კრიპტოგრაფიის სიმეტრიული სისტემის უნივერსალური მოდელის შესახებ

ვალერიან კეკელია
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

კრიპტოგრაფიის სიმეტრიული სისტემის ცეზარის, ვიჟინერის და ვერნამის მეთოდების ბაზაზე დამუშავებულია ტექსტური ინფორმაციის დაშიფვრა/გაშიფვრის უნივერსალური მოდელი, აგრეთვე ამ მოდელის მარეალიზებელი ალგორითმი და ფუნქციონირებადი Microsoft Visual Studio .NET გარემოში პროგრამული მოდულები შემუშავებული დაპროგრამების ობიექტ-ორიენტირებულ ენაზე - C#, რაც პიროვნებებს მიცემს საშუალებას გაცვალონ ერთმანეთში მოკლეტექსტური შეტყობინებები ანუ ისაუბრონ „კრიპტოგრაფიის ენაზე".

საკვანძო სიტყვები: კრიპტოგრაფია. საწყისი ტექსტური ინფორმაცია. შიფროტექსტი. საიდუმლო გასაღები. პროგრამული მოდული.

1. შესავალი

ცნობილია, რომ გამოთვლით სისტემებში ინფორმაციის დაცვის (საიდუმლოებისა და მთლიანობის ანუ ნამდვილობის) უზრუნველყოფის მიმართულება მეცნიერებაში დამკვიდრდა „კრიპტოგრაფიის" სახელწოდებით [1,2]. პრაქტიკაში განიხილავენ კრიპტოგრაფიული სისტემების ორ ძირითად ჯგუფს: სიმეტრიულ და ასიმეტრიულ სისტემებს. სიმეტრიულ სისტემებს მიეკუთვნება ისეთი მეთოდები (კერძოდ, ცეზარის, ვიჟინერის და ვერნამის), რომელთა მიხედვითაც ტექსტური ინფორმაციის - TI დაშიფვრა/გაშიფვრა ხორციელდება ერთი ან რამდენიმე სიმბოლოს (ე.წ. დამშიფრავი სიმბოლო(ები)ს გამოყენებით. მას უწოდებენ აგრეთვე, დაშიფვრის დახურულ ან საიდუმლო გასაღებს. აღნიშნულიდან გამომდინარეობს, რომ სიმეტრიულ სისტემებში გამოიყენება ერთიდაიგივე გასაღები, ინფორმაციის როგორც დასაშიფრად, ასევე მის გასაშიფრადაც.

ცნობილია აგრეთვე, რომ კრიპტოგრაფიის (როგორც სიმეტრიული, ასევე ასიმეტრიული სისტემების) მეთოდები ძირითადად დაფუძნებულია ერთიდაიმავე პრინციპზე, რომლის ძირითადი არსი მდგომარეობს ტექსტურ ინფორმაციაში შემავალ სიმბოლოებზე წინასწარ განსაზღვრული მათემატიკური და ლოგიკური მანიპულაციების განხორციელებაში. განიხილავენ TI წარმოდგენის სამ სახეს [2]:

ა) დასაშიფრი TI ანუ საწყისი TI – STI ;

ბ) დაშიფრული TI – ShifTI (შიფროტექსტი);

გ) TI-ის დამშიფრავი (გამშიფრავი) დახურული (საიდუმლო) გასაღები - DamTI.

შევნიშნოთ, რომ სამივე სახის TI წარმოადგენს პკ კლავიატურიდან შეტანილი სიმბოლოების ნაკრებისაგან ფორმირებულ სტრიქონს, კერძოდ:

$STI = \{S_0\ S_1\ S_2 \ldots S_m\}$,

$ShifTI = \{D_0\ D_1\ D_2 \ldots Dm\}$,

$DamTI = \{K_0\ K_1\ K_2 \ldots Kn\}$,

სადაც, m+1 და n+1 - აღნიშნავს აღწერილ სტრიქონში შემავალი სიმბოლოების რაოდენობას ანუ მოცემული სტრიქონის სიგრძეს, ($n <= m$).

2. ძირითადი ნაწილი

მოცემულ ნაშრომში შემოთავაზებულია TI დაშიფვრა/გაშიფვრის უნივერსალური მოდელი (დამუშავებული ცეზარის, ვიჟინერის და ვერნამის მეთოდების ბაზაზე) და ამ მოდელის მარეალიზებელი ალგორითმის პროგრამული მოდული (პროგრამა - დანართი (Application)), შემუშავებული დაპროგრამების ობიექტ-ორიენტირებულ ენაზე - C# და ფუნქციონირებადი Microsoft Visual Studio .NET გარემოში [3,4], რომელიც იძლევა საშუალებას განხორციელდეს დიალოგი მოსაუბრე პიროვნებებს შორის ,,კრიპტოგრაფიის ენაზე". ამასთან იგულისხმება, რომ დაშიფვრა და გაშიფვრის ალგორითმებში, გამოყენებულია არა მარტო ინგლისური ენის – en (ლათინური ალფაბეტი), არამედ ქართული - ka და რუსული - ru ენების ფონტების შემცველი სიმბოლოების ნაკრებები და მათი შესაბამისი რიცხვითი კოდების მნიშვნელობები, რომლებიც ფიქსირდება კომპიუტერში პროგრამის Microsoft Visual studio 2010 (Default პრინციპით) ინსტალირების შედეგად.

აღვწეროთ ორ მოსაუბრე პიროვნებას, ვთქვათ, ხოსრიკასა და ანას შორის, ტექსტური ინფორმაციის გაცვლის პროცედურები და მათი მარეალიზებელ პროგრამებთან (რომლების საწყისი ტექსტების ძირითადი ნაწილი ნაჩვენებია დანართში 1-დაშიფვრის, ხოლო დანართში-2 გაშიფვრის) მუშაობის წესები. დაუშვათ, რომ ანამ და ხოსრიკამ გადაწყვიტეს ისაუბრონ ,,კრიპტოგრაფიის ენაზე" (ნახ.1).

ნახ.1

დაუშვათ ისიც, რომ ანა არის ინფორმაციის მიმწოდებელი, ხოლო ხოსრიკა მიმღები, რომელმაც უნდა გაშიფროს ანას მიერ გამოგზავნილი შიფროტექსტი. აღნიშნულიდან გამომდინარე, მოსაუბრე პირები:

ა) თავთავიანთი კომპიუტერების ვინჩესტერ-ებზე ქმნიან საქაღალდეს სახელით: D:\VisaubroT_Kriptografiis Enaze;

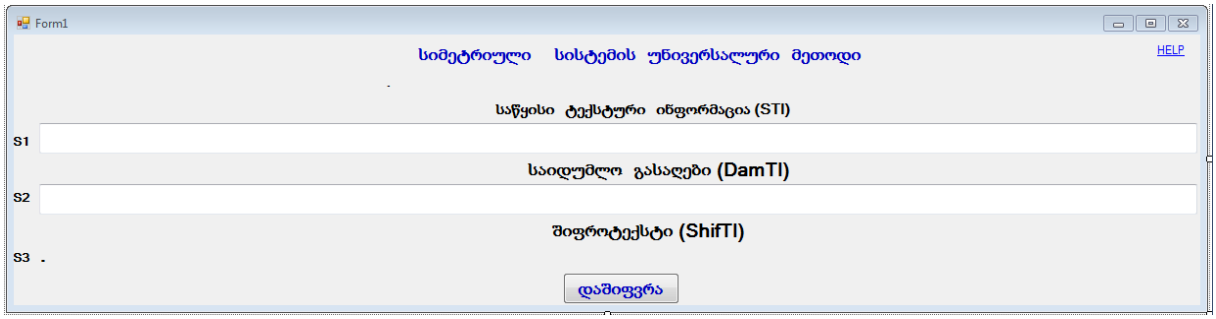
ბ) ირჩევენ საიდუმლო (STI-ის დამშიფრავ / გამშიფრავ) გასაღებს (DamTI),

გ) ქმნიან პროგრამულ მოდულებს (შესაბამისად, ანა მოდულს - TIDasifvra დანართ 1, ხოლო ხოსრიკა მოდულს - TIGasifvra დანართ 2 მოცემული საწყისი ტექსტების მიხედვით) და უზრუნველყოფენ მათ ფუნქციონირებას Microsoft Visual Studio .NET გარემოში.

ანა შეასრულებს რა აღწერილ პუნქტებს, ჩატვირთავს (გაუშვებს) შექმნილ პროგრამს. ეკრანზე აისახება დიალოგური ფანჯარა - ფორმა (ნახ.2).

ა) ამზადებს ხოსრიკასთან გასაგზავნ STI და შეაქვს იგი ფორმაში მითითებულ S1 სტრიქონში (შევნიშნოთ, რომ STI-ის სტრიქონის სიგრძე შეზღუდულია ანუ მასში შემავალი სიმბოლოების რაოდენობა არ უნდა აღემატებოდეს დაახლოებით 120 სიმბოლოს (m <= 120), რაზედაც მიუთითებს ზემოთ აღნიშნული სიტყვა - ,,მოკლეტექსტური"),

ბ) შეიტანს ფორმაში მითითებულ S2 სტრიქონში ხოსრიკასთან შეთანხმებით არჩეულ (STI–ის დამშიფრავ) საიდუმლო გასაღებს ანუ ამ გასაღების შემცველ სიმბოლოებს (ვთქვათ, DamTI -> ანა_GioPrИЙ);



ნახ.2

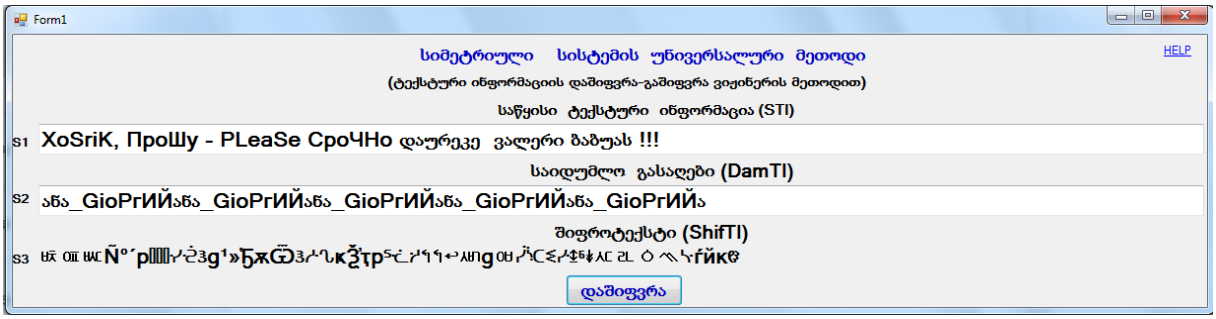
გ) დააწკაპუნებს ღილაკზე „დაშიფვრა“. შედეგად :

- ფორმირდება დამშიფრავი სტრიქონი [1,2];

- სრულდება შეტანილი STI–ის დაშიფვრა (შიფროტექსტის ფორმირება - ნახ.3);

- საქაღალდეში D:\VisaubroT_Kriptografiis Enaze, ფორმირდება ფაილი სახელით ShifTI.txt, რომელიც შეიცავს დაშიფრულ ტექსტურ ინფორმაციას Notepad ტექსტური რედაქტორის ფორმატში;

დ) ელექტრონული ფოსტით უგზავნის (ან სხვა საშუალებებით გადასცემს) ხოსრიკას შიფროტექსტის შემცველ ფაილის - ShifTI.txt.



ნახ.3

ხოსრიკა შეასრულებს რა ზემოთ აღწერილ ა)- ბ) პუნქტებს:

ა) შეიტანს ანასაგან გამოგზავნილ ფაილს - ShifTI.txt საქაღალდეში D:\VisaubroT_Kriptografiis Enaze;

ბ) ჩატვირთავს (გაუშვებს) საშემსრულებლო პროგრამას. შედეგად ეკრანზე აისახება დიალოგური ფანჯარა - ფორმა (ნახ.4);

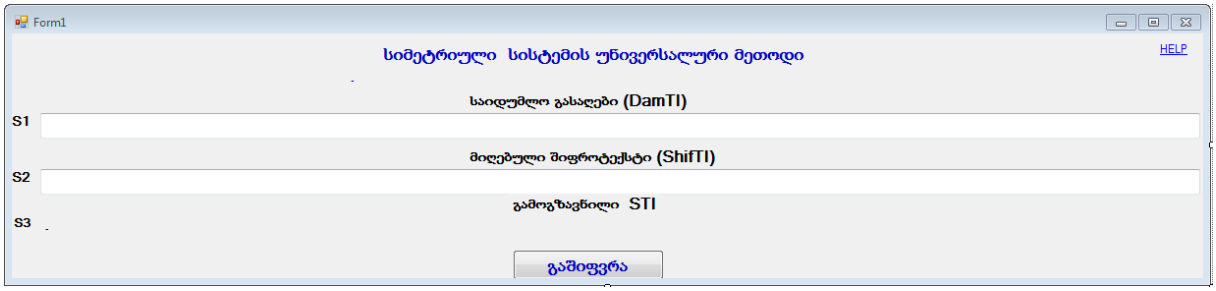
ვ) შეიტანს ფორმაში მითითებულ S1 სტრიქონში დახურულ გასაღებში შემავალ სიმბოლოებს (ანა_GioPrИЙ);

გ) დააწკაპუნებს ღილაკზე „გაშიფვრა“, რის შედეგადაც:

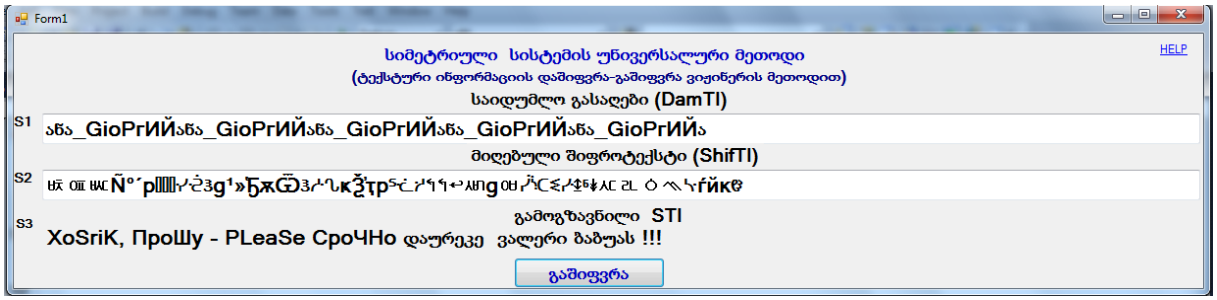
- ფორმირდება დამშიფრავი სიმბოლოების სტრიქონი - DamTI [1,2];

- ფორმაში მითითებულ S2 სტრიქონში ჩაიწერება ანასაგან გამოგზავნილი (გადაცემული) შიფროტექსტი;

- ფორმაში მითითებულ S3 სტრიქონში აისახება ანას მიერ გამოგზავნილი შიფრო ტექსტის შესაბამისი STI (ნახ.5).



ნახ.4



ნახ.5

შევნიშნოთ, რომ თუ ხოსრიკა შიფროტექსტის გასაშიფრავად ფორმაში მითითებულ S1 სტრიქონში ზუსტად არ შეიტანეს ანას მიერ STI დასაშიფრავად გამოყენებულ საიდუმლო გასაღების მნიშვნელობას, მაშინ გაშიფვრის შედეგი, გამოტანილი ეკრანზე (S3 სტრიქონში) იქნება განსხვავებული გამოგზავნილ საწყისი ტექსტური ინფორმაციისაგან - STI.

შევნიშნოთ აგრეთვე, რომ დანართების ბოლო სამი სტრიქონის რეალიზაციით პროგრამულ მოდულებთან მუშაობის ნებისმიერ დროს, ფორმის (იხ. ნახ.1 - ნახ.2) მარჯვენა მხარეს მდებარე HELP ღილაკზე დაწკაპუნებით, ეკრანზე შეიძლება იქნას გამოტანილი MS Word რედაქტორში შექმნილი ფაილის შემცველი ტექსტური ინფორმაცია. კერძოდ, მოცემულ შემთხვევაში, იგულისხმება რომ HELP ღილაკზე დაწკაპუნებით ეკრანზე აისახება D:\VisaubriT_Kriptografiis Enaze\ Guidelines_HELP.docx ფაილში შეტანილი ინფორმაცია.

დანართი 1

```
{  if (textBox2.Text.Length == 1)
      label2.Text =  "(ტექსტური ინფორმაციის დაშიფვრა ცეზარის მეთოდით)";
   else
      if (textBox2.Text.Length < textBox1.Text.Length)
         label2.Text =  "(ტექსტური ინფორმაციის დაშიფვრა ვიჟინერის მეთოდით)";
       else
         if (textBox2.Text.Length >= textBox1.Text.Length)
            label2.Text = "(ტექსტური ინფორმაციის დაშიფვრა ვერნამის მეთოდით)";

      while (textBox1.Text.Length > textBox2.Text.Length)
            { textBox2.Text += textBox2.Text; }
      textBox2.Text = (textBox2.Text).Substring(0, textBox1.Text.Length);
      string ShifTI = "";
      for (int i = 0; i < textBox1.Text.Length; i++)
```

```
            { ShifTI += Convert.ToChar(Convert.ToInt32(textBox1.Text[i]) +
                        Convert.ToInt32(textBox2.Text[i]));
              label8.Text = "";
              label8.Text = ShifTI.ToString();
              File.Delete(@"D:\VisaubriT_Kriptografiis Enaze\ShifTI.txt");
              string path = @"D:\VisaubriT_Kriptografiis Enaze\ShifTI.txt";
              string createText = ShifTI + Environment.NewLine;
              File.WriteAllText(path, createText, Encoding.UTF8);    }
          private void linkLabel1_LinkClicked(object sender, LinkLabelLinkClickedEventArgs e)
        {   System.Diagnostics.Process.Start("D:\\VisaubroT_Kriptografiis
              Enaze\\Guidelines_HELP.docx");  }
```

დანართი 2

```
{       string path = @"D:\VisaubriT_Kriptografiis Enaze\ShifTI.txt";
        string readText = File.ReadAllText(path);
         textBox2.Text = readText;
        textBox2.Text = (textBox2.Text).Trim();
        if (textBox1.Text.Length == 1)
          label2.Text = "(ტექსტური ინფორმაციის გაშიფვრა ცეზარის მეთოდით)";
        else
          if (textBox1.Text.Length < textBox2.Text.Length)
            label2.Text = "(ტექსტური ინფორმაციის გაშიფვრა ვიჟინერის მეთოდით)";
          else
            if (textBox1.Text.Length == textBox2.Text.Length)
              label2.Text = "(ტექსტური ინფორმაციის გაშიფვრა ვერნამის მეთოდით)";
        while (textBox2.Text.Length > textBox1.Text.Length)
          { textBox1.Text += textBox1.Text; }
        textBox1.Text = (textBox1.Text).Substring(0, textBox2.Text.Length);
        label8.Text = "";
        string DasTI = "";
        for (int i = 0; i < textBox2.Text.Length; i++)
         {   DasTI += Convert.ToChar(Convert.ToInt32(textBox2.Text[i]) -
                                        Convert.ToInt32(textBox1.Text[i]));     }
        label8.Text = DasTI.ToString();
}
    private void linkLabel1_LinkClicked(object sender, LinkLabelLinkClickedEventArgs e)
    {  System.Diagnostics.Process.Start("D:\\VisaubroT_Kriptografiis
                                        Enaze\\Guidelines_HELP.docx");  }
```

3. დასკვნა

ტექსტური ინფორმაციის დაშიფვრა/გაშიფვრის შემოთავაზებული უნივერსალური მოდელი და ამ მოდელის მარიალიზებელი პროგრამული მოდულები წარმატებით შეიზლება იქნას გამოყენებულნი იმ პიროვნებების მიერ, ვისაც სურს აწარმოონ ერთმანეთში დიალოგი (ტექსტური ინფორმაციის გაცვლა) "კრიპტოგრაფიის ენაზე".

ლიტერატურა - References - Литература:

1. კეკელია ვ., კოტრიკაძე გ. (2015). კრიპტოგრაფიის სიმეტრიული სისტემის ზოგიერთი მეთოდის რეალიზაციის საკითხების შესახებ. სტუ-ს შრ.კრ. „მას“ N2(20), თბილისი.
2. კეკელია ვ., კოტრიკაძე გ. (2016). კრიპტოგრაფიის სიმეტრიული სისტემის მეთოდები და მოდელები. ნაწ.1, სტუ, თბილისი.
3. სამხარაძე რ. Visual C# .N E T. (2009). სტუ, თბილისი.
4. გაჩეჩილაძე ლ. (2015). დაპროგრამების ალგორითმული ენა C#, ნაწ.1. სტუ, თბილისი.

ON THE REALIZATION OF A UNIVERSAL MODEL OF SYMMETRIC CRYPTOGRAPHY SYSTEMS

Kekelia Valeri

Georgian Technikal Universiti

Summary

On the basis of symmetric cryptographic techniques Caesar system, Vigenere and Vernam a universal model of the encryption / decryption of text information was developed, as well as algorithms and software modules using object oriented programming language C # in Microsoft Visual Studio.NET environment. The aforementioned will provide users the possibility to exchange short text messages i.e. speak in the "language of cryptography".

О РЕАЛИЗАЦИИ УНИВЕРСАЛЬНОЙ МОДЕЛИ СИМЕТРИЧНОЙ СИСТЕМЫ КРИПТОГРАФИИ

Кекелия В.

Грузинский Технический Университет

Резюме

На основе методов криптографии симетричной системы Цезаря, Вижинера и Вернама, разработаны универсальная модель шифрования/дешифрования текстовой информации, а также алгоритм и программные модули на объектно-ориентированном языке программирования - C#, функционирующие в среде Microsoft Visual Studio.NET, что даст лицам возможность обмениваться между собой короткими - текстовыми сообщениями т.е. разговаривать на “языке криптографии”.