# კრიპტოგრაფიისა და კრიპტოანალიზის მართვის ავტომატიზებული სისტემა

თამაზ შეროზია, ოთარ შონია, კორნელი ოდიშარია, ირაკლი ტურაშვილი
საქართველოს ტექნიკური უნივერსიტეტი

## რეზიუმე

განხილულია კრიპტოგრაფიისა და კრიპტოანალიზის საკითხები. წარმოდგენილია შესაბამისი სამსახურების ორგანიზაციული მართვის სისტემა და მის ბაზაზე აგებული მართვის ავტომატიზებული სისტემა. ჩამოყალიბებულია ფუნქციები, რომელთა ავტომატიზაციაც ხორციელდება. შიფრაცია-დეშიფრაციის ერთ-ერთი მეთოდის მაგალითზე. მოცემულია კრიპტოგრაფიისა და კრიპტოანალიზის ალგორითმები და ბლოკ-სქემები.

**საკვანძო სიტყვები:** კრიპტოგრაფია. კრიპტოანალიზი. ავტომატიზებული სისტემები. შიფრაციისა და დეშიფრაციის მეთოდები. დეშიფრაცია უცნობი გასაღებით.

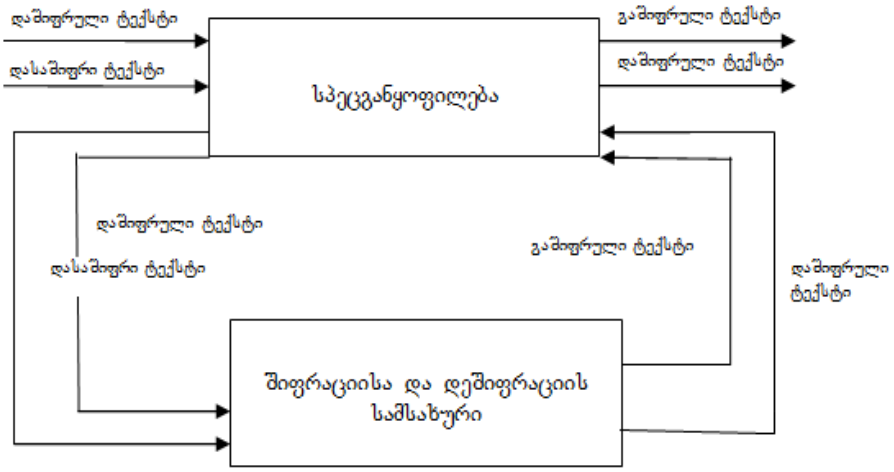
## 1. შესავალი

კრიპტოგრაფიას (კრიპტო-საიდუმლო, გრაფია-წერა), ანუ წერილების გასაიდუმლოების ხელოვნებას, მრავალსაუკუნოვანი ისტორია გააჩნია. იგი ფართოდ გამოიყენებოდა სახელმწიფო, სამხედრო, თუ სხვა საქმიანობაში. მათ იყენებდნენ აგრეთვე კომერციული პირები და ორგანიზაციები.

არ არსებობს ადამიანთა მოღვაწეობის არც ერთი სფერო (მათ შორის საყოფაცხოვრებოც), სადაც დღეს-დღეობით ფართოდ არ ინერგებოდეს კრიპტოგრაფია. თანამედროვე ცხოვრებაში ფართოდ შემოიჭრა და გამოიყენება ისეთი ტერმინები, როგორიცაა, „შიფრი", „გასაღები", „შიფრაცია", „დეშიფრაცია," „კოდი", „კრიპტოგრამა" და სხვა. კრიპტოგრაფია ესაა შიფრების შემუშავება, ხოლო კრიპტოანალიზი ამ შიფრების გახსნაა. დაინტერესებული პირები ცდილობენ იპოვონ გასაღები და მოახდინონ შიფრების გახსნა, ამიტომ ცხადია რომ შიფრები უნდა იყოს მდგრადი და ადვილად არ ექვემდებარებოდეს გახსნას. თანამედროვე კრიპტოგრაფია დაფუძნებულია შიფრებზე „ღია გასაღებით", „ელექტრონულ ხელმოწერაზე" და სხვა.

## 2. ძირითადი ნაწილი

ორგანიზაციულ მართვის სისტემებში, საჭიროების შემთხვევაში, არსებობს ტექსტების (წერილების, დოკუმენტების, შეტყობინებათა) შიფრაციისა და დეშიფრაციის სამსახურები (ნახ.1), რომლებიც ექვემდებარება სპეციალურ განყოფილებას.




ნახ. 1

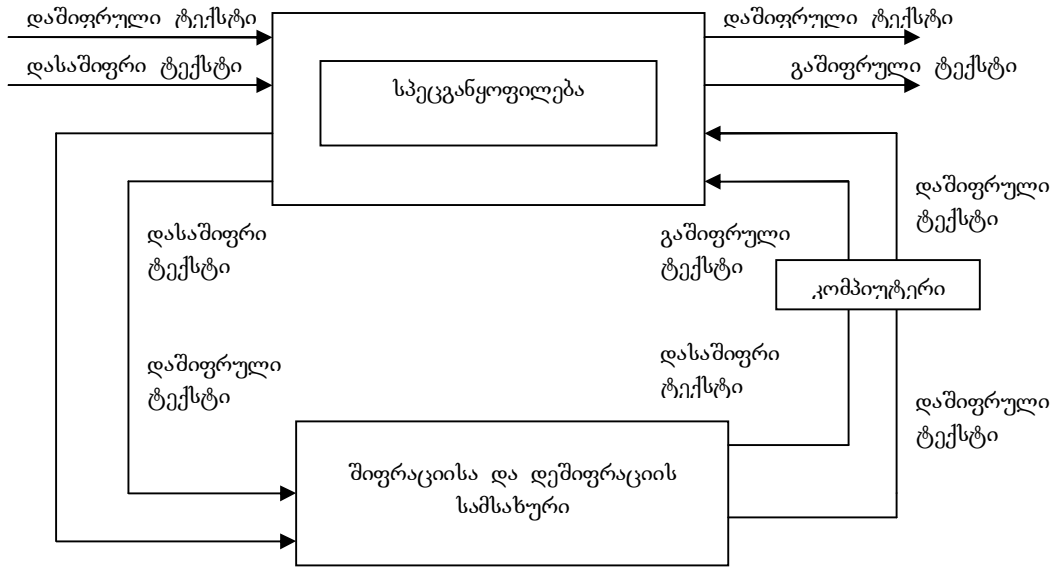
სპეცგანყოფილება მართვის სისტემის სხვადასხვა დანაყოფებიდან, ღებულობს დაშიფრულ წერილებს და გაშიფრვისათვის გადასცემს მათ შიფრაციისა და დეშიფრაციის სამსახურს. ამასთანავე, აგრეთვე ადგენს წერილებს და გადასცემს აღნიშნულ სამსახურს დაშიფრვისათვის. სამსახური ახდენს მიღებული წერილების შესაბამისად შიფრაციას, ან დეშიფრაციას და გადასცემს სპეც განყოფილებას. იგი, თავის მხრივ აანალიზებს მიღებულ წერილებს და გადასცემს მათ სისტემის სხვა დანაყოფებს.

თანამედროვე ინფორმაციულმა ტექნოლოგიებმა მოგვცა შესაძლებლობა გაგვეხორციელებინა ავტომატიზებული მართვა და აგვეგო შესაბამისი მართვის ავტომატიზებული სისტემა (ნახ.2), რომელშიც შიფრაციისა და დეშიფრაციის.

პროცესების გადაწყვეტა ხორციელდება კომპიუტერზე, სპეციალურად შემუშავებული პროგრამების საშუალებით.

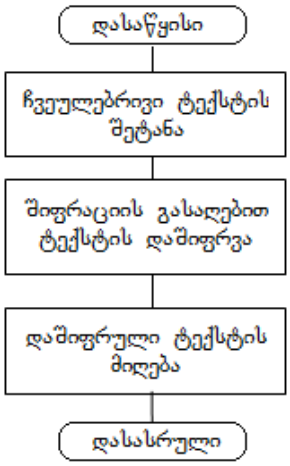
ასეთ სისტემებში შეიძლება გამოვყოთ ის ძირითადი ფუნქციები, რომელთა ავტომატიზაციაც არის შესაძლებელი:

1. ნორმალური ტექსტის შეტანა და ცნობილი გასაღებით მისი შიფრაცია;
2. დაშიფრული ტექსტის შეტანა და ცნობილი გასაღებით მისი დეშიფრაცია;
3. დაშიფრული ტექსტის შეტანა, შიფრაციის გასაღების პოვნა (თუ გასაღები უცნობია) და საწყისი ტექსტის აღდგენა.




ნახ.2

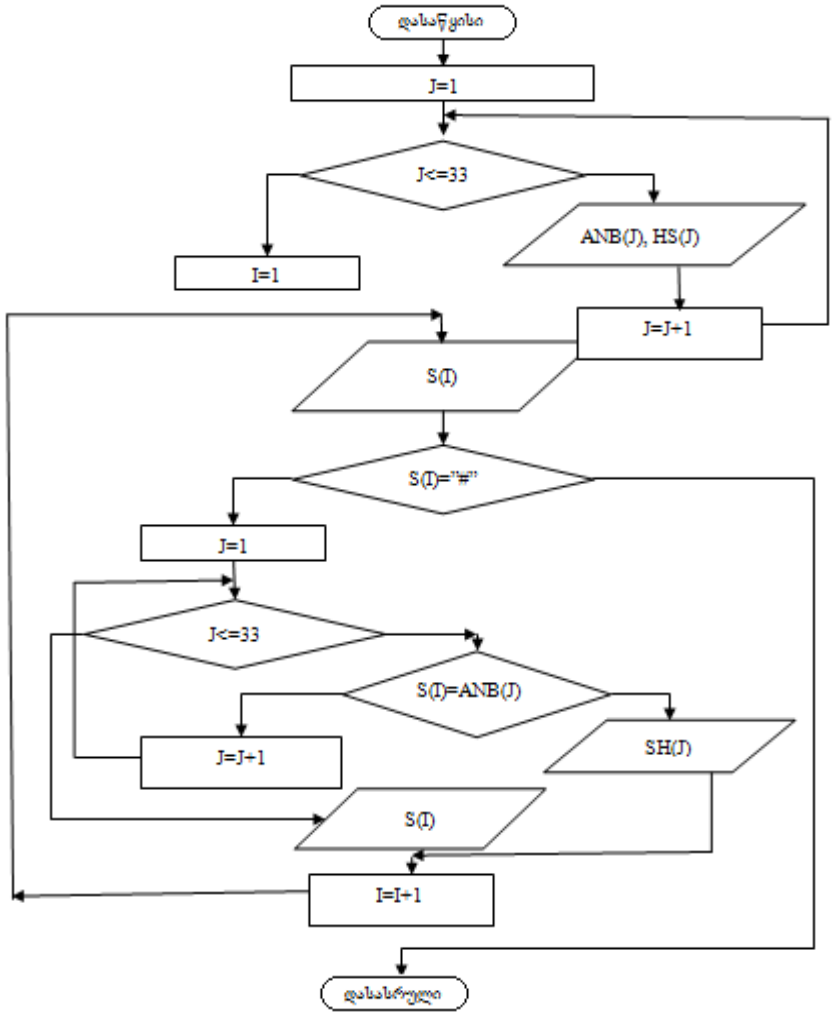
საიდუმლო წერილების შედგენის ტექნიკა დროთა განმავლობაში იხვეწებოდა-იქმნებოდა მათი გასაიდუმლოების სხვადასხვა მეთოდები და საშალებები. წერილების გასაიდუმლოება (ანუ შიფრაცია) და დაშიფრული ტექსტის აღდგენა (ანუ დეშიფრაცია) ხდებოდა შესაბამისი გასაღების საშუალებით. თუ გასაღები ცნობილია, ადვილად ხორციელდება, როგორც ტექსტის დაშიფრვა ასევე მისი გაშიფრვა. მაგრამ, თუ გასაღები უცნობია, მაშინ შიფრაციის (დეშიფრაციის) გასაღების მოძებნა გარკვეული ლოგიკური და ანალიზური პროცესების ჩატარებასთანაა დაკავშირებული. ამიტომ მოწინააღმდეგე, დაინტერესებული მხარე ცდილობდა ხელში ჩაეგდო გასაიდუმლოებული წერილები, სხვადასხვა მეთოდებით ეპოვნა გასაღები და მოეხდინა მათი პირვანდელი სახით აღდგენა.




ნახ.3

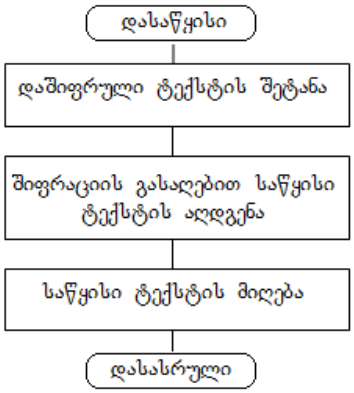
საიდუმლო წერილების შედგენის ერთ-ერთი მეთოდი ესაა ე.წ. „შენაცვლების" მეთოდი და მდგომარეობს იმაში რომ ტექსტში არსებულ ასოებს, გარკვეული შესაბამისობით (გასაღებით) შეანაცვლებენ იგივე ანბანის ასოებოთ (მაგალითად ასო „ა"-ს მაგივრად ასო „რ", „ბ"-ს მაგივრად-„ლ", „გ"-ს მაგივრად-„ქ" და ა.შ.) რის შედეგადაც საწყისი, დაშიფრული ტექსტი აზრს კარგავდა.

შიფრაციის პროცესების ალგორითმი, როდესაც გასაღები ცნობილია, შეიძლება წარმოვადგინოთ მე-3 ნახაზზე. მისი ალგორითმული ბლოკ-სქემა კი გამოსახულია მე-4 ნახაზზე.




ნახ.4

როგორც ალგორითმით ჩანს, ხდება დასაშიფრი ტექსტის (ვიგულისხმოთ, რომ იგი ქართული ანბანითაა შედგენილი) თითოეული სიმბოლოს S(I) წაკითხვა და შემოწმება, თუ რა სიმბოლოა იგი. თუ სიმბოლო ასოა, შიფრაციის გასაღებით მივიღებთ (იბეჭდება) მის შესაბამის სიმბოლოს (შიფრს), წინააღმდეგ შემთხვევაში იბეჭდება წაკითხული სიმბოლო (მაგ. „.", „.", „!", " ", "?", და სხვა). ტექსტის დასასრული აღნიშნულია „#" სიმბოლოთი. საბოლოოდ მივიღებთ დაშიფრულ ტექსტს.




ნახ.5

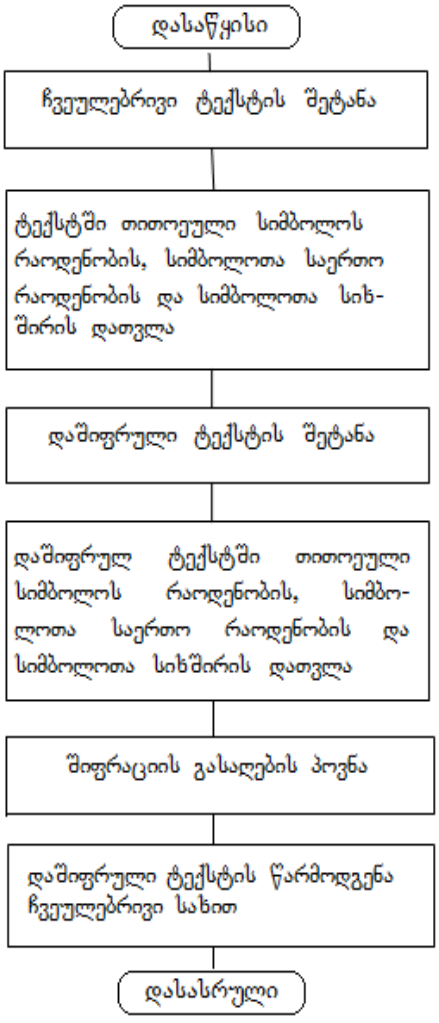
ტექსტის დეშიფრაცია, როდესაც გასაღები ცნობილია შეიძლება გამოვსახოთ პროცესების ალგორითმით (ნახ.5).

რაც შეეხება დეშიფრაციის ალგორითმის ბლოკ-სქემას, იგი ანალოგიურია მე-4 ნახაზზე წარმოდგენილი სქემისა, ოღონდ ასოების შესაბამისობა დგინდება უკვე დეშიფრაციის გასაღებით (უკუ-მიმართულებით, რომელ შიფრს რომელი ასო შეესაბამება).

თუ შიფრაციის გასაღები უცნობია, ასეთი მეთოდით დაშიფრული ტექსტის აღდგენა გარკვეულ კანონზომიერებასთანაა დაკავშირებული.

დადგენილია, რომ თითქმის ნებისმიერ ენაზე დაწერილ ტექსტში, ენის ანბანის თითოელი ასოს სიხშირე (ტექსტში ასოს რაოდენობის ფარდობა, ასოების საერთო რაოდენობასთან ტექსტში), თითქმის ერთი და იგივეა (მუდმივია), და რაც უფრო მეტი ასოა ტექსტში, მით უფრო ზუსტია ეს რიცხვი. ამიტომ, თუ დაშიფრულ ტექსტში დავითვლით თითოეული ასოს სიხშირეს და მას შევცვლით ჩვეულებრივი ტექსტის იგივე სიხშირის ასოთი, ამით ვიპოვნით შიფრაციის გასაღებს და შევძლებთ დაშიფრული ტექსტის გაშიფრვას.

დეშიფრაციის პროცესების თანამიმდევრობა, როდესაც გასაღები უცნობია, წარმოდგენილია მე-6 ნახაზზე.

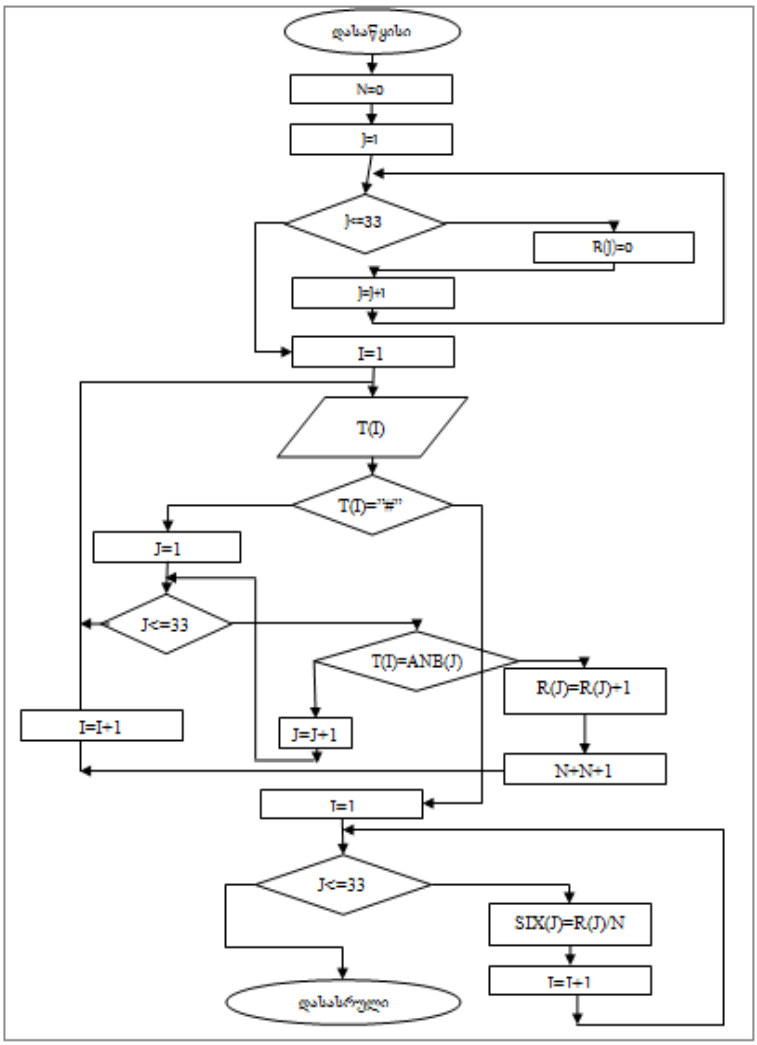



ნახ.6

როდესაც ანბანის თითოეული ასოს სიხშირე ცნობილია, იგი შეიძლება უშუალოდ გამოვიყენოთ. წინააღმდეგ შემთხვევაში ისინი უნდა გამოვთვალოთ. ამისათვით უნდა ავიღოთ ნებისმიერი ტექსტი და მასში განვსაზღვროთ თითოეული ასოს სიხშირე. მე-7 ნახაზზე წარმოდგენილია ქართული ტექსტისათვის, ამ სიხშირეების დათვლის ალგორითმის ბლოკ-სქემა. ბლოკ-სქემაზე ცვლადებს აქვს შემდეგი დანიშნულება: T(I)-შეტანილი ტექსტის სიმბოლოები (I=1,2,3,…). R(J)- ტექსტში ანბანის J-ური ასოს რაოდენობა (J=1,2,3,…33). ANB(J)-ქართული ანბანის J–ური სიმბოლო (პირველი სიმბოლო „ა”, მეორე სიმბოლო „ბ”, და ა.შ.). SIX(J)-ტექსტში J-ური ასოს სიხშირე. N-ასოების საერთო რაოდენობა. `#”- Setanili ტექსტის ბოლო სიმბოლო.

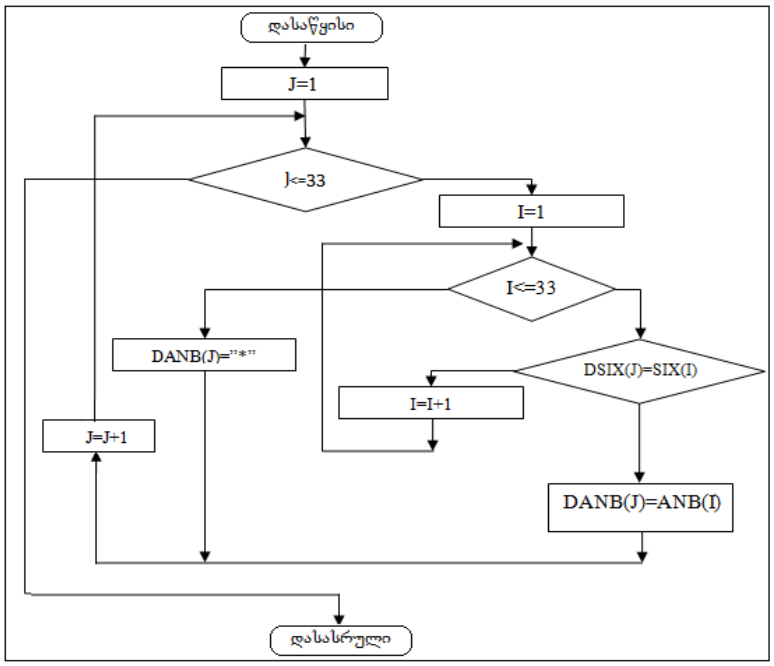
დეშიფრაციის შემდეგი ამოცანაა (ნახ.6) დაშიფრულ ტექსტში თითოეული ასოს სიხშირის დათვლა. მისი ალგორითმი ანალოგიური იქნება მე-7 ნახაზზე წარმოდგენილი ალგორითმისა, რის შედეგადაც მივიღებთ დაშიფრულ ტექსტში თითოეული ასოს სიხშირეს. აღვნიშნოთ იგი DSIX(J), სადაც J-1,2,3,…33 (J=1 შეესაბამება ანბანის პირველ ასოს `a~, J=2 მეორე ასოს „ბ” და ა.შ.).

შიფრაციის გასაღების, ანუ ასოების შესაბამისობის დადგენა ხორციელდება მიღებული ასოების სიხშირის (DSIX(J)) შედარებით ჩვეულებრივი ტექსტის ასოების სიხშირესთან (SIX(I), სადაც I=1,2,3,…33, J=1,2,3,…33), და მათი ტოლობის შემთხვევაში მივიღებთ დაშიფრული ტექსტის ანბანს DANB(J) (J=1,2,3,…33), რომლის DANB(1) იქნება ის ასო, რომლის სიხშირე DSIX(1) დაემთხვევა SIX(I)-s. ანალოგიურად DAN(2) იქნება ის ასო, რომლის სიხშირე DSIX(2) დაემთხვევა SIX(I)-s, და ა.შ. ანალოგიურად მივიღებთ დანარჩენ ასოებსაც.

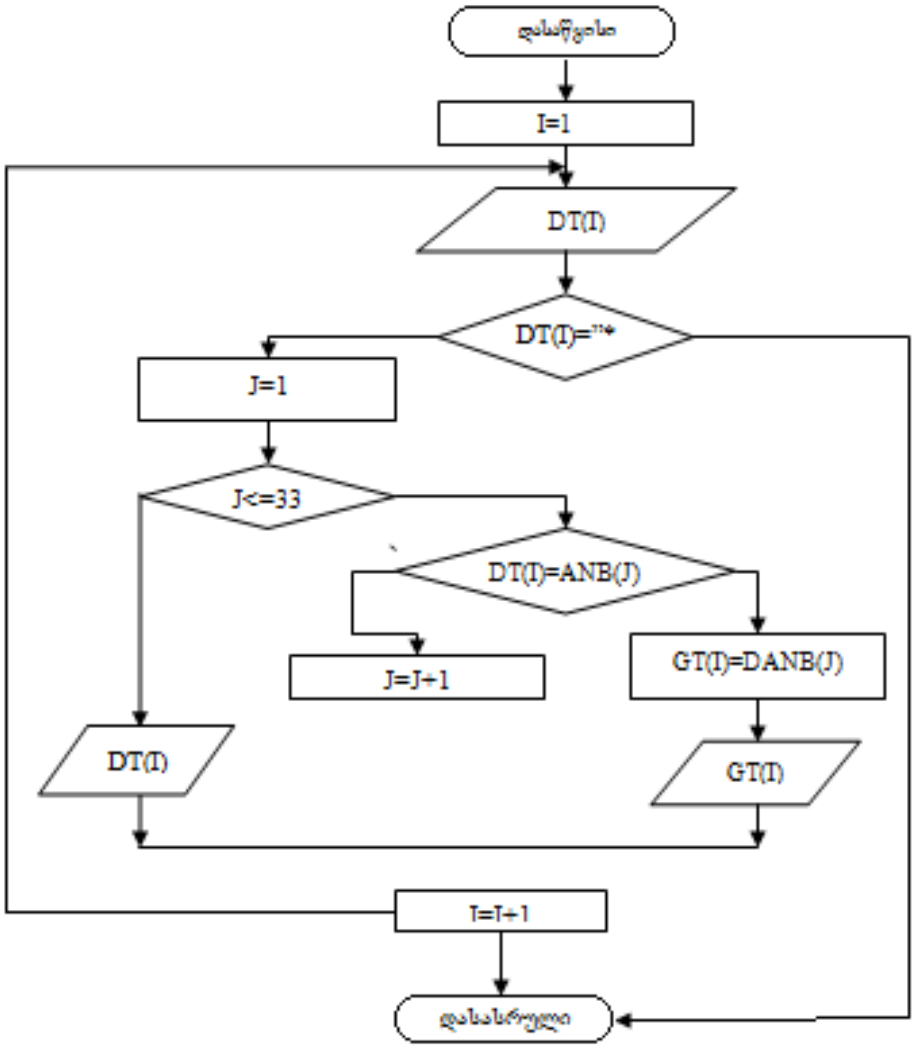



ნახ.7

თუ DSIX(J) არ დაემთხვევა არც ერთ SIX(I)-ს, მაშინ DSIX(J)–ის შესაბამის ასოს მივანიჭებთ „*” სიმბოლოს. შესაბამისი ალგორითმის ბლოკ-სქემას ექნება სახე (ნახ.8).




ნახ.8




ნახ.9

ტექსტის ნორმალური სახით წარმოსადგენად, დაშიფრული ტექსტის თითოეულ სიმბოლოს DT(I), დაწყებული პირველიდან, ვადარებთ ჩვეულებრივი ანბანის ასოებს- „ა", „ბ",..., „ჰ" და მათი დამთხვევის შემთხვევაში მივიღებთ გაშიფრული ტექსტის შესაბამის ასოს GT(I)=DANB(J) (J=1,2,3,…33), წინააღმდეგ შემთხვევაში სიმბოლო (მაგალითად, „ . ", „ , ", „?"„ !" და ა.შ.) რჩება უცვლელი. საბოლოოდ მივიღებთ გაშიფრულ ტექსტს. ალგორითმის ბლოკ-სქემას ექნება სახე (ნახ. 9).

ამ მარტივი მაგალითიდანაც კი ნათლად ჩანს, რომ შიფრაციისა და დეშიფრაციის საკითხების გადაწყვეტა, საკმაოდ რთული და შრომატევადი სამუშაოა, რომ აღარაფერი ვთქვათკრიპტოგრაფიისა და კრიპტოანალიზის თანამედროვე მეთოდებზე. მათი კვლევა კი, ალბათ ცალკე განსჯის საგანია.

## 3. დასკვნა

ამ მაგალითიდან ნათლად ჩანს, რომ შიფრაციისა და დეშიფრაციის მარტივი საკითხების გადაწყვეტა, მართვის ავტომატიზებული სისტემების პირობებშიც კი, საკმაოდ რთული და შრომატევადი სამუშაოა, რომ აღარაფერი ვთქვათ კრიპტოგრაფიისა და კრიპტოანალიზის თანამედროვე მეთოდებზე. მათი კვლევა კი, ალბათ ცალკე განსჯის საგანია.

**ლიტერატურა:**

1. შონია ო., შეროზია თ. ინფორმაციული ტექნოლოგიები და უსაფრთხოება. სტუ, თბ., 2010
2. Ван Тилборг Х.К.А. Основы криртологии. М., Мир. 2006
3. Ященко И. В . Введение в криптографию. М., ЧеРо. 1999
4. Аграновский А. В. Хади Р. А .Практическая криптография. Алгоритмы и их програмирование. М., Солон-Р. 2002
5. Смарт Н. Криптография. М., 2005.

## THE AUTOMATED CONTROL SYSTEM OF CRYPTOGRAPHY AND CRYPTANALYSIS

Sherozia Tamaz, Shonia Otar, Odisharia Korneli, Turashvili Irakli
Georgian Technical University

**Summary**

This article examines cryptography and cryptanalysis. The system of organizational administration and the system of the automated management of the services based on the previous system are represented. The automated functions are formed. On the basis of the method sample, the algorithms and block-schemes of references and dereferences documents are being developed.

## АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ КРИПТОГРАФИЕЙ И КРИПТОАНАЛИЗОМ

Шерозия Т., Шония О., Одишария К., Турашвили И.
Грузинский Технический Университет

**Резюме**

Рассмотрены вопросы криптографии и криптоанализа. Представлена система организационного управления и построенная на ее базе система автоматизированного управления соответсвующих служб. Сформированы автоматизированные функции. На примере одного из методов разработаны алгоритмы и блок-схемы шифрации и дешифрации засекреченных документов.