	0	1	1	1	1	1	0	0	0
0	0	1	1	0	1	1	0	0	0	0	0	1	0	0	0
0	1	1	0	0	0	1	1	0	1	0	0	1	1	0	0
0	1	0	0	1	0	1	1	0	0	1	0	0	1	1	1
0	1	1	0	0	1	1	1	1	0	1	1	1	0	1	0
1	0	1	1	1	0	1	0	0	1	1	0	0	1	1	0
1	1	0	0	0	1	1	1	0	0	0	1	1	1	1	1
1	1	0	0	0	1	1	1	0	0	0	1	1	1	1	1

ასეთი სახის, ანუ ორობითი სიმეტრიული მატრიცები, გვაძლევს მატრიცათა ველს.

გამოყენებული ლიტერატურა

1. Мишина А. М. и Проскуряков М. В. **Высшая алгебра**. 1967.

2. Эндбюс Г. **Теория разбиений**. 1992.

3. Курош А. Г. **Курс высшей алгебры**. М. Физ.-мат. литер., 1963.

4. Тараканов В. Е. **Комбинаторные задачи и (0,1) матрицы**. 1993.

5. Хорн Р., Джонсон Ч. **Матричный анализ**. Москва “Мир” 1999.

6. Маркус М., Минк Х. **Обзор по теории матриц и матричных неравенств**. 1998.

7. Питерсон У., Уэлдон, Э. **Коды, исправляющие ошибки**. "Мир" 1976. I-II том.

8. Берлекэмп Э. **Алгебраическая теория кодирования**. М. Мир, 1971.

9. Ван дер Варден Б. Л. **Алгебра** М. Наука, 1976.

10. Анин Б. **Зашита компьютерной информации**. Москва. 2000.

11. Молдовян А. А., Молдовян Н. А., Гуц Н.Д., Изотов Б. В**. Криптография, Скоростные шифры**. Санкт-Петербург. 2002.

12. Wiener W. **Cybernetics or Control and Communication in the Animal and the Machine.** John Wiley, New York, 1958. Русский пер: Винер Н. Кибернетика, или Управление и связь в животном и мащине, М,. Советское радио. 1969.

13. Wiener W. **The Human Use of Human Beings, Cybernetics and Society. Houghton Mifflin Co**., Boston, 1948. ქართული თარგმანი: ვინერი ნ. კიბერნეტიკა და საზოგადოება. თბილისი. 1958.

14. Shannon C.E. **A mathematical theory of communication**. Bell System Tech J. 27, 1948, n.3, pp. 379-423. 1948. п.4, pp. 623-656. Русский пер. Шеннон К. Работы по теории информации и кибернетике. М., Ил, 1963.

15. Shanon C. E. (1957) **Certain results in coding theory for noisy chsnnels. Information and Control**, p.p.6-25, თარგმანი [3].

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

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

18. Golay M.J.E. **Notes on Digital Coding. Proc**. IRE, 37, 1949, p.657.

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

20. Ростовцев А. Г. **Решеточный криптоанализ // Безопасность информационных технологий,** 1997. Вып. 2. С. 53-55.

21. Ростовцев А. Г., Маховенко Е. Б. **Введение в криптографию с открытым ключом,** - СПБ.: Мир и Семья, 2001.

22. Гост Р. 34.11 – 94. **Государственный стандарте Российской Федерации. Криптографическая зашита информации. Функция хеширования**. М.: Госстандарт Россий, 1994.

23. Лидл Р., Нидеррайтер Г. **Конечные ноля**: Пер с англ. М.: Мир, 1988. Т. 1-400ст.

24. Hamming R. W. **Error detecting and error correcting codes.** Bell System Tech. J., v, 29, 1950, pp. 147-160. Русский перю, Хемминг Рю Коды с обнаружением и исправлением ошибок. М., ИЛ, 1956.

25. Касами Т., Токура Н., Ивадари Е., Инагаки Я. **Теория кодирования**. М., Мир, 1978.

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

27. Wiener N. **My Connection with Cybernetics, its Origins and its Future.** Cybernetica (Namur), 1958, vol, n.1, pp.1-14. Русский пер., Винер Н. Мое отношение к кибернетике, ее прошлое и будущее. М., Совестское радио, 1969.

28. Гантмахер Ф.Р. **Теория матриц,** М., Наука, 1967.

29. Мельников В.В. **Защита информации в компьютерных системах**. М., Финансы и статистика, Электронинформ, 1997.

30. Diffie W. and Hellman M.E. **New directions in cryptography**. IEEE Trans. Inform. Theory, vol. IT-22, pp. 644-654, Nov, 1976.

31. Matsui M. **Linear cryptanalysis method for DES cipher // Advances in Cryptology** – EUROCRYPT '93, LNCS, v. 765, 1994.

32. S. C. Pohlig and M. E. Hellman, **AN improved algorithm for computing logarithms in GF(p) and its cryptographic significance**, IEEE Trans. Inform. Theory, vol. IT-24, pp.106-111, Jan. 1978.

33. Tuher Elgamal. **A public Key cryptosystem and signature scheme based on discrete logarithms in G. R. Klukley and David Chaum Fditors**. Advences in cryptology: Proseeding of crypto 84, volume 196 of lecture Notes in Computer Sience, pp.10-18, 19-22, Aug. 1984, Sgringer-Verlag 1985.

34. Merkle R. **Secure communications over insecure channels**. Commun. ACM, April 1978 (t.2.c.315, пример 15).

35. Rivest R.L. Shamir A. and Adelman L. **On digital signatures and public key cryptosystems.** Commun. ACM, vol, 21, no. 2, pp. 120-126. Feb1978.

36. Бухштаб А.А. **Теория чисел**, М., Госуд. учебн.-пед. издат., 1960.

37. Бухштаб А.А. **Теория чисел**. 2-е изд. М. Просвещение, 1966.

38. Гантмахер Ф. Р. **Теория матриц**. 1954.

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

40. Хассе Г. **Простие числа** М. ИЛ, 1953.

41. Ленстра Х.У. **Алгоритмы проверки на простоту //Алгебра и теория чисел** (с приложениями) Ж СБ, статей, М., Мир, 1987, вып. 43.

42. Василенко О.Н. **Применение круговых полей в криптосистемах RSA // IV Международная конференция «Современные проблемы теории чисел и ее приложения»,** Тела, 10-15 сентября, 2001, Тезисы докладов. с.35-40.

43. ElGamal Taher. **A subexponential-time algorithm for computing discrete logarithms over GF(p2). In David Chaum editor.Advanced in Cryptology**. Proceedings of crypto 83, pp.275-292, august 2003. Plenum Press, 1984.

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

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

46. Kolmogorov A. N. **To the Shannon theory of information in the continues signal case.** IRE Trans, P.G.I.T. , 1956. pp. 102-108 (Теория передачи информации, изд, ФР СССЗ, 1956).

47. Andrew M. Odlyzko, "**The future of integer factorization**", AT&T Bell Laboratories, July 11, 1995.

48. Coppersmith D. **Fast evaluation of discrete logarithms in fields of characteristic two**. IEEE Trans // Inform. Theory. 1984. V. 30(4). P.580-600.

49. Кострикин А. И. **Введение в алгебру**. М. Нфукф, 1977.

50. Боревич З. И., Шафаревич И. Р. **Теория чисел**. М, Мир, Наука, 1985.

51. Ленг С. **Алгебра**, М, Мир, 1968.

52. Шеннон К. **Работы по теории информации и кибернетике**. М., Ил, 1963.

53. Фано Р. **Передача информации. Статистическая теория связи**. М. Мир, 1965.

54. Мак-Вильямс Ф.дж., Слоэн Н.дж. **Теория кодов, исправляющих ошибки.** – М.: - Связь, 1979.

55. Василенко О. Н. **В 19 Теоретика – числовые алгоритмы в криптографии**. – М. МЦНМО, 2003. 328с.

56. Писсанецки С. **Технология разреженных матриц.** М. Мир, 1988.

57. Нечаев В. И. **Сложность дискретного логарифма // Научные труды МГПУ**. 1994. с.45-48.

58. Прахар К. **Распределение простых чисел**. М. Мир, 1967.

59. Трост Э. **Простые числа**. М. Физ-мат. литер. 1959.

60. Диксон Л. Е. **Введение в теорию чисел. Тбилиси**, Издат. Акад. Наук, 1941.

61. Холл М. **Комбинаторика.** М. Мир, 1970.

62. Ван дер Варден Б. Л**. Алгебра**, М. Наука, 1976.

63. Райзер Г. Дж. **Комбинаторная математика**. М. Мир, 1966.

64. Василенко О. Н. **Некоторые алгоритмы построения больших простых чисел** // Вестн. Моск. ун-та. Сер. 1. Матем. Механ. 1997. №5. с.62-65.

65. Рейнгольд Э., Нивергельт Ю. Део Н. **Комбинаторные алгоритмы. Теория и практика.** М. Мир, 1980.

66. Сидельников В.М., О **системе шифрования, построенной на основе кодов Рида-Соломона, Дискретная математика**, ., вып. /, стр.57-65, 1992.

67. Берлекэмп Э.П. **Алгебраическая теория кодирования**, М.: - Мир, 1971.

68. Смарт Н. **Криптография**, М, Технисфера, 2005, 528с.

69. Rivest R.L. Shamir A. and Adelman L. **On digital signatures and public key cryptosystems.** Commun. ACM, vol, 21, no. 2, pp. 120-126. Feb., 1978.

70. Shannon C.E. **A mathematical theory of communication. Bell System Tech J.** 27, 1948, n.3, pp. 379-423. 1948. п.4, pp. 623-656. Русский пер. Шеннон К. Работы по теории информации и кибернетике. М., Ил, 1963.

71. Niquist H. **Certain factors affecting telegrafh speed**. Bell System Tech. J. 1924, April, p.324; Certain topics in telegraph transmission theory, AIEE Trans., 47, 1928, April, p.617.

72. Adleman L. **The function field sieve //Proceedings of ANTS-I**. 1994. (Lect. Notes in Comput. Sci. V. 877). P.106-122.

73. Fiat A., Shamir A. **How to prove yourself: Practical solutions to identification and signature problems // Advances in Cryptology** – Crypto 86, Lecture Notes in Computer Science. Springer-Velag. 1987. Vol. 263 p. 186-194.

74. Виноградов И. М. **Основы теории чисел**. М. Наука, 1972.

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

76. Ростовцев А.Г. **Алгебраические основы криптографии**, ! Мир и Семья, СПБ, 2000.

77. Shanon C.E. **Communication Theory of Secrecy Systems**. Bell System Technical Journal, v. 28, n. 4, 1949.. pp. 656-715.

78. Kahn D. The Codebreakers: **The story of Secret Writting** New York: Macmilcan Publishing Co. 1967.

79. RSA Laboratories, PKCS #1: **RSA Encryption Standard**, version 1.5. Nov 1993.

80. RSA Laboratories, PKCS#3, **Diffie-Hellman Key-Agreement Standard**, version 1.4. Nov 1993.

81. ETEBAC, **Echanges Telematiques Entre Les Banques et Leurs Clients, Standard ETEBAC 5, Comite Francais d,Organisation et de Normalisation Bancaires**, Apr. 1989. (In French).

82. Diffie W. and Hellman M. E. **New directions in cryptography**, IEEE Trans. Inform. Theory, vd, It – 22, pp. 644-654 Nov. 1976.

83. Vernam G. S. **Cipher printing telegraph systems for secret wire and radio telegraphic communication**, J. Am. Inst. Electr. Eng. 45(1926), 109-115.

84. Date Encrypticn Standard. **National Bureau of standarts (NBS**), Federal Information Processing standard (FIPS) Publication nc. 46, Jan, 1977.

85. Schneier B. **Appliend cryptography**, Jehn Wiley and Sons, Inc. New York, 1996.

86. Menezes A., Oorschot van P., Vanstone S. **Handbook of Applied Cryptography.**

87. Shneier B. **Applied Cryptography**. John Wiley and Sons. Inc. New York. 1996.

88. Elgamal T. **A public key cryptosystem and signature**. Scheme based on discrete logarithms. IEEE Transactions on Infomation Theory, v. IT – 31, n. 4, 1985. pp 469-472.

89. Мейер Б. Бодуен К. **Методы программирования**, М., Мир, 1982.

90. Яглом А. М. Яглом И.М. (1973). **Вероятность и информация**. М. "Наука".

91. Fano R. M. (1949) Technical №65, **The Research Laboratory of Electronics**. MIT, March 17.

92. Nyguist H. **Certain factors effecting telegraph speed**. Bell Syst. Tech. J. April, 324, (1924), Certain topics in telegraph transmission theory, AIEE T rans, 47, April. 617.

93. 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.

94. Hartley, R.V.L., **Transmission of information**. Bell Syst, Techn. 1928, July, p.535. русский пер. Хартли Р. Передача информации. В сб. Теория Информации и ее приложения. М.: Физматгиз, 1959, с.5-35.

95. Shennon C.E. Weaver E. (1949), **Mathematical theory of communication**. Univ. of IM. Press. Urbana, I.U.

96. Kraft L.C. (1944), A. **Davice for Quantizing, Grouping and Coding Amplitude Modulated**. Pulses. M.S. thesis, Electrical Engineering Department MIT. march.

97. Brillouin L. (1956), **Science and Information Theory**. Academic Press Inc. Publishers. New York.

98. Дмитриев В.И. (1989**). Прикладная теория информации**. М. "Высшая алгебра".

99. Huffman D. A. (1952). A. **Method for the vonstruction of Minimum Redundancy Codes.** Proc. IRE, 40. 1098-1101.

100. Feinstein A. (1958) **Foundation of Information Theory.** Mograw Hill Book Comp. Inc. New York Toronto – London (თარგმანი: Файнстейн А. (1960) Основа Теории информации, М. Ил.

101. Gallager R. G. (1968). **Information Theory and Reliabl Communication.** John Willey and sons, Inc. New York. London. Sydney, Toronto (თარგმანი: Галлагер Р. (1974) Теория информации и наденая связь. М. Совстское радио.

102. Hartley, R.V.L. (1928), **Transmission of information**. Bell Syst, Techn. July, 535.

103. Мегрелишвили Р. П., Тогонидзе В. А., Булавришвили Д. З. **О методе ассоциативной идентификации, основанной на алгебраических структурах кодирования.** Труды Тбилисского государственного университета им. Ив. Джавахишвили, Прикладная математика, компьютерные науки, Т. 330 (19), с.67-71, 1998.

104. Мегрелишвили Р. П. **Высокоэффективные коды с коррекцией пакетов ошибок, обладающие простым алгоритмом декодирования**. Сообщения АН ГССР, Т. 91, №3, с. 581-584, 1978.

105. კოტრიკაძე გ. **ინფორმაციის დამუშავებისა და დაცვის, მეთოდური და ალგორითმული საშუალებანი**, პერიოდული სამეცნიერო ჟურნალი "აღმაშენებელი", 2007წ. №3, გვ.139-147.

106. კოტრიკაძე გ. **ინფორმაციის ღიად გადაცემის ახალი მეთოდის შემუშავება, პ**ერიოდული სამეცნიერო ჟურნალი "აღმაშენებელი", 2008წ. №4, გვ.20-27.

107. ბაღდავაძე გ., კოტრიკაძე გ. **მართვის მოწყობილობების სინთეზის ამოცანის გადაწყვეტის ალგორითმული მოდულების ეფექტურობის ამაღლების აუცილებელი და საკმარისი პირობები**, პერიოდული სამეცნიერო ჟურნალი "აღმაშენებელი", 2008წ. №4, გვ.57-62.

108. კოტრიკაძე გ. **ინფორმაციის დაცვის ასიმეტრიული სისტემის ახალი მეთოდის შემუშავება**, შრომები მართვის ავტომატიზებული სისტემები, სტუ, 2009წ., №1(6), გვ.53-57.

109. კოტრიკაძე გ. **ურთიერთკომუტატიურ მატრიცათა სიმრავლის შექმნა და მისი გამოყენება ინფორმაციის დასაცავად**, შრომები მართვის ავტომატიზებული სისტემები, სტუ, 2009წ., №1(6), გვ.58-61.