შებრუნებული მატრიცული მეთოდის დაბალი მედეგობა და მისი გაშიფვრის გზები

გულნარა კოტრიკაძე, ქეთევან ცომაია
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განიხილება კრიპტოგრაფიული სისტემები და მეთოდები. ჩვენი მიზანია მატრიცული მეთოდის „გატეხვა“, ამიტომ ნაშრომში კონკრეტულად მოცემულია შებრუნებული მატრიცის გამოყენებით საწყისი ინფორმაციის დაშიფვრა-დეშიფრაციის პროცესი. აღნიშნული მეთოდის შემთხვევაში, კონკრეტულ მაგალითებზე დაყრდნობით, გამოთვლილია და დადგენილია მატრიცათა სიმრავლე, გატეხვის ალბათობა, მეთოდის დაბალი მედეგობა და გაშიფვრის გზები.

საკვანძო სიტყვები: კრიპტოგრაფია. მატრიცა. განზომილება. საიმედოობა.

1. შესავალი

ინფორმაციის დაცვა-გასაიდუმლოება, არის საკმაოდ აქტუალური საკითხი ყოველდღიურ ცხოვრებაში, სამთავრობო ორგანიზაციებში და ა.შ. ინფორმაციის დაცვა კრიპტოგრაფიის სახელითაა ცნობილი. იგი იყოფა ორ მიმართულებად, რომლებშიც შედის სხვადასხვა მეთოდები თავისი სპეციფიკიდან გამომდინარე და ამ მიმართულებებს ქვია სიმეტრიული და ასიმეტრიული სისტემები [1,2].

სიმეტრიულ სისტემებს მიეკუთვნება ისეთი მეთოდები, სადაც მომხმარებლები გასაღებს არ ითვლიან, არამედ ერთ-ერთი მომხმარებელი ირჩევს კონკრეტულ პარამეტრს გასაღების სახით და საიდუმლოდ უგზავნის მეორე მომხმარებელს, ხოლო ამ გასაღების გამოყენებით დაშიფრული ინფორმაციის გაგზავნა ხდება ღია არხით, დასაშიფრი და გასაშიფრი გასაღები არის ერთიდაიგივე.

ასიმეტრიულ სისტემებში გასაღებს ითვლის მომხმარებლები. ასევე სიმეტრიული სისტემებისაგან განსხვავებით დასაშიფრი და გასაშიფრი გასაღებები არის სხვადასხვა. გასაღების გამოთვლა მიმდინარეობს ღია არხით და დაშიფრული ინფორმაციის გაგზავნა აქაც ხდება ღია არხით [3].

ინფორმაციის გადაცემის დროს, როდესაც უპირატესობას ვანიჭებთ სიჩქარეს ვიდრე საიმედოობას, გამოიყენება სიმეტრიული სისტემის მეთოდები, ხოლო როცა ჩვენთვის უფრო ღირებული ხდება საიმედოობა ვიდრე სიჩქარე, მაშინ გამოიყენება ასიმეტრიული სისტემის მეთოდები [4].

2. ძირითადი ნაწილი

შებრუნებული მატრიცის მეთოდი მიეკუთვნება სიმეტრიულ სისტემებს. კანონიერი მომხმარებლები გასაღებს ანუ ამ შემთხვევაში მატრიცას არ ითვლიან, ირჩევს ერთ–ერთი მომხმარებელი და საიდუმლო გზით აწვდის მეორე მომხმარებელს და ორივე მომხმარებელს შეუძლია საიდუმლო გასაღების ანუ ამ შემთხვევაში, მატრიცის გამოყენებით, გამოთვალოს მისი შებრუნებული მატრიცა, რადგან საწყისი მატრიცა გამოიყენება ინფორმაციის დასაშიფრად და შებრუნებული მატრიცა კი - გასაშიფრად. საწყისი მატრიცის გამრავლება შებრუნებულ მატრიცაზე გვაძლევს ერთეულოვან მატრიცას. ამიტომ შებრუნებული მატრიცა გამოიყენება გასაშიფრად, რადგან დაშიფრული ინფორმაციის მასზე გამრავლებით, გასაღები ანუ საწყისი მატრიცა მოიხსნება და მიიღება საწყისი ინფორმაცია [2,4].

ვთქვათ საწყისი მატრიცა არის A, მისი შებრუნებული A^{-1}. მათი ნამრავლია $A\times A^{-1}=n\times E$, სადაც E არის ერთეულოვანი მატრიცა, ხოლო n არის მატრიცების ნამრავლის შედეგად მიღებული მატრიცის დიაგონალზე მოთავსებული რიცხვი. ვთქვათ m არის საწყისი ინფორმაცია. ინფორმაცია

უნდა დავყოთ ბლოკებად და ბლოკში უნდა შედიოდეს იმდენი ელემენტი, რამდენიც მატრიცის სვეტშია, ნათქვამი ავღნიშნოთ $m_1, m_2, m_3 \dots$.

პირველი მომხმარებელი მიღებულს ამრავლებს A მატრიცაზე, ანუ:

$$m_1 \times A = b_1, \quad m_2 \times A = b_2, \quad m_3 \times A = b_3 \dots .$$

მიღებულ $b_1, b_2, b_3 \dots$ სიდიდეებს უგზავნის მეორე მომხმრებელს ღია არხით. აღნიშნულს მიმღები ამრავლებს A^{-1}-ზე და მიიღებს საწყის ინფორმაციას, ანუ:

$$b_1 \times A^{-1} = n \times m_1, \quad b_2 \times A^{-1} = n \times m_2, \quad b_3 \times A^{-1} = n \times m_3 \dots .$$

განვიხილოთ კონკრეტული მაგალითები.

საწყისი მატრიცა არის $\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 3 & 2 & 1 \end{pmatrix}$, მისი შებრუნებული მატრიცა არის $\begin{pmatrix} 7 & 4 & 5 \\ 12 & -8 & -4 \\ -3 & 4 & 1 \end{pmatrix}$.

მათი ნამრავლის შედეგად მიიღება მატრიცა $\begin{pmatrix} 8 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 8 \end{pmatrix} = 8 \times \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = n \times E$, სადაც n=8.

ინფორმაციის სახით ავიღეთ ქართული ანბანი თანმიმდევრობით და აღნიშნული დავშიფრეთ საწყის მატრიცაზე გამრავლებით. რადგან მატრიცის სვეტი შეიცავს 3 ელემენტს, ამიტომ ინფორმაცია დავყავით ბლოკებად, სადაც თითოეულ ბლოკში შედის 3 ელემენტი და მიღებული სტრიქონული ჩანაწერი თანმიმდევრობით გავამრავლეთ საწყის მატრიცაზე. სულ მივიღეთ 3 ელემენტისაგან შემდგარი 11 ვარიანტი, რაც ქვემოთ არის ნაჩვენები.

$$(1\ 2\ 3) \times \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 3 & 2 & 1 \end{pmatrix} = (10\ 10\ 14) \quad (19\ 20\ 21) \times \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 3 & 2 & 1 \end{pmatrix} = (82\ 100\ 158)$$

$$(4\ 5\ 6) \times \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 3 & 2 & 1 \end{pmatrix} = (20\ 25\ 38) \quad (22\ 23\ 24) \times \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 3 & 2 & 1 \end{pmatrix} = (94\ 115\ 182)$$

$$(7\ 8\ 9) \times \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 3 & 2 & 1 \end{pmatrix} = (34\ 40\ 62) \quad (25\ 26\ 27) \times \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 3 & 2 & 1 \end{pmatrix} = (106\ 130\ 206)$$

$$(10\ 11\ 12) \times \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 3 & 2 & 1 \end{pmatrix} = (46\ 55\ 86) \quad (28\ 29\ 30) \times \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 3 & 2 & 1 \end{pmatrix} = (118\ 145\ 230)$$

$$(13\ 14\ 15) \times \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 3 & 2 & 1 \end{pmatrix} = (58\ 70\ 110) \quad (31\ 32\ 33) \times \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 3 & 2 & 1 \end{pmatrix} = (130\ 160\ 254)$$

$$(16\ 17\ 18) \times \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 3 & 2 & 1 \end{pmatrix} = (70\ 85\ 134)$$

ნამრავლის შედეგი იგზავნება მეორე მომხმარებელთან ღია არხით, ანუ ყველასათვის ხელმისაწვდომია დაშიფრული ინფორმაცია. მიღებულ დაშიფრულ ინფორმაციას მეორე მომხმარებელი, ანუ მიმღები კანონიერი მომხმარებელი, ამრავლებს შებრუნებულ მატრიცაზე და n=8 კოეფიციენტის გამოყენებით იღებს საწყის ინფორმაციას, ანუ ახდენს დეშიფრაციას.

რაც შეეხება მესამე პირს, ანუ არაკანონიერ მომხმარებელს, მას, როგორც ავღნიშნეთ, შეუძლია დაშიფრული ინფორმაციის დანახვა, მაგრამ ავტორის თქმით მეთოდი საიმედოა, ხასიათდება მაღალი მედეგობით და არ ტყდება მარტივად.

თუმცა, ჩვენ დავაკვირდით გამოთვლებს, მიღებულ შედეგებს, რის საფუძველზეც, მივიღეთ შემდეგი:

(10 10 14) განაყოფი (1 2 3) - ზე თანმიმდევრობით გვაძლევს (10, 5, 4(2))
(20 25 38) განაყოფი (4 5 6) - ზე თანმიმდევრობით გვაძლევს (5, 5, 6(2))
(34 40 62) განაყოფი (7 8 9) - ზე თანმიმდევრობით გვაძლევს (4(6), 5, 6(8))
(46 55 86) განაყოფი (10 11 12) - ზე თანმიმდევრობით გვაძლევს (4(6), 5, 7(2))
(58 70 110) განაყოფი (13 14 15) - ზე თანმიმდევრობით გვაძლევს (4(6), 5, 7(5))
(70 85 134) განაყოფი (16 17 18) - ზე თანმიმდევრობით გვაძლევს (4(6), 5, 7(8))
82 100 158) განაყოფი (19 20 21) - ზე თანმიმდევრობით გვაძლევს (4(6), 5, 7(11))
(94 115 182) განაყოფი (22 23 24) - ზე თანმიმდევრობით გვაძლევს (4(6), 5, 7(14))
(106 130 206) განაყოფი (25 26 27) - ზე თანმიმდევრობით გვაძლევს (4(6), 5, 7(17))
(118 145 230) განაყოფი (28 29 30) - ზე თანმიმდევრობით გვაძლევს (4(6), 5, 7(20))
(130 160 254) განაყოფი (31 32 33)- ზე თანმიმდევრობით გვაძლევს (4(6), 5, 7(23))

განაყოფის შედეგებში პირველი და მეორე რიცხვები ერთიდაიგივეა 4(6) და 5, რაც შეეხება მესამე რიცხვს განაყოფი ერთიდაიგივეა და ნაშთი იზრდება 3 ინტერვალით, რადგან მატრიცის განზომილება არის 3-ის ტოლი, რაც გვიჩვენებს გარკვეულ კანონზომიერებას.

გარდა ამისა, მატრიცაში შემავალი პირველი სვეტის ელემენტების ჯამი არის 4 და შესაბამისად, პირველი განაყოფია 4(6). მეორე სვეტის ელემენტების ჯამი არის 5 და განაყოფიც არის 5. მესამე სვეტის ელემენტების ჯამი არის 8 ხოლო, ამ შემთხვევაში, განაყოფი არის 7(2)– დან დაწყებული 3 ინტერვალის ზრდადობით, ჯამში კი - ერთით მეტი.

აღნიშნულ შედეგში, რომ დავრწმუნებულიყავით, რომ ყოველთვის ასეთ შედეგს მივიღებთ, ამისათვის გამოთვლები ჩავატარეთ სხვადასხვა სამგანზომილებიანი მატრიცის გამოყენებითაც, რის საფუძველზეც მივიღეთ ანალოგიური კანონზომიერების მქონე შედეგები, უბრალოდ სხვადასხვა განაყოფების სახით. ასევე ავიღეთ ოთხ, ხუთ და ექვს განზომილებიანი მატრიცებიც, სადაც განაყოფის შედეგებში კანონზომიერება იგივე მიიღება, უბრალოდ სხვადასხვა ციფრების სახით. დავადგინეთ მატრიცის სვეტებში შემავალი ელემენტების ჯამისა და სიმრავლეს შორის დამოკიდებულება (ცხრ.1).

სვეტის რიცხვების ჯამებისა და შესაბამისი სიმრავლის დამოკიდებულება ცხრ.1

ჯამი	1	2	3	4	5	6	7	8	9
სიმრავლე	3	6	10	15	21	28	36	45	55
ჯამი	10	11	12	13	14	15	16	17	18
სიმრავლე	66	78	91	105	120	136	153	171	190
ჯამი	19	20	21	22	23	24	25	26	27
სიმრავლე	210	231	253	276	300	325	351	378	406

მატრიცული მეთოდის საიმედოობა არ არის დაცული, რადგან მეთოდში არის მხოლოდ საიდუმლო გასაღები, რომლის გაცვლის პროცესი მიუღებელია. გარდა ამისა ერთი გასაღები არ არის საკმარისი საიმედოობისათვის. ასევე მეთოდში არ არის გათვალისწინებული მიღებული დაშიფრული ტექსტის ნამდვილობა. მესამე პირმა შესაძლოა აიღოს ნებისმიერი მატრიცა და გაგზავნილი დაშიფრული ინფორმაცია შეცვალოს, მიმღებს კი არა აქვს შემამომწმებელი კოდი, რითაც დაადგენს მიღებულის ნამდვილობას, რაც მეთოდს კიდევ უფრო არასაიმედოს ხდის.

გარდა ამისა, ინფორმაციის მოცულობიდან გამომდინარე ასეთი მატრიცები ხშირად უნდა შეიცვალოს, თან გაცვლა მომხმარებლებს შორის უნდა მოხდეს საიდუმლოდ, ეს კი დღესდღეობით უკვე მიუღებელია და საერთოდ, რეალურ დღევანდელ ცხოვრებაში, სიმეტრიული სისტემის არცერთი მეთოდი აღარ გამოიყენება, რადგან არც ერთი არ გამოირჩევა საიმედოობით, გარდა

ვერნამის მეთოდისა [2]. ინფორმაციის დასაშიფრად უმჯობესია გამოიყენებოდეს, როგორც ღია, ასევე საიდუმლო გასაღები და ნამდვილობის დამადასტურებელი პარამეტრი.

3. დასკვნა

- ზემოაღნიშნული გამოთვლებიდან გამომდინარე, ღიად გაგზავნილი დაშიფრული ინფორმაციიდან, რომელიც შეუძლია ქსელის საშუალებით ჩაიჭიროს მესამე პირმა, შესაძლებელია საწყის ინფორმაციაზე გასვლა. მიღებული დაშიფრული ინფორმაციის თითოეულ რიცხვს ვყოფთ საწყის ინფორმაციაზე და ვიღებთ გარკვეულ კანონზომიერებამდე;

- დაშიფრული ინფორმაცია საწყისზე გაყოფით, გვაძლევს საინტერესო შედეგს. მიღებული პასუხები თანმიმდევრობით, ერთი და იგივე ინტერვალით იზრდება;

- ასევე მიღებული დაშიფრული ინფორმაციიდან დავადგინეთ, საწყის მატრიცაში შემავალი ელემეტების ჯამი სვეტების მიხედვით და გამოვთვალეთ ასეთი მატრიცების ყველა შესაძლო ვარიანტების რაოდენობა ანუ სიმრავლე.

ლიტერატურა:

1. კუციავა ვ., კაცაძე გ., დიაკონიძე ქ. (2005). ინფორმაციის დაცვა. სტუ, „ტექნიკური უნივერსიტეტი"

2. მეგრელიშვილი რ. (2009). ინფორმაციის დაცვის სისტემები, თსუ.

3. Касами Т., Токура Н., Ивадари Е., Инагаки Я. (1978). Теория кодирования. М., "Мир"

4. Питерсон У., Уэлдон, Э. Коды, исправляющие ошибки. "Мир" 1976. I-IIтом.

5. ყიფშიძე ზ., ანანიაშვილი გ. (2003). ინფორმაციის თეორია, კოდირება და სინერგეტიკა, თსუ.

LAW ENDURANCE OF INVERSE MATRIX METHOD AND IT'S DECODING WAYS

Kotrikadze Gulnara, Tsomaia Ketevan

Georgian Technical University

Summary

The thesis describes Cryptography in general with its systems and methods. Taking into consideration that our goal was to break the matrix method, the work specifically provides the encryption-decryption process of the initial information using the inverse matrix. According to this case and based on the specific examples, we calculated and determined the set of matrix, breaking probability, low resistance of the method and decoding ways.

НИЗКОЕ СОПРОТИВЛЕНИЕ МЕТОДА ОБРАТНОЙ МАТРИЦЫ И ПУТИ ЕГО ДЕКОДИРОВАНИЯ

Котрикадзе Г., Цомаиа К.

Грузинский Технический Университет

Резюме

Описываются общие методы криптографии и рассматривается процесс шифрации-дешифрации исходной информации с использованием обратной матрицы. На конкретном примере вычислены множества матриц, вероятность взлома и пути декодирования.