ინფორმაციის დაცვის ასიმეტრიული სისტემის ახალი მეთოდის შემუშავება

გულნარა კოტრიკაძე
თბილისის დავით აღმაშენებლის სახ. უნივერსიტეტი

რეზიუმე

განიხილება ინფორმაციის დაცვის ახალი მეთოდი, რომელშიც გამოყენებულია კრიპტოგრაფიის ასიმეტრიული სისტემა, კერძოდ დიფი-ჰელმანის მეთოდი. ამ მეთოდში გამოიყენება ახარისხების ფუნქცია, ჩვენს მიერ შემოთავაზებულში კი - მატრიცაზე გამრავლება. ასეთი მიდგომით გასაღების მისაღებად შედარებით ნაკლები დროა საჭირო, ვიდრე დიფი-ჰელმანის მეთოდით.

საკვანძო სიტყვები: კრიპტოგრაფია. შიფრაცია-დეშიფრაცია. სიმეტრიულ-ასიმეტრიული. კრიპტოანალიზის სირთულე. გასაღების გენერაციის დრო. კომუტატიურობა. საიმედოობა.

1. შესავალი

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 [1,2,4].

საზოგადოდ, კრიპტოგრაფიას შეხება აქვს ინფორმაციის დაცვისა და დასაიდუმლოების მრავალ ასპექტთან, როგორიცაა – ტექსტის შიფრაცია-დეშიფრაცია, დაცვა არასანქციონირებული შეღწევისაგან, ღია ტექსტის ელექტრონული (ციფრული) ხელმოწერა და სხვ. აქედან გამომდინარე, ფართოა მისი გამოყენების არეალი: სამხედრო-სახელმწიფოებრივი დანიშნულებისა და საბანკო-საფინანსო კომერციული სისტემები, ლოკალური და გლობალური კომპიუტერული ქსელები და სხვ., რაც ინფორმატიზაციის თანამედროვე ეპოქაში მის აქტუალობასა და მნიშვნელობას განაპირობებს [3].

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 [3,5].

2. ძირითადი ნაწილი

2.1. ასიმეტრიული სისტემა

- ***დიფი-ჰელმანის ალგორითმი.*** ალგორითმი ეყრდნობა **GF(P)** ველში ლოგარითმების გამოთვლის სირთულეს. გასაღების ღია არხით გაცვლა ხორციელდება შემდეგი სქემით:

X და Y მხარეებს შორის ხდება ინფორმაციის გაცვლა.

გაცხადებულია (ცნობილია) **P** (მარტივი) და **a** (მთელი) რიცხვები **(1<a<P). X** მხარე ირჩევს $\mathbf{x_1}$ საიდუმლო რიცხვს და კავშირის ღია არხით გადასცემს Y მხარეს

$$y_1 \equiv a^{x_1} \bmod P$$

გამოთვლილ მნიშვნელობას. Y-ი შერჩეული $\mathbf{x_2}$ საიდუმლო რიცხვის მეშვეობით აფორმირებს **K** გასაღებს:

$$\mathbf{K = (a^{x_1})^{x_2} \equiv a^{x_1 x_2} \ modP.}$$

თავის მხრივ, Y მხარე X მხარეს ღია არხით გადასცემს

$$y_2 \equiv a^{X_2} \ modP$$ -ის

მნიშვნელობას, ხოლო X-ი აფორმირებს იგივე **K** გასაღებს:

$$\mathbf{K = (a^{x_2})^{x_1} \equiv a^{x_2 x_1} \ modP.}$$

მაშასადამე, ორივე მხარემ მიიღო ერთი და იგივე K გასაღები;

$$\mathbf{K = a^{x_1 x_2} \ modP = a^{x_2 x_1} \ modP.}$$

შიფრაციის მედეგობა (საიმედოობა) ეფუძნება y-ის მიხედვით X_1, X_2 საიდუმლო რიცხვების მიღების სირთულეს [1,5].

2.2. სიმეტრიული და ასიმეტრიული სისტემების მახასიათებლები

1-ელ ცხრილში მოცემულია სიმეტრიული და ასიმეტრიული სისტემების მახასიათებლები.

ცხრ.1.

№	მახასიათებლები	სიმეტრიული	ასიმეტრიული
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

ცხრილში ნათლად ჩანს, სიმეტრიული და ასიმეტრიული სისტემების დადებითი და უარყოფითი მხარეები, რაც მდგომარეობს შემდეგში: სიმეტრიული სისტემის გასაღების სიგრძე მოკლეა, შესაბამისად, მცირე დრო სჭირდება გასაღების გადასინჯვას, თანაც გამოყენებულია გადანაცვლების ფუნქცია, რაც იმას ნიშნავს, რომ გასაღების პოვნა ადვილი შესაძლებელია. ე.ი. სიმეტრიული სისტემა არ არის საიმედო, ადვილად გატეხვადია. ხოლო ასიმეტრიული სისტემის გასაღების სიგრძე გაცილებით მეტია, ვიდრე სიმეტრიული გასაღების სიგრძე, გასაღების ამორჩევისათვის გამოიყენება ახარისხების ფუნქცია, რაც იმას ნიშნავს, რომ საკმაოდ დიდი დროა საჭირო გასაღების პოვნისათვის. ეს მიგვითითებს იმაზე, რომ ასიმეტრიული არის საიმედო და ხასიათდება მაღალი მედეგობით.

რადგან სიმეტრიული სისტემა არ არის საიმედო, ხოლო ასიმეტრიული სისტემა საიმედოა, აქედან გამომდინარე, შევქმენით ახალი მეთოდი, რომელშიც გამოვიყენეთ ასიმეტრიული სისტემა, კერძოდ კი დიფი-ჰელმანის მეთოდი.

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

ინფორმაციის გადაცემა ხდება ღია არხით, გაცხადებულია (ცნობილია) P (მარტივი) რიცხვი ანუ მოდული და e ვექტორი. ცნობილია e ვექტორი, ნიშნავს, რომ ცნობილი ხდება განზომილებაც, ასევე ცნობილია ვექტორში და მატრიცაში შემავალი ელემენტების სიდიდე, რადგან ვიცით P რიცხვი [10].

X მხარე ირჩევს თავის $\mathbf{A_1}$ საიდუმლო მატრიცას და კავშირის ღია არხით გადასცემს **Y** მხარეს გამოთვლილ $\mathbf{y_1}$ მნიშვნელობას

$$\mathbf{y_1} \equiv e \times A_1 \ modP,$$

Y-ი შეარჩევს თავის $\mathbf{A_2}$ საიდუმლო მატრიცას და აფორმირებს **K** გასაღებს:

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

თავის მხრივ **Y** მხარე **X** მხარეს ღია არხით გადასცემს გამოთვლილ $\mathbf{y_2}$ მნიშვნელობას

$$\mathbf{y}_2 \equiv e\times A_2 \,\mathrm{mod}P,$$

ხოლო **X**-ი აფორმირებს **K** გასაღებს:

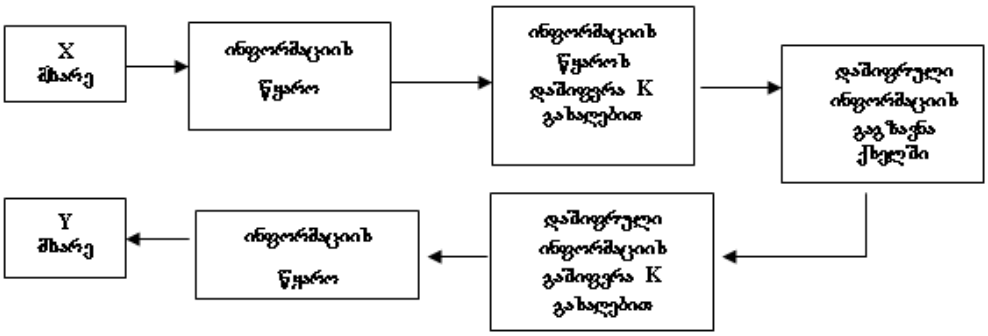
$$\mathbf{K} = (e\times A_2)\times\mathbf{A_1} \equiv e\times A_2\times\mathbf{A_1}\ \mathrm{mod}P.$$

მასასადამე, ორივე მხარემ მიიღო ერთიდაიგივე **K** გასაღები:

$$\mathbf{K = e\times A_1\times A_2\ modP \equiv e\times A_2\times A_1\ modP.}$$

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

შიფრაციის მედეგობა (საიმედოობა) ეფუძნება, A_1 და A_2 საიდუმლო მატრიცების, მატრიცათა სიმრავლიდან ამორჩევის სირთულეს [6,9]. როგორც მეთოდიდან ჩანს, Y მხარე იღებს X-ის მიერ აღებულ საწყის ინფორმაციას, ანუ ახდენს მიღებული დაშიფრული ინფორმაციის გაშიფვრას (ნახ.1).



ნახ.1 ინფორმაციის გაშიფვრა

აქვე უნდა აღვნიშნოთ განხილული მეთოდის მნიშვნელოვანი საკითხი, რაც მდგომარეობს შემდეგში: იმისათვის რომ, ორივე მხარემ, მიიღოს ერთიდაიგივე **K** გასაღები **აუცილებელია და საკმარისი**, ისეთი $\mathbf{A_1}$ და $\mathbf{A_2}$ მატრიცები [7], და საერთოდ, მატრიცათა სიმრავლე, საიდანაც მოხდება ამ მატრიცების ამორჩევა, შედგებოდეს **ურთიერთკომუტატიური** მატრიცებისაგან, რაც იმას ნიშნავს, რომ

$$\mathbf{A_1\times A_2 \equiv A_2\times A_1},$$

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

მაშასადამე, უნდა შეიქმნას კომუტატიურ მატრიცათა სიმრავლე და მხოლოდ მას შემდეგ, **X** და **Y** მხარეები ამ სიმრავლიდან აირჩევენ ნებისმიერ $\mathbf{A_1}$ და $\mathbf{A_2}$ საიდუმლო მატრიცებს და მიიღებენ K გასაღებს.

ე.ი. შიფრაციის **მედეგობა** ეფუძნება $\mathbf{A_1}$ და $\mathbf{A_2}$ 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 მატრიცების ამორჩევა მატრიცათა სიმრავლიდან, რეალურ დროში, რადგან მატრიცების სიმრავლე არის $\mathbf{n^2!}$, სადაც **n** არის მატრიცის განზომილება [8].

3. დასკვნა

შევქმენით ახალი მეთოდი, რომელიც არის მსგავსი ასიმეტრიული სისტემის, დიფი-ჰელმანის მეთოდის, მაგრამ ახარისხება შევცვალეთ მატრიცაზე გამრავლებით, რამაც მოგვცა საიმედო შედეგი. რაც მეტია **e** ვექტორის სიგრძე ანუ შესაბამისად მეტია მატრიცის განზომილებაც, მით ძნელია და საერთოდ შეუძლებელი ხდება ამ მეთოდის გატეხვა. მოდულისა და განზომილების ზრდასთან ერთად, საკმაოდ სწრაფად იზრდება მატრიცათა სიმრავლე. შესაბამისად, მესამე **Z** სუბიექტისათვის, მით უფრო რთულდება და შეუძლებელი ხდება, რეალურ დროში, მოცემული მატრიცათა სიმრავლიდან, იმ ორი კონკრეტული $\mathbf{A_1}$ და $\mathbf{A_2}$ საიდუმლო მატრიცების ამორჩევა.

ახალი მეთოდის მახასიათებლები:

№	მახასიათებლები	ახალი მეთოდი
1.	შიფრაციის სიჩქარე	შედარებით მაღალი
2.	გამოყენებული ფუნქცია	მატრიცაზე გამრავლება
3.	გასაღების სიგრძე	n განზომილება
4.	კრიპტოანალიზის სირთულე	მატრიცათა სიმრავლიდან ამორჩევა
5.	გასაღების გენერაციის დრო	წუთები
6.	გასაღების ტიპი	ასიმეტრიული

ზემოაღნიშნულიდან გამომდინარე, შეიძლება თამამად ვთქვათ, რომ ეს ამოცანა იძლევა ნამდვილად კარგ შედეგს. წარმოდგენილი მეთოდი და შესაბამისად, მასში განხილული ალგორითმი არის საიმედო, მის საიმედოობას უზრუნველყოფს მატრიცათა სიმრავლიდან A_1 და A_2 მატრიცების ამორჩევის სირთულე, P მოდულით.

ე.ი. ამოცანაში აღწერილი, ასიმეტრიული სისტემის ახალი მეთოდი, გამოირჩევა მაღალი მედეგობით.

ლიტერატურა:

1. Schneier B. Appliend cryptography. Jehn Wiley and Sons. Inc. New York. 1996
2. Diffie W., Hellman M. E. New directions in cryptography, IEEE Trans. Inform. Theory, vd, It – 22, pp. 644-654 Nov. 1976
3. Date Encrypticn Standard. National Bureau of standarts (NBS), Federal Information Processing standard (FIPS) Publication nc. 46, Jan, 1977
4. Shanon C.E. Communication Theory of Secrecy Systems. Bell System Technical Journal, v. 28, n. 4, 1973. pp. 656-715
5. Мельников В.В. Зашита информации в компьютерных системах. М., 1997.
6. Гантмахер Ф.Р. Теория матриц. М., 1954.
7. Мишина А.М., Проскуряков М.В. Висшая алгебра. М., 1989.
8. Эндбюс Г. Теория разбиений. М., 1982.
9. Курош А.Г. Курс высшей алгебры. Наука. М., 1967.
10. კოტრიკაძე გ. ინფორმაციის დამუშავებისა და დაცვის, მეთოდური და ალგორითმული საშუალებანი. თდასუ-ს პერ. სამეცნ.ჟურნ. ,,აღმაშენებელი'', №3. თბ., 2007.

TO MAKE A NEW METHOD FOR DETENSE INFORMATION

Gulnara Kotrikadze
Tbilisi David Aghmashenebeli University

Summary

For defense of information, we made a new method. Where we used asymmetrical system of cryptography. Privetly, the method of Dipy-helman, in which is used making the degree function, but in the new method we used multiplication metrix, which needs less time to get the key than Dipy-helman method. Making the degree was changed with multiplication. Rtustworthness of the method establishes to choose A_1 and A_2 metrix from multiplication metrix. Despite of, that the metrix multiplity is known for everybody. Its important to notice that any metrix which is taken from metrix multiplity is intercomutativ toward all ather metrix. And of course, all metrix are quadratic. In ather case, commutative will be desturbe. Choosing A_1 and A_2 metrix for third person is impossibl, because these matrixes multitude make very great number. $n^2!$, where n is space and it is beforehand known for everybody too. The mention method is distingvished with its rtustworthiness, which conditions high stability of the new method.

ВЫРАБОТКА НОВЫХ АСИММЕТРИЧЕСКИХ МЕТОДОВ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Котрикадзе Г.
Тбилисский Университет им. Давида Агмашенебели

Резюме

Для защиты информации создан новый метод, в котором использована асимметричная система криптографии, в частности метод Диф-Гельмана. В методе Диф-Гельмана используется функция возведения в степень, а в предложенном новом методе использовано умножение на матрицу, во время которого для получения ключей нужно значительно меньше времени, чем во время метода Диф-Гельмана, иначе возведение в степень заменяется умножением. Надежность этого метода основывается на выборе сложности матриц, независимо от того, множество матриц известно заранее или нет. Надо отметить, что A_1 и A_2 матрицы коммутативные, или же взятая любая матрица из множества матриц является взаимокоммутативной ко всем другим матрицам и, конечно же, все матрицы являются квадратными, в противном случае коммутативность будет расторгнута. Выбор A_1 и A_2 матриц для третьего лица в определенный срок невозможен, так как множество матриц составляет огромное количество $n^2!$, где n – пространство, которое также известно. Принятый метод выделяется надежностью, что определяет высокую стойкость нового метода.