ინფორმაციის დაცვის მოცულობითი მატრიცის მეთოდის დამუშავება და მისი შედარება ასიმეტრიულ მეთოდებთან

გულნარა კოტრიკაძე, ნუგზარ ჩადუნელი
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

დამუშავებულ იქნა ახალი მოცულობითი მატრიცული მეთოდები, სადაც გამოყენებულ იქნა ორივე სისტემა: სიმეტრიული და ასიმეტრიული. მიღებულმა მეთოდებმა მნიშვნელოვნად გაზარდა გასაღების მიღებისა და, შესაბამისად, დაშიფვრისა და გაშიფვრის სისწრაფეც. დამუშავდა მათემატიკური მოდელები და ალგორითმები ზემოაღნიშნული მეთოდებისათვის.

საკვანძო სიტყვები: ინფორმაციის დაცვა. რიპტოგრაფია. მოცულობითი მატრიცული მეთოდები. სიმეტრიული და ასიმეტრიული მეთოდები. შიფრაცია. დეშიფრაცია. მათემატიკური მოდელები.

1. შესავალი

ნაშრომის მთავარი მიზანი და არსია ორ კანონიერ მომხმარებელს შორის ინფორმაციის საიმედო გაცვლა. ორ სუბიექტს შორის ინფორმაციის გაცვლა საჭიროებს დაცვითი მექანიზმის არსებობას. როცა ინფორმაციის გაცვლა ხორციელდება დახურული არხით, ამ დროს გასაღების გაცვლისათვის გამოიყენება კურიერი, ანუ მესამე პირი. ხოლო როცა ინფორმაციის გაცვლა ხდება ღია არხით, ანუ კურიერის გარეშე, გასაღების დაფიქსირება ხდება ღია არხით ორივე მხარეს. ამ დროს შესაძლებელია, რომ მესამე სუბიექტმა დაუკითხავად დაიჭიროს ეს ინფორმაცია. სასურველია, რომ მან ვერ შეძლოს რეალურ დროში მისი წაკითხვა („გატეხვა“), ანუ ინფორმაცია საჭიროებს საიმედო დაცვას.

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

თუმცა, ხდება ისეთი შემთხვევებიც, როცა ადგილი აქვს ინფორმაციის გამჟღავნებას, უფრო მეტიც – ინფორმაციის ჩანაცვლებას, გაყალბებას და ა.შ.

დავუშვათ, რომ გვაქვს ორი X და Y მხარეები, რომელთა შორის ხდება ინფორმაციის გაცვლა. ვთქვათ 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 აღვნიშნეთ, არსებობს ორი სახის სისტემა სიმეტრიული და ასიმეტრიული. ორივე სისტემებში განხილული მეთოდები გამოირჩევა საიმედოობით, მაგრამ მათაც აქვს დადებითი და უარყოფითი მხარეები. 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.

ორივე მეთოდი გამოირჩევა სხვადასხვა დადებითი მახასიათებლებით, ორივე მიღებულია კრიპტოგრაფიაში და დამტკიცებულია. 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. ჰაკერი ეცდება ჩაიჭიროს სუსტი რგოლი, ეს კი აუცილებლად უნდა გაითვალისწინოს მომხმარებელმა ინფორმაციის დაცვის დროს. გამოყენებულ უნდა იქნეს ისეთი მექანიზმები, რომ ინფორმაცია იყოს მთლიანად დაცული არაკანონიერი მომხმარებლებისაგან.

გასაღებში იგულისხმება, როგორც მარტივი რიცხვი, ასევე ვექტორი, ტექსტი და ა.შ. დაშიფრული 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.

კრიპტოგრაფია საკმაოდ აქტუალური თემაა და გამოყენებადია პრაქტიკაში. ჩვენს შემთხვევაში, ამოცანა მდგომარეობს შემდეგში: გამოყენებულია როგორც ასიმეტრიული მეთოდი ცალკე, და შექმნილია ორიგინალური მეთოდი, ასევე ორივე სიმეტრიული და ასიმეტრიული მეთოდების სინთეზი. განხილულია და აგებულია კომუტატიური მოცულობითი მატრიცები გასაღების მიღებისათვის, აიგება საკმაოდ მარტივად და თანაც მათი სიმრავლე არის იმდენად დიდი M^{nnn}, რომ მათი მოძებნა და ამორჩევა ყველასათვის ცნობილი და ხელმისაწვდომი მატრიცათა სიმრავლიდან, რეალურ დროში, შეუძლებელია [3-7].

ნაშრომის მიზანია ინფორმაციის დაცვის მაღალსაიმედო კრიპტოგრაფიული მეთოდების შექმნა, რომელიც უნდა ხასიათდებოდეს შიფრაციის და გასაღების გენერაციის მაღალი სიჩქარითა და მაღალი საიმედოობით არსებულ მეთოდებთან შედარებით. ჩვენი მიზანი იყო შეგვექმნა ისეთი ორიგინალური მეთოდი, რომელიც გამორჩეული იქნებოდა უკვე არსებული მეთოდებისაგან. განვიხილეთ არსებული, პრაქტიკაში გამოყენებადი მეთოდები და მივიღეთ ახალი მეთოდები. 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.

2. ძირითადი ნაწილი

2.1. ამოცანის დასმა

- მოცულობითი მატრიცის ასიმეტრიული მეთოდი.

გვაქვს ორი X და Y მხარეები.

ცნობილია P (მარტივი) რიცხვი, ცნობილია e სიდიდე. ე.ი. ცნობილია განზომილება, ასევე ცნობილი ხდება, e სიდიდეში და მატრიცაში შემავალი ელემენტები, რადგან ვიცით P რიცხვი. ცნობილია მატრიცათა სიმრავლე, რაც ყველასათვის ხელმისწვდომია.

- ასიმეტრიული მოცულობითი მატრიცული მეთოდის კომბინაცია სიმეტრიულ მეთოდთან.

გვაქვს ორი X და Y მხარეები, რომელთა შორის ხდება ერთიდაიგივე გასაღების დაფიქსირება. e სიდიდე უცნობია, გადაეცემა დახურული არხით. ამით უცნობი ხდება, როგორც e სიდიდის ასევე მოცულობითი მატრიცის განზომილება და მასში შემავალი ელემენტები. ინფორმაციის დაშიფვრა-გაშიფვრა და შესაბამისად გაცვლა ხდება ღია არხით (ამოცანა 1) [1,2,8,9].

სამეცნიერო სიახლე:

ამოცანა 1-ის ამოხსნისათვის გამოყენებულ იქნა დიფი-ჰელმანის მეთოდი, მაგრამ ახარისხების ფუნქცია შევცვალეთ მოცულობით მატრიცაზე გამრავლებით. ამით გასაღების გენერაციის დრო შემცირდა, საიმედოობით კი გაუტოლდა დიფი-ჰელმანის მეთოდის საიმედოობას.

ამოცანა 2-ში გამოყენებული იქნა მეთოდთა კომბინაცია. სიმეტრიული მეთოდით ანუ დახურული არხით ხდება საწყისი სიდიდის გადაცემა. ამის შემდეგ ღია არხით (ამოცანა 1) ხორციელდება გასაღების გენერაცია. რის შედეგადაც გასაღების გენერაციის სიჩქარე უმნიშვნელოდ შემცირდა, მედეგობის მნიშვნელოვნად გაზრდის ხარჯზე.

2.2. მოცულობითი მატრიცის ასიმეტრიული მეთოდი

ჩვენი მიზანი იყო, შეგვექმნა ისეთი ასიმეტრიული მატრიცული მეთოდი, რომელიც არსებულ მეთოდებთან შედარებით გამორჩეული იქნებოდა საიმედოობით, გაშიფვრის და ასევე დაშიფვრის სიჩქარით. გამოვიყენეთ კომუტატიური მოცულობითი მატრიცები. კერძოდ ღია არხით, ანუ რაც ყველასათვის ხელმისაწვდომია, მოვახდინეთ ჯერ გასაღების გამოთვლა, შემდეგ ინფორმაციის დასაიდუმლოება მიღებული გასაღებით.

მოცულობით მატრიცათა განზომილება და შესაბამისად სიმრავლე ცნობილია. საწყისი მომხმარებელი ანუ ის პიროვნება ვინც უგზავნის მეორე მხარეს ანუ მიმღებს ინფორმაციას, ის იღებს საწყის მატრიცას, მეორე მომხმარებელი კი – კომუტატიურ მატრიცას.

პირველ ეტაპზე, ორივე მომხმარებელმა უნდა მიიღოს ერთიდაიგივე გასაღები. წინასწარ ცნობილია E სიდიდე, ე.ი. ცნობილია განზომილება და სიმრავლე. ასევე ცნობილი ხდება მატრიცაში შემავალი ელემენტები.

გვაქვს ორი X და Y მხარეები.

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

$$y_1 \equiv e \times A_1 \ \mathrm{mod} P \ . \qquad (2.1)$$

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

$$K_1 = (e \times A_1) \times A_2 \equiv e \times A_1 \times A_2 \ \mathrm{mod} P \ . \qquad (2.2)$$

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

$$y_2 \equiv e \times A_2 \ \mathrm{mod} P \ . \qquad (2.3)$$

ხოლო X-ი აფორმირებს K გასაღებს:

$$K_2 = (e \times A_2) \times A_1 \equiv e \times A_2 \times A_1 \ \mathrm{mod} P \ . \qquad (2.4)$$

მაშასადამე, ორივე მხარემ მიიღო ერთიდაიგივე K გასაღები –

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

შიფრაციის საიმედოობა ეფუძნება, A_1 და A_2 საიდუმლო მატრიცების, მატრიცათა სიმრავლიდან ამორჩევის სირთულეს. მიუხედავად იმისა, რომ მატრიცის განზომილება ცნობილია, ე.ი. ცნობილი ხდება მატრიცაში შემავალი ელემენტების რაოდენობა, ასევე ცნობილია სიმრავლე 2^{n3}. ალბათობა არის $1/2^{n3.}$

აქვე უნდა აღვნიშნოთ განხილული მეთოდის საწყისი მოთხოვნა, რაც მდგომარეობს შემდეგში: იმისათვის რომ, ორივე მხარემ, მიიღოს ერთიდაიგივე K გასაღები აუცილებელია და საკმარისი, ისეთი A_1 და A_2 მატრიცების შერჩევა, რომლებიც იქნებიან ურთიერთკომუტატიური ანუ აკმაყოფილებენ პირობას:

$$\mathbf{A_1 \times A_2 \equiv A_2 \times A_1}\ . \qquad (2.6)$$

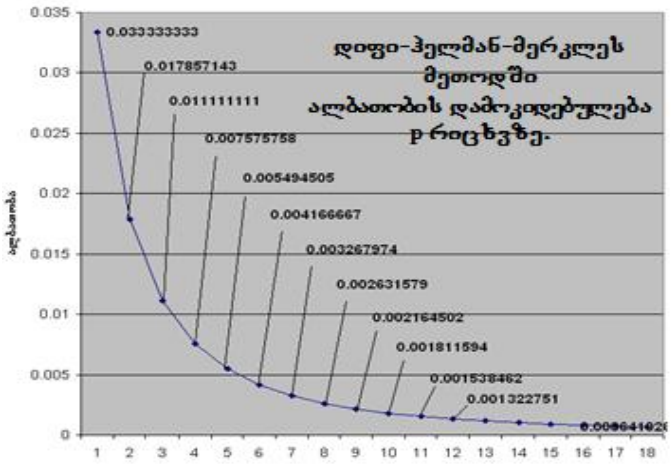
წინააღმდეგ შემთხვევაში, X და Y მხარეები ერთიდაიგივე K გასაღებს ვერ მიიღებს, რაც აუცილებელია წარმოდგენილი მეთოდისათვის [1,2,7,8].

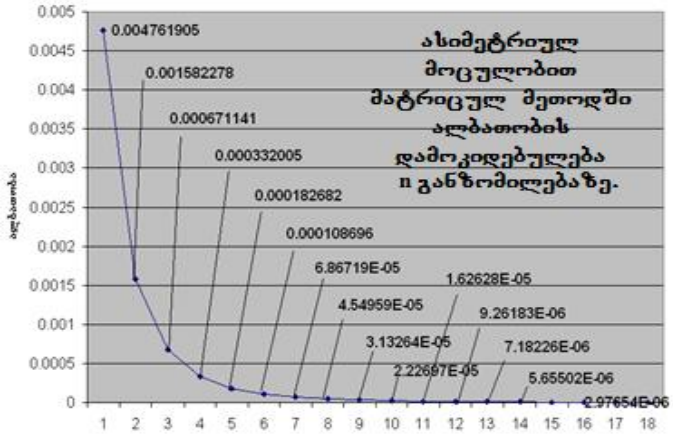
2.3. ასიმეტრიული მოცულობითი მატრიცული მეთოდის კომბინაცია სიმეტრიულ მეთოდთან

პირველ რიგში სანამ დაფიქსირდება გასაღები, სიმეტრიული მეთოდის გამოყენებით, ანუ კურიერით ხდება E სიდიდის გაცვლა. ამის შემდეგ უკვე ასიმეტრიული (ღია) არხით ხდება, ყველა დანარჩენი ოპერაციების ჩატარება. რადგან ვექტორი გადავეცით დახურული არხით, ამით უცნობი გახდა განზომილება. აქედან გამომდინარე, რადგან განზომილება გახდა საიდუმლო, მატრიცის ამორჩევის ალბათობა სიმრავლიდან კიდევ უფრო შემცირდა, რადგან სხვა მომხმარებელმა ჯერ განზომილება უნდა დაადგინოს და მერე უნდა ამოარჩიოს სიმრავლიდან, აღნიშნული კი გარკვეულ დროსა და ოპერაციების ჩატარებას მოითხოვს. საბოლოოდ კი მივდივართ იქამდე, რომ კომბინირებული მეთოდი უფრო საიმედო ხდება, ვიდრე ზემო აღნიშნული მეთოდი (იხ.2.1 ნახაზი) თუმცა, კომბინირებული მეთოდი, გამომდინარეობს ზემო აღნიშნული მეთოდიდან. არსებული და მიღებული მეთოდთა მახასიათებლები მოცემულია ცხრილის სახით. იხ. ცხრილი 2.1. [4,5,9].

მეთოდთა მახასიათებლები **ცხრ.2.1**

მახასიათებელი	დიფი-ჰელმანის მეთოდი	კვადრატული მატრიცული მეთოდი	მოცულობითი მატრიცული მეთოდი	სიმეტრიული და ასიმეტრიული მეთოდი
გამოყენებული ფუნქცია	ახარისხება	გამრავლება, შეკრება	გამრავლება, შეკრება	გამრავლება, შეკრება
გასაღების სიგრძე ბიტებში	500-ზე მეტი	100-ზე მეტი	100-ზე მეტი	100-ზე მეტი
კრიპტოანალიზის სირთულე	მამრავლებად დაშლა	სიმრავლიდან ამორჩევა	სიმრავლიდან ამორჩევა	სიმრავლიდან ამორჩევა
გასაღების ტიპი	ასიმეტრიული	ასიმეტრიული	ასიმეტრიული	სიმეტრიული და ასიმეტრიული
ჩასატარებელი ოპერაციების რაოდენობა	$p^{1/2}$	$2(n^2+n(n-1))$	$2(n^3+n^2(n^2-1)+$ $+n(n-1))$	$n^3+ 2(n^3+n^2(n^2-$ $1)+n(n-1))$
სიმრავლე	$2^{p/2}$	$2^{n\times n}$	$2^{n\times n\times n}$	$2^{n\times n\times n}$
ალბათობა	$1/2^{p/2}$	$1/2^{n\bullet n}$	$1/2^{n\bullet n\bullet n}$	$1/\left(\sum_{i=2}^{n} 2^i + 2^{n\bullet n\bullet n}\right)$





ნახ. 2.1. p რიცხვისა და n განზომილების დამოკიდებულება ალბათობაზე

3. დასკვნა

დამუშავებულ იქნა ახალი მეთოდები:

1. დიფი-ჰელმანის მეთოდის გამოყენებით მიღებულ იქნა ახალი მეთოდი, ოღონდ დიფი-ჰელმანის ახარისხება შეცვლილი იქნა მოცულობით 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. საწყისი სიდიდის 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. ანუ საიმედოობა მნიშვნელოვნად გაიზარდა.

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 – $M^{m\times n\times k}$. რადგან ვიყენებთ კომუტატიურ-კვადრატულ-მოცულობით მატრიცებს, როცა m=6, k=6 და n=6, მაშინ ათობითში – სიმრავლე იქნება 10^{216}. რეალურ დროში, ამ სიმრავლიდან მატრიცის ამორჩევა არის შეუძლებელი.

მატრიცათა სიმრავლე არის მატრიცათა ველი, ანუ ჩაკეტილი სიმრავლე. ორი მატრიცის გამრავლებით მიიღება ისეთი მესამე მატრიცა, რომელიც მოთავსებულია ამავე მატრიცათა სიმრავლეში. დიფი-ჰელმანის მეთოდში ალბათობა არის $1/2^{p/2}$, კომუტატიური კვადრატული მატრიცის დროს – $1/2^{nn}$, მიღებული მეთოდების შემთხვევაში კი – მოცულობითი კვადრატული კომუტატიური მატრიცის მეთოდში – $1/2^{nnn}$, კომბინირებული მეთოდის დროს კი – $1/2^{nnn}$, ამ სიდიდეს დაემატება იგივე რიცხვის ჯამური სიდიდე, რადგან განზომილებაა უცნობი.

მიღებული ახალი მეთოდები, მიეკუთვნება ასიმეტრიულ სისტემებს და გამოირჩევა მაღალი მედეგობით. კრიპტოსირთულეს წარმოადგენს მოცულობით მატრიცათა სიმრავლიდან ამორჩევის სირთულე, რასაც ემყარება მიღებული მეთოდების საიმედოობა. შეიძლება აღინიშნოს, რომ მიღებული მეთოდების საიმედოობა, გაუტოლდა დიფი-ჰელმანის მეთოდის საიმედოობას.

ლიტერატურა:

1. Тараканов В. Е. Комбинаторные задачи и (0,1) матрицы. М., 1993.
2. Гантмахер Ф.Р. Теория матриц. М., Наука, 1967
3. Анин Б. Зашита компьютерной информации. М., 2000
4. Молдовян А. А., Молдовян Н. А., Гуц Н.Д., Изотов Б. В. Криптография, Скоростные шифры. Ст-Петербург. 2002
5. Ростовцев А. Г., Маховенко Е. Б. Введение в криптографию с открытым ключом - СПБ.: Мир и Семья, 2001
6. Мельников В.В. Защита информации в компьютерных системах. М., Финансы и статистика, Электронинформ, 1997
7. Diffie W. and Hellman M.E. New directions in cryptography. IEEE Trans. Inform. Theory, vol. IT-22, Nov, 1976. pp. 644-654
8. კოტრიკაძე გ. ურთიერთკომუტატიურ მატრიცათა სიმრავლის შექმნა და მისი გამოყენება ინფორმაციის დასაცავად. შტუ-ს შრ.კრებ. "მას"- №1(6), 2009, გვ.58-62
9. კოტრიკაძე გ. ასიმეტრიული მატრიცული მეთოდის სინთეზი სიმეტრიულ მეთოდთან. ინტელექტი, №1(33), 2009., გვ.110-113
10. კოტრიკაძე გ. ინფორმაციის დაცვისათვის სხვადასხვა სახის მატრიცის გამოყენების შედეგები. "ინტელექტი", №1(33), 2009, გვ.113-115.

PROCESSING OF THE METHODS OF CAPACITIVE MATRIX FOR THE INFORMATION PROTECTION, ITS COMPARISON WITH AN ASYMMETRIC METHODS

Kotrikadze Gulnara, Chaduneli Nugzar
Georgian Technical University

Summary

The new matrix methods are developed where both systems are applied: symmetrical and asymmetrical. Received methods have considerably increased rate of keys reception and accordingly rate of enciphering. Mathematical models and algorithms are developed for the above-stated methods.

РАЗРАБОТКА МЕТОДА ЕМКОСТНОЙ МАТРИЦЫ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ И ЕГО СРАВНЕНИЕ С АСИММЕТРИЧНЫМИ МЕТОДАМИ

Котрикадзе Г., Чадунели Н.
Грузинский Технический Университет

Резюме

Разработаны новые матричные методы, в которых применены обе системы: симметричная и асимметричная. Полученные методы значительно увеличивают скорость формирования ключей и, соответственно, скорость шифрации и дешифрации. Разработаны математические модели и алгоритмы для реализации вышеуказанных методов.