გ.კოტრიკაძე, ინფორმაციის უსაფრთხოება, 2015წ. (მაგისტრატურა 2)

განხილულია დაშიფვრის როგორც ტრადიციული ისე თანამედროვე კრიპტოგრაფიული მეთოდები და ალგორითმები. აღწერილია ის მეთოდები და საშუალებები, რომლებიც უზრუნველყოფენ ლოკალური, შიდა კორპორაციული და კორპორაციათაშორისი ქსელების ინფორმაციულ უსაფრთხოებას. მოყვანილია რამოდენიმე კრიპტოგრაფიული ალგორითმის განმახორციელებელი პროგრამა.

დამხმარე სახელმძღვანელო განკუთვნილია 2101 სპეციალობის (ტექნიკური, ადმინისტრაციულ-ეკონომიკური სისტემის მართვა და კომპიუტერული ავტომატიზაცია) სტუდენტებისათვის.

წინასიტყვაობა

ინფორმაციული ტექნოლოგიების სწრაფმა განვითარებამ გამოიწვია ლოკალური ქსელებისა და ისეთი გლობალური ქსელების შექმნა,როგორიცაა internet, intranet (შიდა კორპორაციული ქსელი), ეხტრანეტ (კორპორაციათაშორისი ქსელი). ამ ქსელების შექმნით მოხდა ისეთი ინფორმაციული გარემოს ფორმირება, რომელიც გავლენას ახდენს ადამიანის მოღვაწეობის ყველა სფეროზე. კომპიუტერის მომხმარებლებს მიეცათ ინფორმაციის ოპერატიული გაცვლის ახალი შესაძლებლობები.

ინტერნეტ ქსელი ისეთი სამსახურების მეშვეობით, როგორიცაა: ელექტრონული ფოსტა(e-mail), ჰიპერტექსტური ინფორმაცია (www), ფაილების გადაცემა (Ftp), ტელეკონფერენცია(uzenet), კომპიუტერის დაშორებული მართვა (telnet), დომენების გაცვლა (dns), სასაუბრო კონფერენცია (irc) და სხვ. უზრუნველყოფს როგორც ინფორმაციის ტრანსპორტირებას კომუნიკაციების სხვადასხვა მეთოდების გამოყენებით, ისე საკმარისად ფართო და მაღალდონიან ინფორმაციულ მომსახურებას.

Internet-ის მეშვეობით შესაძლებელია:

-იაფი და ხელმისაწვდომი კავშირგაბმულობის არხების ორგანიზება;

-ელექტრონული ბიზნესის, ელექტრონული კომერციის და მობილური კომერციის განხორციელება;

-დისტანციური განათლების სისტემის ორგანიზება;

-ფულის ელექტრონული გადახდის ორგანიზება;

-ბირჟის, აუქციონის, მაღაზიის, ვიტრინის გვერდების გავრცელება;

-ფულის გადახდის დებეტური სისტემის (ელექტრონული ფული, ელექტრონული ქვითარი) ორგანიზება;

-ტრეიდინგური ოპერაციების ჩატარება;

-დაზღვევის პროცედურის განხორციელება;

-ტელევირკინგის (სახლიდან გამოუსვლელად რაიმე სამუშაოს შესრულება) განხორციელება და სხვ.

რადგან ახალი ინფორმაციული ტექნოლოგიები აადვილებენ ინფორმაციის გავრცელების პროცედურას, ამაღლებენ საწარმოო პროცესების ეფექტურობას, ხელს უწყობენ ბიზნესის სფეროში საქმიანი ოპერაციების გაფართოებას და სხვ., ამიტომ ეს ტექნოლოგიები აქტიურად მკვიდრდება სახალხო მეურნეობის ყველა სფეროში. იქმნება ახალ-ახალი კორპორაციული ინფორმაციული სისტემები, რომლებიც წარმოადგენენ კორპორაციაში შემავალი სხვადასხვა სტრუქტურების ლოკალური ქსელების გაერთიანებას.

აქვე უნდა აღინისნოს, რომ კომპიუტერული საშუალებების და ინფორმაციული ტექნოლოგიების ინტენსიური განვითარება სამწუხაროდ არ ამცირებს თანამედროვე ინფორმაციული სისტემების და კომპიუტერული ქსელების ნაკლოვან მხარეებს. თუ ლოკალური ქსელისათვის არაა გადაწყვეტილი ინფორმაციული უსაფრთხოების უზრუნველყოფის პრობლემები, მაშინ ასეთ ქსელში ადვილად აღწევენ ჰაკერები, კრაკერები და ფრაკერები. ისინი ადვილად იგებენ გადაცემული ინფორმაციის შინაარსს და იყენებენ მას თავიანთი მიზნების სესასრულებლად. აქედან გამომდინარე, ელექტრონული თაღლითების (ჰაკერი,კრაკერი და სხვ.) და ვირუსების ეპოქაში, აუცილებელია, რომ კომპანიის ხელმძღვანელობისათვის პრიორიტეტულ ამოცანას წარმოადგენდეს intranet ქსელისა და მასში შმავალი ლოკალური ქსელების ინფორმაციული უსაფრთხოების უზრუნველყოფა, რადგან კორპორაციული ინფორმაციული რესურსების კონფიდენციალურობაზე და მთლიანობაზე დიდადაა დამოკიდებული როგორც ოპერატიული გადაწყვეტილების მიღება ,ისე კომპანიის ეფექტური მუშაობა. კომპანიის ინფორმაციული უსაფრთხოების საკიტხის ტრადიციულ გადაწყვეტას წარმოადგენს ისეთი ქვესისტემის შექმნა, რომელიც მასში გამოყენებული ინფორმაციის დაცვის თანამედროვე ტექნოლოგიების,სტანდარტების და პროტოკოლების გამოყენებით უზრუნველყოფს ინფორმაციული უსაფრთხოების სასურველ დონეს.

საზოგადოდ, ინფორმაციული უსაფრთხოების ქვეშ იგულისხმება როგორც გადასამუშავებელი, შესანახი და გადასაცემი მონაცემების დაცვის მდგომარეობა მისი არაკანონიერი გაცნობის, გარდაქმნისა და მოსპობის საწინააღმდეგოდ, ისე ინფორმაციული რესურსების დაცვის მდგომარეობა იმ ზემოქმედებისაგან (მომსახურე პერსონალის მიერ დაშვებული შეცდომები,აპარატული და პროგრამული საშუალებების მწყობრიდან გამოსვლა, სტიქიური უბედურება და სხვ.), რომლებიც იწვევენ ამ რესურსების მუშაობის უნარის დარღვევას.

დამხმარე სახელმძღვანელო მოიცავს თორმეტ თავს და დანართს.

პირველ თავში განხილულია კომპიუტერული ქსელების სახეობები, ლოკალური ქსელების აგების პრინციპები და ტოპოლოგია, ლოკალური კომპიუტერული ქსელების კლასიფიკაცია მათი დანიშნულების მიხედვით.

მეორე თავში მოცემულია კრიპტოგრაფიული დაცვის სისტემების ზოგადი სქემები(სიმეტრიული ერთგასაღებიანი, ასიმეტრიული ორგასაღებიანი და სედგენილი) და კრიპტოანალიზური შეტევების სახეობები.

მესამე თავში განხილულია ტრადიციული სიმეტრიული კრიპტოსისტემები მათი წარმოშობის ისტორიული ქრონოლოგიის მიხედვით. კერძოდ, არწერილია შიფრები, მიღებული: ასოების გადანაცვლებით, დამშიფრავი ცხრილებით და მარტივი შეცვლით (პოლიბის, ცეზარის, ტრისემუსის, პლეიფეირის, ჩარლზ უიტსონის,გრონსფელდის, ვიჟინერის, ვერნამის, მრავალალფაბეტიანი და ჰილის). ამავე თავში განხილულია საკითხი დაშიფვრის სისტემის საიდუმლოების შესახებ.

მეოთხე თავში მოცემულია გამა - მიმდევრობით დაშიფვრის მეთოდი. განხილულია ფსევდოშემთხვევითი რიცხვების გენერატორების სახეობები.

მეხუთე თავში განხილულია შერევისა და ჩასმების ერთობლივი გამოყენებით მიღებული ისეთი შიფრების (შედგენილი შიფრების) ალგორითმები, როგორიცაა: DES, IDEA და GOST 28147-89.

მეშვიდე თავში აღწერილია ფაქტორები, რომლებიც იწვევენ ინფორმაციის დაკარგვას ან მის შეცვლას (შემთხვევითი ფაქტორები, კომპიუტერული ვირუსები, ბოროტგანმზრახველის მიზანმიმართული მოქმედებები).

მერვე თავი ეძღვნება კომპიუტერულ ქსელში ინფორმაციის დაცვის მეთოდებს (ორგანიზაციული, ტექნიკური, ანტივირუსული პროგრამები, პაროლები, ელექტრონული გასაღები და სხვ.)

მეცხრე თავში განხილულია იდენტიფიკაციი და აუტენტიფიკაციის საკითხები (იდენტიფიკაციის და აუტენტიფიკაციის პროტოკოლები, ელექტრონული ხელმოწერა, DSA და RSA ალგორითმები, ბრმად ხელისმოწერის ალგორითმი, უდავო ხელისმოწერის ალგორითმი და აუტენტიფიკაციის პროტოკოლი ნულოვანი ცოდნის გადაცემით).

მეათე თავში აღწერილია ელექტრონული ფოსტის დაცვის PGP სისტემა.

მეთერთმეტე თავში განხილულია Internet ქსელიდან განხორციელებული შემოტევების აცილების მეთოდები და საშუალებები (ქსელთაშორისი ეკრანი, გამფილტრავი მარშრუტიზატორი,გამოყენებითი რაბი და სხვ.).

მეთორმეტე თავში მოცემულია პასკალის ენაზე შესრულებული ზოგიერთი ტრადიციული სიმეტრიული კრიპტოსისტემის პროგრამული უზრუნველყოფა.

დანართი მოიცავს რიცხვთა თეორიის იმ საკითხებს, რომლებიც საჭიროა სახელმძღვანელოში განხილული დაშიფვრის მეთოდების ალგორიტმების შესადგენად.

ავტორები მადლიერების გრძნობით მიიღებენ მკიტხველისაგან ნებისმიერ შენიშვნას სახელმძღვანელოს შინაარსის გაუმჯობესების მიზნით.

1.კომპიუტერული ქსელი

კომპიუტერული ქსელი წარმოადგენს ღია სისტემას, რომელშიც ერთიანი ფუნქციური გარემოს საშუალებიტ ერთმანეთთან დაკავშირებულია პერსონალური კომპიუტერები, ფაილ-სერვერები, მოდემები და სხვა სახის მოწყობილობები.

ერთიანი ფუნქციური გარემოს ქვეშ იგულისხმება იმ საერთო წესების (პროტოკოლების) ერთობლიობა, რომლებიც უზრუნველყოფენ კომპიუტერულ ქსელში შემავალი სხვადასხვა სახის პერსონალური კომპიუტერებისა და მოწყობილობების ურთიერთშეთანხმებულ მუსაობას.

თანამედროვე კომპიუტერული ქსელების უმეტესობა მომხმარებლისათვის წარმოადგენს მძლავრ საკომუნიკაციო საშუალებას. მათი დახმარებიტ შესაძლებელია ქსელში ჩართული პერსონალური კომპიუტერების რესურსების გაერთიანება-გადანაწილება და ძვირადღირებული მოწყობილობების (ლაზერული პრინტერი, მოდემი, ფაილ-სერვერი და სხვ.) კოლექტიური გამოყენება.

ნებისმიერი კომპიუტერული ქსელი უნდა აკმაყოფილებდეს შემდეგ მოთხოვნებს:

- მას უნდა გააჩნდეს ღია არქიტექტურა (სხვა ქსელთან დაკავშირების შესაძლებლობა);
- ქსელში მონაცემების ურთიერთგაცვლა უნდა მიმდინარეობდეს მაღალი სიჩქარით;
- ქსელში მონაცემების გადაცემის პროცესში შეცდომების წარმოქმნის ალბათობა უნდა იყოს მცირე.

უმარტივესი კომპიუტერული ქსელის ძირითადი კომპონენტებია: მუშა სადგურები, ფაილ-სერვერები და გადამცემი გარემო (ნახ. 1.1)

გასაღები არის მონაცემების კრიპტოგრაფიული გარდაქმნის ალგორითმის ზოგიერთი პარამეტრის ისეთი კონკრეტული საიდუმლო მდგომარეობა, რომელიც უზრუნველყოფს მოცემული ალგორითმისთვის ყველა შესაძლო ვარიანტიდან მხოლოდ ერთი ვარიანტის არჩევას.

კონკრეტული Z გასაღების საშუალებით ხდება ღია ტექსტის დაშიფვრა და გაშიფვრა. გასაღების პარამეტრის შერჩევა ხდება Z გასაღებების სივრცის სასრული სიმრავლიდან.

გაშიფვრის მიმართ დაშიფვრა შეიძლება იყოს სიმეტრიული, ასიმეტრიული და შედგენილი. აქედან გამომდინარე, არსებობს კრიპტოსისტემის სამი კლასი: სიმეტრიული (ერთგასაღებიანი), ასიმეტრიული (ორგასაღებიანი) და შედგენელი (სიმეტრიულ/ასიმეტირული).

2.1. სიმეტრიული (ერთგასაღებიანი) კრიპტოგრაფული სისტემები

ერთაგასღებიანი კრიპტოგრაფიული სისტემები ინფორმაციის დაცვის კლასიკურ სისტემებია. ამ სისტემებში ინფორმაციული შეტყობენების დაშიფვრისას და გაშიფვრისას გამოიყენება ერთი და იგივე საიდუმლო $Z_ს$ გასაღები, რომლის საიდუმლოდ შენახვა განაპირობებს ინფორმაციის დაცვის საიმედოობას. ერთგასაღებიანი კრიპტოგრაფიული სისტემის სტრუქტურული სქემა ნაჩვენებია 2.2. ნახ-ზე.

ნახ.2.2.

დაშიფვრისა და გაშიფვრის პროცესი ამ სისტემაში შეიძლება გამოისახოს შემდეგნაირად:

$Y=E_{Z_ს}(X)$,

$X=D_{Z_ს}(Y) D_{Z_ს}((E_{Z_ს}((X))$,

სადაც: X არის ღია ტექსტი (დაშიფვრამდე და გაშიფვრის შემდეგ);

Y - დაშიფრული ტექსტი;

$Z_ს$ - საიდუმლო გასაღები, რომელიც ცნობილია როგორც შეტყობინების გამგზავნისთვის ისე მიმღებისთვის;

$E_{Z_ს}$ - დაშიფვრის ფუნქცია;

$D_{Z_ს}$ - გაშიფვრის ფუნქცია.

ამასთან, დაშიფვრისა და გაშიფვრის ურთიერთცალსახობისთვის აუცილებელია შემდეგი სახის ტოლობის შესრულება:

$E_{Z_ს}D_{Z_ს}=e$, სადაც e-ერთადერთი გარდაქმნაა. ყველა ცნობილი ერთგასაღებიანი კრიპტოგრაფიული სისტემა დაშიფვრის მეთოდების მიხედვით იყოფა ბლოკურ, ნაკადურ და კომბინირებულ სისტემებად (შიფრებად). ვინაიდან შეტყობინების ღია ტექსტს გააჩნია ნებისმიერი სიგრძე, ზოგჯერ საკმაო დიდი, ამიტომ ისეთი შეტყობინება იყოფა ფიქსირებული სიგრძის ბლოკებად. ამ ბლოკების ტექსტების დაშიფვრა ხდება ერთმანეთისაგან დამოუკიდებლად. ერთგასაღებიანი ბლოკური შიფრი იყოფა სამ ჯგუფად: შიფრი გადანაცვლებით, შიფრი შეცვლით (ჩასმით) და შედგენილი შიფრი.

ნაკადურ სისტემებში დაშიფვრის პროცესი მიმდინარეობს შეტყობინების ბლოკებად დაყოფის გარეშე. ასეთ სისტემაში დიდი მოცულობის გადასაცემი ინფორმაციის დაშიფვრა და გაშიფვრა პრაქტიკულად მიმდინარეობს რეალურ დროში. ნაკადური შიფრი ორი სახისაა: სინქრონული და თვითსინქრონიზებადი.

დაშიფვრის კომბინირებულ სისტემაში გამოიყენება როგორც ბლოკური, ისე ნაკადური დაშიფვრის პრინციპები.

2.3.ნახ-ზე ნაჩვენებია ერთგასაღებიანი კრიპტოგრაფიული სისტემების დაყოფა დაშიფვრის მეთოდებისა და შიფრების მიხედვით.

ნახ. 2.3.

სიმეტრიულ კრიპტოგრაფიულ სისტემაში (კრიპტოსისტემაში) საიდუმლო გასაღები უნდა გადაეგზავნოს გადამცემს და კანონიერ მიმღებს დაცული არხით (2.2. ნახ.-ზე წყვეტილი ხაზით ნაჩვენებია დაეკრანებული კავშირის ხაზი).

2.2. ასიმეტრიული (ორგასაღებიანი) კრიპტოგრაფიული სისტემები

ასეთ სისტემებში გამოიყენება ორი გასაღები: ღია (არასაიდუმლო) და დახურული (საიდუმლო). ამ გასაღებების გამოყენების ვარიანტების მიხედვით შესაძლებელია დაშიფვრის ორი სახეობის მიღება. თუ ღია გასაღები გამოიყენება დაშიფვრისათვის, ხოლო საიდუმლო გასაღები _ გაშიფვრისათვის, მაშინ მიიღება ღია გასაღებით დაშიფვრის სისტემა (ნახ. 2.4.).

ნახ. 2.4.

ამ შემთხვევაში ღია გასაღების მფლობელს შეუძლია ღია ტექსტის დაშიფვრა, ხოლო მიღებული შიფრის გაშიფვრა შეუძლია მხოლოდ საიდუმლო გასაღების მფლობელს.

დაშიფვრისა და გაშიფვრის პროცესების რეალიზაცია გამოისახება შემდეგი გამოსახულებებით:

$$Y=E_{Z_ღ}(X),$$

$$X=D_{Z_ს}(Y)D_{Z_ს}(E_{Z_ღ}(X)).$$

თუ საიდუმლო გასაღები გამოიყენება დაშიფვრისას, ხოლო ღია გასაღები - გაშიფვრისას, მაშინ ამ შემთხვევაში მხოლოდ საიდუმლო გასაღების მფლობელს შეუძლია ტექსტის დაშიფვრა, ხოლო გაშიფვრა შეუძლია ღია გასაღების ნებისმიერ მფლობელს. დაშიფვრისა და გაშიფვრის პროცესების რეალიზაცია გამოისახება შემდეგი გამოსახულებებით:

$$Y=E_{Z_ღ}(X),$$

$$X=D_{Z_ღ}(Y)D_{Z_ღ}(E_{Z_ს}(X)).$$

ეს ვარიანტი გამოიყენება ელექტრონული ციფრული ხელმოწერის სისტემებში. ე.ი. საიდუმლო გასაღების მფლობელი ასრულებს ხელის მოწერას, ხოლო ღია გასაღების მფლობელი ამოწმებს ამ ხელმოწერას.

ორგასაღებიან კრიპტოგრაფიულ სისტემებში დაშიფრვისა და გაშიფვრის ფუნქციების ურთიერთცალსახობის აუცილებელი პირობაა $E_{Z_ს}\cdot D_{Z_ს}=e$ $E_{Z_ს}\cdot D_{Z_ს}=e$.

ასიმეტრიულ კრიპტოსისტემაში დაუცველი არხით გადაიცემა მხოლოდ ღია გასაღები, ხოლო საიდუმლო გასაღები ინახება მის მფლობელთან.

2.3. შედგენილი კრიპტოგრაფიული სისტემები

არსებული სიმეტრიული და ასიმეტრიული სისტემების ეფექტურობის გამომსახველი მახასიათებლების შედარებითმა ანალიზმა აჩვენა, რომ ასიმეტრიულ სისტემაში დაშიფვრის ალგორითმი მუშაობს გაცილებით ნელა, ვიდრე ერთგასაღებიან კლასიკურ სისტემაში. ამასთან, შეტყობინების დაშიფვრას გააჩნია ისეთი დადებითი თვისებები, რომელთა განხორციელება ერთაგასაღებიან დაშიფვრის სისტემაში შეუძლებელია.

1991 წელს ამერიკელმა სკრიპტოლოგმა ზიმერმანმა წამოაყენა წინადადება ე.წ. შედგენილი კრიპტოგრაფიული სისტემის ზოგადი სქემა ნაჩვენებია 2.5. ნახ.-ზე

ნახ.2.5.

ღია ტექსტის დასაშიფრად გამოიყენება სიმეტრიული დაშიფვრის ხარისხიანი და სწრაფი ალგორითმი საიდუმლო ძ გასაღებით. საიდუმლო გასაღებს წარმოადგენს სეანსურ გასაღებად გამოყენებული შემთხვევითი რიცხვი. გარდა ამისა, მიმდინარეობს სეანსური გასაღების $k=Ez_{ღ}(Z)$ გადაცემა მიმღებს.

გაშიფვრის პროცესი წარმოადგენს დაშიფვრის უკუპროცესს. მიმღების საიდუმლო Z გასაღები გამოიყენება სეანსური Z გასაღების აღსადგენად. ეს უკანასკნელი ახდენს მიღებული შიფრტექსტის სიმეტრიულ $D_Z(Y)$ გაშიფვრის პროცესი წარმოადგენს დაშიფვრის უკუპროცესს. მიმღების საიდუმლო $Z_ს$ გასაღები გამოიყენება სეანსური Z გასაღების აღსადგენად. ეს უკანასკნელი ახდენს მიღებული შიფრტექსტის სიმეტრიულ $D_Z(Y)$ გაშიფვრას და ღია X ტექსტის აღდგენას.

2.4. კრიპტოანალიზური შეტევა

2.6. ნახ.-ზე ნაჩვენებია კრიპტოსისტემის სქემა, სადაც კავშირის არხთან მიერთებულ არაკანონიერ მიმღებს შეუძლია კავშირის არხით გადაცემული ყველა შიფრტექსტის არა მარტო წაკითხვა, არამედ ამ შრიფტექსტების შეცვლა თავისი განზრახვების შესასრულებლად.

ნახ. 2.6.

არაკანონიერი მიმღების მხრიდან ყველანაირი მცდელობა Y შიფრტექსტის გასაშიფრად ან თავისი საკუთარი X ტექსტის დაშიფვრის მცდელობას კანონიერი მიმღებისათვის დამაჯერებელ Y შიფრტექსტად, Z გასაღების არცოდნის შემთხვევაში, ეწოდება კრიპტოანალიზური შეტევა. კრიპტოანალიზი ეს არის მეცნიერება დაშიფრული ტექსტიდან საწყისი ტექსტის აღდგენის შესახებ Z გასაღების მნიშვნელობის არცოდნის შემთხვევაში. თუ კრიპტოანალიზური შეტევა ვერ აღწევს დასახულ მიზანს და კრიპტოანალიტიკოსს არშეუძლია გასაღების მნიშვნელობის არცოდნის შემთხვევაში მიიღოს X ღია ტექსტი Y-დან ან Y შიფრტექსტი X–დან, მაშინ ამბობენ, რომ ასეთი კრიპტოსისტემა არის კრიპტომედეგი. კრიპტოსისტემის მედეგობა განისაზღვრება ძ გასაღების მნიშვნელობის საიდუმლოებით. კრიპტოანალიტიკოსი ინფორმაციის დაშიფვრის გასაღების გამოსათვლელად, მის ხელთ არსებული საწყისი მონაცემებიდან გამომდინარე, ასრულებს ქვემოთ განხილული კრიპტოანალიზური შეტევებიდან ერთ-ერთს.

1. კრიპტოანალიზური შეტევა, როცა ცნობილია მხოლოდ შიფრტექსტი.

კრიპტოანალიტიკოსი ფლობს ერთი და იგივე Ez ალგორითმით დაშიფრულ რამდენიმე შეტყობინების $Y_1, Y_2,...,Y_1$ შიფრტექსტებს და მისი მიზანია შეძლებისამებრ რაც შეიძლება ბევრი $X_1,X_2,...,X_1$ შეტყობინების აღდგენა ან უკეთეს შემთხვევაში Z გასაღების მნიშვნელობის გამოთვლა.

2. კრიპტოანალიზური შეტევა, როცა ცნობილია ღია ტექსტი.

კრიპტოანალიკოსისათვის ცნობილია რამდენიმე შეტყობინების

$Y_1, Y_2,...,Y_1$ შიფრტექსტები და $X_1, X_2,..., X_1$ ღია ტექსტები. მისი მიზანია გასაღების მნიშვნელობის გამოთვლა ან იგივე გასაღებით დაშიფრული ნებისმიერი ახალი შეტყობინების გაშიფვრის Dz ალგორითმის მოძებნა.

3. კრიპტოანალიზური შეტევა ღია ტექსტის არჩევის შემთხვევაში.

კრიპტოანალიტიკისთვის ცნობილია $Y_1, Y_2,...,Y_1$ შიფრტექსტები და მათთან დაკავშირებული $X_1, X_2,...,X_1$ ღია ტექსტები. ამასთან მას შეუძლია სურვილისამებრ შეარჩიოს ღია ტექსტი, რომელსაც შემდეგ მიიღებს დაშიფრული სახით. ასეთი კრიპტოანალიზი უფრო მძლავრია, ვიდრე კრიპტოანალიზი, როცა ცნობილია ღია ტექსტის ისეთი ბლოკები, რომლებიც განაპირობებენ Z გასაღების შესახებ უფრო მეტი ინფორმაციის მიღების შესაძლებლობას. კრიპტოანალიტიკოსის მიზანია დაშიფვრისას გამოყენებული Z გასაღების გამოთვლა ან იგივე გასაღებით დაშიფრული ახალი შეტყობინების გაშიფვრის D_Z ალგორითმის მოძებნა.

4. კრიპტოანალიზური შეტევა ღია ტექსტის ადაპტური შერჩევით.

ეს არის ღია ტექსტის შერჩევით შეტევის განსაკუთრებული ვარიანტი. კრიპტოანალიტიკოსს შეუძლია არა მხოლოდ შეარჩიოს ღია ტექსტი, რომელიც შემდეგ განიცდის დაშიფვრას, არამედ დაშიფვრის რეზულტატიდან გამომდინარე შეცვალოს შერჩეული ტექსტი ახალი ტექსტით. კრიპტოანალიტიკოსი თავდაპირველად ირჩევს ღია ტექსტის შედარებით პატარა საცდელ ბლოკს და, დაშიფვრის რეზულტატებიდან გამომდინარე, აგრძელებს ღია ტექსტის ბლოკების შერჩევას.

5. კრიპტოანალიზური შეტევა არჩეული შიფრტექსტის გამოყენებით.

კრიპტოანალიტიკოსს შეუძლია შეარჩიოს გასაშიფრად სხვადასხვა $Y_1, Y_2,..., Y_1$ შიფრტექსტები და ამასთან მიეწვდომება გაშიფრულ $X_1,X_2,...,X_1$ ტექსტებთან. მაგალითად, კრიპტოანალიტიკოსს მიეცა შესაძლებლობა შეაღწიოს არასანქციონირებულ მიერთებისგან დაცულ ისეთ ბლოკში, რომლის მოვალეობაა შიფრტექსტის ავტომატური გაშიფვრა. კრიპტოანალიტიკოსის მიზანია Z გასაღების მნიშვნელობის გამოთვლა. კრიპტოანალიზის ეს სახეობა გამოიყენება ღია გასაღების მქონე ალგორითმის გამოსათვლელად.

6. კრიპტოანალიზური შეტევა გასაღებების ყველა შესძლო ვარიანტების გადარჩევის მეთოდით.

ამ შემთხვევაში კრიპტოანალიტიკოსი იყენებს ცნობილ შიფრტექსტს და გასაღებების ყველა შესაძლო ვარიანტების განხილვით ამოწმებს არის თუ არა გაშიფვრის შედეგად მიღებული ღია ტექსტი სასურველი, საჭირო ინფორმაცია. ასეთი შეტევისას საჭიროა გამოთვლითი ტექნიკის დიდი რესურსი და ამიტომ იგი ცნობილია ძალისმიერი შეტევის სახელწოდებით.

7. ბანდიტური კრიპტოანალიზი. "კრიპტოანალიტიკოსი" დაშინების, შანტაჟის, წამების ან ქრთამის მიცემის გზით ცდილობს გასაღების მნიშვნელობის მოპოვებას. კრიპტოანალიზური შეტევის მეთოდი ითვლება დაშიფვრის ალგორითმის გახსნის ერთ-ერთ მძლავრ და ეფექტურ მეთოდად. დაშიფვრის ალგორითმის გახსნის ერთ-ერთ მძლავრ და ეფექტურ მეთოდად. დაშიფვრის ალგორითმის გახსნის სირთულე შეიძლება დაიყოს შემდეგ კატეგორიებად:

ა) სრული გახსნა - კრიპტოანალიტიკოსი გასაღების არცოდნის შემთხვევაში პოულობს გაშიფვრის ალგორითმის ექვივალენტურ ალტერანატიულ ალგორითმს.

ბ) გლობალური დედუქცია - კრიპტოანალიტიკოსი Z გასაღების არცოდნის შემთხვევაში პოულობს გაშიფვრის $D_Z(Y)$ ალგორითმის ექვივალენტურ ალტერნატიულ ალგორითმს.

გ) შემთხვევითი (ნაწილობრივი) დედუქცია - კრიპტოანალიტიკოსი პოულობს (მაგალითად, იპარავს) მის ხელთ არსებული შიფრტექსტის შესაბამის ღია ტექსტს;

დ) ინფორმაციული დედუქცია - კრიპტოანალიტიკოსი მოიპოვებს რაღაც ინფორმაციას გასაღების ან ღია ტექსტის შესახებ.

3. ტრადიციული სიმეტრიული კრიპტოსისტემები

ინფორმაციის დაცვის საშუალებათა უმეტესობა ემყარება კრიპტოგრაფიული შიფრებისა და დაშიფვრა-გაშიფვრის პროცედურების გამოყენებას.

შიფრის განსაზღვრების ქვეშ იგულისხმება შიფრის გასაღებისა და კრიპტოგრაფიული ალგორითმით მოცემული შექცევადი გარდაქმნის საშუალებით ღია მონაცემების სიმრავლის ასახვა დაშიფრული მონაცემების სიმრავლეზე.

შიფრის ძირითადი მახასიათებლია კრიპტომედეგობა, რომელიც განსაზღვრავს შიფრის სიმტკიცეს კრიპტოანალიზის მეთოდებით მისი გაშიფრვის მცდელობისას. ეს მახასიათებელი განისაზღვრება იმ დროის ინტერვალით, რომელიც საჭიროა შიფრის გასახსნელად.

კრიპტოგრაფიული შიფრი ითვლება უდავო მედეგად, თუ კრიპტოანალიტიკოსისათვის ღია ტექსტის აღდგენა შეუძლებელია ნებისმიერი მოცულობის შიფრტექსტის ცოდნის შემთხვევაში.

ინფორმაციის კრიპტოგრაფიული დაცვისთვის გამოყენებული შიფრი უნდა აკმაყოფილებდეს შემდეგ მოთხოვნებს:

- უნდა ხასიათდებოდეს საკმარისი კრიპტომედეგობით (მონაცემების დახურვის საიმედოობით);
- დაშიფვრისა და გაშიფვრის პროცესი უნდა იყოს მარტივი;
- დაშიფვრის შედეგად მიღებული ინფორმაციისთვის დასაშვებია უმნიშვნელო სიჭარბე;
- შიფრი უნდა იყოს არამგრძნობიარე დაშიფვრის პროცესში დაშვებული მცირეოდენი შეცდომების მიმართ.

ამ მოთხოვნებს მეტნაკლებად აკმაყოფილებენ მონაცემების გადანაცვლებით, შეცვლით (ჩასმით), გამირებით და ანალიზური გარდაქმნით მიღებული შიფრები.

გადანაცვლებით დაშიფვრისას დასაშიფრი ტექსტის სიმბოლოები გარკვეული ბლოკის ფარგლებში განიცდიან გადანაცვლებას განსაზღვული წესის მიხედვით.

შეცვლით (ჩასმით) დაშიფვრისას დასაშიფრი ტექსტის სიმბოლოები იცვლება იგივე ან სხვა ალფაბეტის სიმბოლოებით შეცვლის წინასწარ განსაზღვული სქემის მიხედვით.

შეცვლით დაშიფვრისას მიღებულ შიფრებს შენაცვლებითი შიფრები ეწოდება. კლასიკურ კრიპტოგრაფიაში განასხვავებენ ოთხი სახის შენაცვლებით შიფრს:

- მონოალფაბეტური შიფრი - ეს არის მარტივი შიფრი, რომელშიც ღია ტექსტის თითოეული სიმბოლო იცვლება შიფრტექსტის შესაბამისი სიმბოლოთი.
- ომოფონიკური შენაცვლებითი შიფრი - ღია ტექსტის თითოეული სიმბოლოს შეიძლება შეესაბამოს შიფრტექსტის ერთი ან რამდენიმე სიმბოლო. მაგალითად, A-ს შეიძლება შეესაბამოს 5, 17, 29 ან 63; B-ს 4, 21, 47 ან 83 და ა.შ.;

- n-გრამა შიფრი - შიფრავს ღია ტექტის სიმბოლოების ბლოკებს ჯგუფებად. მაგალითად, ბლოკი „ABD“ შეიძლება შეიცვალოს „QRS“-ით, ბლოკი „ABD“ -„TCJ“-ით და ა.შ.;
- მრავალჯერადი შენაცვლებითი შიფრი - წარმოადგენს რამდენიმე მარტივი შენაცვლებითი შიფრის გაერთიანებას.

გამირებით დაშიფვრისას დასაშიფრი ტექსტის სიმბოლოები იკრიბება რომელიღაც შემთხვევითი მიმდევრობის სიმბოლოებთან. ამ შემთხვევითი მიმდევრობას ეწოდება შიფრი გამა. დაშიფვრის მედეგობა ძირითადად განისაზღვრება გამა შიფრის სიგრძით (პერიოდით, ე.ი. შიფრის განუმეორებადი ნაწილის სიგრძით).

ანალიზური გარდაქმნით დაშიფვრისას დასაშიფრი ტექსტი გარდაიქმნება რომელიღაც ანალიზური წესით (ფორმულით). მაგალითად, შეიძლება გამოყენებულ იქნეს ვექტორისა და მატრიცის გამრავლების წესი. ამასთან, მატრიცა წარმოადგენს შიფრის გასაღებს (ამიტომ მატრიცის განზომილება და მისი გამოსახულება ინახება საიდუმლოდ), ხოლო ვექტორის სიმბოლოები - დასაშიფრ ტექსტს.

როგორც ღია ტექსტი, ისე დაშიფრული ტექსტი (შიფრტექსტი) გამოსახულია ალფაბეტის ასოებით. ეს ასოები წარმოადგენენ სიმბოლოების სასრულ სიმრავლეს. ალფაბეტის სახეობებია: მთავრული ასოების, ნუსხური ასოების, მთავრული და ნუსხური ასოების, არაბული ციფრების.

3.1. შიფრი ასოების გადანაცვლებით

ჩვენს წელთაღრიცხვამე მე-5 საუკუნეში სპარტელების მმართველის სამხედრო კავშირების დასამყარებლად გააჩნდათ კარგად დამუშავებული დაშიფვრის სისტემა. ისინი შიფრავდნენ შეტყობინებას უმარტივესი კრიპტოგრაფიული მოწყობილობის გამოყენებით. კერძოდ, ცილინდრული ფორმის მქონე ღეროზე სპირალურად ხვია-ხვიასთან ახვევდნენ პერგამენტის ზოლს და შედეგად წერდნენ პერგამენტზე (თითო სიმბოლო ერთ ხვიაზე) ღეროს გასწვრივ დასაშიფრ ტექსტს. ამგვარად მიღებული დაშიფრული ტექსტი პერგამენტის ზოლზე წარმოადგენს ქაოსურად განლაგებულ ასოებს. იგივე რეზულტატი მიიღება, თუ შეტყობინების ასოები დაიწერება რგოლურად, ოღონდ არა მთლიანად, არამედ გარკვეული რაოდენობის სიმბოლოებით მთლიანად ტექსტის ამოწურვამდე.

მაგალითად, თუ თითოეულ სტრიქონში რგგოლურად ჩაიწერება შეტყობინების НАСТУПАЙТЕ სამ-სამი ასო, მაშინ დაშიფრული ტექსტი მიიღებს შემდეგ სახეს НАТУПЕСАТЙ (ნახ.3.1.). ასეთი სახით დაშიფრული ტექსტის გასაშიფრად საჭიროა როგორც დაშიფვრის წესის ცოდნა, ისე იგივე დიამეტრის ცილინდრის ფორმის ღეროს არსებობა.

ნახ. 3.1.

3.2. დამშიფრავი ცხრილები

კრიპტოგრაფიის განვითარება დაიწყო აღორძინების ეპოქაში (მე-14 საუკუნის მიწირულს). კრიპტოგრაფია გამოიყენებოდა როგორც პოლიტიკაში, დიპლომატიაში, სამხედრო საქმეში, ისე ინტელექტუალური საკუთრების დასაცავად ინკვიზიციის დევნისაგან. შიფრტექსტების მისაღებად გამოიყენებოდა დასაშიფრი ცხრილები. გასაღების როლს ასრულებდა:

- ცხრილის ზომა;
- სიტყვა ან ფრაზა, რომელიც ედებოდა საფუძვლად გადანაცვლებას;
- ცხრილის სტრუქტურის თავისებურებანი.

ყველაზე სპრიმიტიული დასაშიფრი ცხრილი მიიღება სიმბოლოების უბრალო გადანაცვლებით. ასეთი ცხრილის გასაღებია ცხრილის ზომა. მაგალითად, შეტყობინება ТЕРМИНАТОР ПРИБЫВАЕТ СЕДЬМОГО В ПОЛЬНОЧЬ იწერება 5x7 განზომილებიან ცხრილში მიმდევრობით სვეტების სახით. (ნახ. 3.2.).

ნახ. 3.2.

დაშიფრული ტექსტი მიიღება სტრიქონების წაკითხვით. თუ შრიფტექსტი ჩაიწერება ხუთ-ხუთი ასოს შემცველი ბლოკებით, მაშინ მიიღება:

ТНПВЕ ГЛЕАР АДОНР ТИЕЬВ ОМОБТ МПЧИР ЫСООЬ.

გაშიფვრის პროცესი მიმდინარეობს პირიქით. ე.ს. დაშიფრული ტექსტი იწერება იმავე განზომილების ცხრილში თანმიმდევრულად სტრიქონებში და შემდეგ იკითხება სვეტები თანმიმდევრულად.

ცხრილში საწყისი შეტყობინების ჩაწერისა და წაკითხვის მარშრუტის ცვლილებით შესაძლებელია სხვადასხვა შიფრტექსტების მიღება. მაგალითად, თუ იგივე შეტყობინება ცხრილში ჩაიწერება ჰორიზონტალური მარშრუტით, დაწყებული მარჯვენა ზედა კუთხიდან და რიგრიგობით მარცხნიდან მარჯვნივ და მარჯვნიდან მარცხნივ, მაშინ ცხრილი მიიღებს 3.3. ნახ.-ზე ნაჩვენებ სახეს.

Т	Е	Р	М	И	Н	А
Б	И	Р	П	Р	О	Т
Ы	В	А	Е	Т	С	Е
В	О	Г	О	М	Ь	Д
П	О	Л	Н	О	Ч	Ь

ნახ.3.3.

თუ შიფრტექსტის ამოწერა შესრულდება ვერტიკალური მარშრუტით, დაწყებული მარჯვენა ზედა კუთხიდან და რიგრიგობით ზემოდან ქვევით და ქვევიდან ზემოთ, მაშინ ხუთ-ხუთი ასოს შემცველი ბლოკებით გამოსახულ შიფრტექსტს ექნება შემდეგი სახე:

АТЕДЬ ЧЬСОН ИРТМО НОЕПМ РРАГЛ ООВИЕ ТБЫВП.

გადანაცვლებისას, სიტყვის ან ფრაზის გამოყენების შემთხვევაში, გასაღებს წარმოადგენს გამოყენებული სიტყვა ან ფრაზა. ცხრილის პირველ სტრიქონში იწერება სიტყვა (გასაღები), ხოლო მეორე სტრიქონში ასოების ნომრები (1,2,3...) ალფაბეტის რიგითობის მიხედვით. მაგალითად, თუ გასაღებად აღებული იქნება სიტყვა ПЕЛИКАН, მაშინ დაუშიფრავი ცხრილი მიიღებს 3.4. ნახ-ზე ნაჩვენებ სახეს.

П	Е	Л	И	К	А	Н
7	2	5	3	4	1	6
Т	Н	П	В	Е	Г	Л
Е	А	Р	А	Д	О	Н
Р	Т	И	Е	Ь	В	О

М	О	Б	Т	М	П	Ч
И	Р	Ы	С	О	О	Ь

ნახ. 3.4.

თუ სიტყვა-გასაღები შეიცავს ერთნაირ ასოებს, მაშინ მათი დანომვრა მოხდება მარცხნიდან მარჯვნივ. მაგალითად, ვთქვათ, სიტყვა გასაღებია ТАБЛИЦА. ამ შემთხვევაში მიიღება ციფრების შემდეგი განლაგება:

Т А Б Л И Ц А

6 1 3 5 4 7 2.

დაშიფრული ცხრილის მისაღებად საჭიროა სვეტების გადაადგილება ნუმერაციის ზრდილობის მიხედვით (ნახ.3.5.).

А	Е	И	К	Л	Н	П
1	2	3	4	5	6	7
Г	Н	В	Е	П	Л	Т
О	А	А	Д	Р	Н	Е
В	Т	Е	Ь	И	О	Р
П	О	Т	М	Б	Ч	М
О	Р	С	О	Ы	Ь	И

ნახ. 3.5.

დაშიფრული ტექსტის მისაღებად საჭიროა სტრიქონების თანმიმდევრული წაკითხვა. შიფრტექსტს ექნება შემდეგი სახე:

ГНВЕП ЛТОАА ДРНЕВ ТЕЬИО РПОТМ БЧМОР СОЫЬИ.

დაშიფრული ტექსტის მისაღებას შეიძლება წაკითხვა განხორციელდეს დიაგონალურად (ნახ. 3.6.).

$Г_{1}$	$Н_{2}$	$В_{4}$	$Е_{7}$	$П_{11}$	$Л_{16}$	$Т_{21}$
$О_{3}$	$А_{5}$	$А_{8}$	$Д_{12}$	$Р_{17}$	$Н_{22}$	$Е_{26}$
$В_{6}$	$Т_{9}$	$Е_{13}$	$Ь_{18}$	$И_{23}$	$О_{27}$	$Р_{30}$
$П_{10}$	$О_{14}$	$Т_{19}$	$М_{24}$	$Б_{28}$	$Ч_{31}$	$М_{33}$
$О_{15}$	$Р_{20}$	$С_{25}$	$О_{29}$	$Ы_{32}$	$Ь_{34}$	$И_{35}$

ნახ. 3.6.

შიფრტექსტებს ექნება შემდეგი სახე:

ГНОВАВЕ АТППДЕО ОЛРЬТРТ НИМСЕОБ ОРЧЫМЬИ.

დამატებითი დაცვის განსახორციელებლად შეიძლება დაშიფრული შეტყობინების ხელმეორედ დაშიფვრა. დაშიფრვის ასეთ მეთოდს ეწოდება ორმაგი გადანაცვლება.

ორმაგი გადანაცვლებისას მიიღება სვეტებისა და სტრიქონების გადანაცვლებით მიღებული ცხრილები ცალ-ცალკე. თავდაპირველად ცხრილში იწერება შეტყობინების ტექსტი და შემდეგ თანმიმდევრულად ხდება ჯერ სვეტების, ხოლო შემდეგ სტრიქონების გადანაცვლება (ნახ. 3.7.). გაშიფვრისას გადანაცვლების თანმიმდევრობა

უნდა შესრულდეს პირიქით. შიფრის გასაღებს წარმოადგენს საწყისი ცხრილის სვეტებისა და სტრიქონების ნომრების თანმიმდევრობა 4132 და 3142 შესაბამისად.

ორმაგი გადანაცვლებისას ვარიანტების რაოდენობა დამოკიდებულია ცხრილის ზომებზე. nxn ცხრილისთვის ვარიანტების რაოდენობა იქნება:$P_n^2 = (1 \cdot 2 \cdot 3 \cdot .....n)^2$

შიფრი ორმაგი გადანაცვლებით არ გამოირჩევა მაღალი მედეგობით და ადვილად „ტყდება“ დაშიფვრის ცხრილის ნებისმიერი ზომების შემთხვევაში.

	4	1	3	2
3	П	Р	И	Л
1	Е	Т	А	Ю
4	В	О	С	Ь
2	М	О	Г	О
	1	2	3	4
3	Р	Л	И	П
1	Т	Ю	А	Е
4	О	Ь	С	В
2	О	О	Г	М

საწყისი ცხრილი სვეტების გადანაცვლები

	1	2	3	4
1	Т	Ю	А	Е
2	О	О	Г	М
3	Р	Л	И	П
4	О	Ь	С	В

სტრიქონების გადანაცვლება

ნახ. 3.7.

დამშიფრავი ცხრილებით შესაძლებელია ე.წ. მარშრუტული გადანაცვლების განხორციელება. მარშრუტულ გადანაცვლებას მიეკუთვნება:

- დაშიფვრა მაგიური კვადრატების გამოყენებით;
- დაშიფვრა სპეციალური ტრაფარეტის (მბრუნავი გისოსის) გამოყენებით;
- დაშიფვრა ჭადრაკის დაფის გამოყენებით.

დაშიფვრა მაგიური კვადრატით გამოიყენებოდა შუა საუკუნეებში. მაგიური კვადრატი ეწოდებოდა კვადრატულ ცხრილს, რომლის უჯრებშიც იწერება ისეთი ნატურალური რიცხვების მიმდევრობა დაწყებული 1-დან, რომელთა ჯამიც ნებისმიერ სვეტში, ნებისმიერ სტრიქონში და ნებისმიერ დიაგონალზე წარმოადგენს ერთი და იგივე რიცხვს. დასაშიფრი ტექსტის სიმბოლოები რიგითი თანმიმდევრობით იწერება მაგიური კვადრატის შესაბამის უჯრებში (უჯრაში მოთავსებული რიცხვი ემთხვევა ტექსტში შემავალი სიმბოლოს რიგით ნომერს). შიფრტექსტის მისაღებად საჭიროა ასოებით შევსებული ცხრილის წაკითხვა სტრიქონების მიხედვით.

- ნახ-ზე ნაჩვენებია რვა 4x4 მაგიური კვადრატი (ჯამით 34) და პირველი კვადრატის შევსება დასაშიფრი შეტყობინებით ПРИЛЕТАЮ ВОСЬМОГО

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

4	10	7	13
5	15	2	12
9	3	14	8
16	6	11	1

4	6	9	15
3	16	5	10
14	1	12	7
13	11	8	2

12	2	5	15
7	13	10	4
9	3	8	14
6	16	11	1

16	1	4	13
6	11	10	7
9	8	5	12
3	14	15	2

10	5	11	8
6	9	7	12

3	4	14	13
15	16	2	1

7	5	12	10
9	11	8	6
4	2	13	15
14	16	1	3
9	6	12	7
5	10	8	11
4	3	13	14
16	15	1	2
О	И	Р	М
У	О	С	Ю
В	Т	А	Ь
Л	Г	О	П

П Р И Л Е Т А Ю В О С Ь М О Г О.
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

ნახ. 3.8.

შიფრტექსტია: ОИРМ ЕОСЮ ВТАЬ ЛГОП.

კვადრატის ზომების გაზრდით სწრაფად იზრდება მაგიური კვადრატების რიცხვი. 3x3 კვადრატს შეესაბამება ერთი მაგიური კვადრატი (შემობრუნების უგულვებელყოფით), 4x4 კვადრატს შეესაბამება 880 მაგიური კვადრატი, ხოლო 5x5 კვადრატს - 250 000-მდე.

მაგალითად, თუ 3.8. ნახ-ზე თითოეული კვადრატი შემობრუნდება 90^0-ით სამჯერ და შემდეგ განხორციელდება ყველა კვადრატის სარკისებრი ასახვა ჰორიზონტალური ან ვერტყიკალური მიმართულებით, მაშინ მიიღება 64 სახის 4x4 მაგიური კვადრატი.

შეტყობინების დასაშიფრად შესაძლებელია სპეციალური ტრაფარეტის (მბრუნავი გისოსის) გამოყენება. მბრუნავი გისოსი, განზომილებით nxn (n ლუწი რიცხვია), არის n^2 რაოდენობის კვადრატული უჯრების გაერთიანება. კვადრატული უჯრები დაყოფილია ჯგუფებად და თითოეულ ჯგუფში შემავალი კვადრატული უჯრების რაოდენობა $n^2/4$/ თითოეული ჯგუფიდან ამოჭრილია ერთი კვადრატი ისე, რომ გისოსის ოთხი შემობრუნებით ხდება გისოსის მიერ დაკავებული მთლიანი ფართის გადაფარვა. გისოსის ყოველი მდებარეობისას თითოეულ ამოჭრილ კვადრატში იწერება ღია ტექსტში შემავალი თითო სიმბოლო, მაშასადამე, ერთი ტრაფარეტით შესაძლებელია n^2 რაოდენობის სიმბოლოს შემცველი ღია ტექსტის დაშიფვრა. დაშიფრული ტექსტი მიიღება

ტრაფარეტის სტრიქონების თანმიმდევრობითი წაკიხთვის შედეგად. თუ ღია ტექსტში შემავალი სიმბოლოების რაოდენობა ნაკლებია n^2-ზე, მაშინ ხდება სიმბოლოების რაოდენობის შევსება ნებისმიერი სიმბოლოების დამატებით.

მაგალითის სახით განვიხილოთ 4x4 და 6x6 ტრაფარეტები. პირველი შეიცავს 16 კვადრატულ უჯრას ოთხი ჯგუფით, ხოლო მეორე - 36 უჯრას ოთხი ჯგუფით (ნახ. 3.9.).

ნახ.3.9.

განვიხილოთ შეტყობინების ЗАСЕДАНИЕ СОСТОИТСЯ ЗАВТРА ЮСТАС დაშიფვრა 4x4 ტრაფარეტის გამოყენებით. მოცემული შეტყობინება იყოფა ოთხ-ოთხ სიმბოლოდ. რადგან სულ არის 29 სიმბოლო, ამიტომ საჭიროა კიდევ სამი ნებისმიერი სიმბოლოს დამატება (А,Б,В). ე.ს. დასაშიფრია რვა ოთხეული ЗАСЕ, ДАНИ, ЕСОС, ТОИТ, СЯЗА, ВТРА, ЮСТА, САБВ. 3.10. ნახ-ზე ნაჩვენებია დაშიფვრის პროცესი.

ნახ.3.10.

შევსებული ცხრილები იქნება (ნახ. 3.11.).

Т	Д	Е	З
А	О	А	С
С	О	Н	И
С	Е	Т	И
С	В	Ю	С
Т	А	Я	С
З	Т	Р	Б
А	А	В	А

ნახ. 3.11.

შიფრტექსტი იქნება: ТДЕЗ АОАС СОНИ СЕТИ СВЮС ЗТРБ ААВА.

იგივე შეტყობინების დასაშიფრად 6x6 ტრაფარეტის გამოყენებით საჭიროა შეტყობინების დაყოფა 9-9 სიმბოლოდ (აქ დაემატება შვიდი სიმბოლო):

ЗАСЕДАНИЕ СОСТОИТСЯ ЗАВТРАЮСТ АСАБВГДЕЗ.

დაშიფვრის პროცესი ნაჩვენებია 3.12. ნახ-ზე.

ნახ.3.12.

შევსებული ცხრილს ექნება 3.13. ნახ-ზე ნაჩვენები სახე.

С	З	А	З	О	А
А	С	В	С	С	А
Б	Е	Т	В	Г	Д
Р	Т	О	А	А	И
Т	Ю	Д	Н	С	С
И	Е	Т	Я	Е	З

ნახ.3.13.

შიფრტექსტი იქნება:

С ЗАЗОААСВССАБЕТВГДРТОАААИТЮДНССИЕТЯЕЗ.

მბრუნავ გისოსად შეიძლება მართკუთხა ფორმის ისეთი ტრაფარეტის გამოყენება, რომელიც შეიცავს 2mx2k რაოდენობის კვადრატულ უჯრას. ტრაფარეტში ამოჭრილია m . k რაოდენობის უჯრები ისე, რომ ტრაფარეტის ოთხი ვარიანტით განლაგებამ იგივე ზომის სუფთა ფურცელზე გამოიწვიოს ამოჭრილი უჯრებით ფურცლის მთლიანი ფართის გადაფარვა. ტრაფარეტის განლაგების ვარიანტებია:

1-პირდაპირი; 2-პირველი ვარიანტის შემობრუნება 180^0-ით; 3-პირველი ვარიანტის სარკისებრი ასახვა ჰორიზონტალური მიმართულებით; 4- მესამე ვარიანტის შემობრუნება 180^0-ით.

3.14. ნახ-ზე ნაჩვენებია 4x6 და 6x10 რაოდენობის უჯრის შემცველი ტრაფარეტების თითო ვარიანტი. ამოჭრილი კვადრატების რაოდენობა, სესაბამისად, 6 და 15-ის ტოლია.

ნახ. 3.14.

3.15. ნახ.ზე ნაჩვენებია 6x10 ტარაფარეტის გამოყენებით შეტყობინების ШИФРРЕШЕТКА ЯВЛЯЕТСЯ ЧАСТНЫМ СЛУЧАЕМ ШИФРАМАРШРУТНОЙ ПРЕСТАНОВКИ დაშიფვრა. ტრაფარეტის ამოჭრილ თითოეულ უჯრაში იწერება შეტყობინების თითო ასო და შევსება იწყება მარცხენა ზედა კუთხიდან სტრიქონების თანმიმდევრული გავლით (ნახ. 3.15.).

ნახ. 3.15.

შიფრტექსტი იქნება

ЕШАТСЕНЯНШИИОЙФПРРЕЧЕРЕАФЕШСРСЕТАТТНМАКЫАРАМСШЛРУНУОТЯВКВЛИЧЯ.

ცნობილმა მათემატიკოსმა ლეონარდო ეილერმა 1759 წელს აღმოაჩინა ჭადრაკის დაფაზე მხედრის შემოვლის ჩაკეტილი მარშრუტი (მხედარი შემოივლის დაფის ყველა უჯრას და, ამასთან იგი თითოეულ უჯრაზე მხოლოდ ერთხელ მოხვდება). ჭადრაკის დაფაზე მხედრის შემოვლის თანმიმდევრობა, დაწყებული a4 უჯრიდან, ნაჩვენებია 3.16. ნახ-ზე.

ნახ.3.16.

თუ დასაშიფრი ტექსტის სიმბოლოები რიგითი თანმიმდევრობით ჩაიწერება ამ ცხრილში და შემდეგ წაკითხვა შესრულდება სტრიქონების მიხედვით ზემოდან ქვევით ან პირიქით, მაშინ მიიღება შიფრტექსტი.

თუ შეტყობინება შეიცავს 32 სიმბოლოს, მაშინ გამოიყენება ამ ცხრილის ქვედა ან ზედა ოთხი სტრიქონი (ზედა ოთხი სტრიქონის გამოყენებისას დასაშიფრი ტექსტის სიმბოლოების რიგითი თანმიმდევრობა იწყება 33-ით). მაგალითად, ვთქვათ დასაშიფრი ტექსტია:

К А К Д Ы М О Т Е Ч Е С Т В А Н А М С Л А Д О К И П Р И Я Т Е Н .
1 2 3 4 5 . . . 10 . . . . 15 . . . . 20 . . . . 25 . . . . 30 . 32

რადგან ტექსტი შეიცავს 32 სიმბოლოს, ამიტომ ცხრილის ქვედა ნაწილის შევსებით მიიღება 3.17. ნახ-ზე ნაჩვენებია ცხრილი.

ნახ.3.17.

თუ წაკითხვა შესრულდება სტრიქონების მიხედვით ზემოდან ქვემოთ, მაშინ შიფრტექსტი იქნება:

КПАЛОНТДНСТИВАМЕРАА ЧЯДОСМЕИККЕТЫ.

3.3. შიფრი მარტივი შეცვლით (ჩასმით)

ასეთი შიფრის მისაღებად საჭიროა დასაშიფრი ტექსტის სიმბოლოების გარკვეული წესით შეცვლა იგივე ან სხვა ალფაბეტის სიმბოლოებით. ე.ი. შეტყობინება $M=m_1m_2m_3m_4...$ სადაც $m_1m_2m_3m_4...$ - სიმბოლოების მიმდევრობა, გადადის $E=e_1e_2e_3e_4...=f(m_1)\ f(m_2)\ f(m_3)\ f(m_4)$ კრიპტოგრამაში. ამასთან, f(m) ფუნქციას აქვს შექცეული ფუნქცია f(m).

ჩვენს წელთაღრიცხვამდე ორი საუკუნით ადრე ბერძენმა მწერალმა და ისტორიკოსმა მოლიბიმ დაშიფვრისათვის გამოიყენა ბერძნული ასოების შემთხვევითი თანმიმდევრობით შევსებული კვადრატული ცხრილი განზომილებით 5x5 (ნახ.3.18.).

λ	ε	υ	ω	γ
ρ	ζ	δ	σ	ο
μ	η	β	š	τ
ψ	π	θ	α	Χ
χ	V		φ	ι

ნახ. 3.18.

დაშიფვრისას ამ კვადრატში ეძებდნენ ღია ტექსტის მორიგ სიმბოლოს და შიფრტექსტში წერდნენ იმ ასოს, რომელიც მოთავსებული იყო ამ ასოს ქვემოთ იმავე სვეტში. თუ მოძებნილი სიმბოლო მოთავსებული იყო სვეტის ბოლოში, მაშინ იღებდნენ იგივე სვეტის ყველაზე ზედა ასოს.

მაგალითად, სიტყვისათვის ταυροσ მიიღება შიფრტექსტი χφδμτš.

ჩვენს წელთაღრიცხვამდე 50-იან წლებში გაიუს იულიუს ცეზარი და მარკუს ტულიუს ციცერონი ერთმანეთთან მიწერ-მოწერისას იყენებდნენ შიფრის მარტივი შეცვლით. დაშიფვრის ეს სიტემა ატარებს ცეზარის სახელს. ამ სისტემით საწყისი ტექსტის თითოეული ასო გარკვეული წესით იცვლება იმავე ალფაბეტის სხვა ასოთი. შემცვლელი ასო განისაზღვრება შესაცვლელი ასოს k პოზიციით გადადგილებისას ალფაბეტის გასწვრივ. ალფაბეტის ბოლოში გასვლისას ხდება ციკლური გადასვლა ალფაბეტის დასაწყისში. ცეზარმა გამოიყენა დაძვრა kx3. მაგალითად, ცეზარის დაშიფვრის სისტემით ინგლისური ალფაბეტის შემთხვევაში მიიღება 3.19. ნახ-ზე გამოსახული ცხრილი.

ნახ. 3.19.

ე.ი. დაშიფვრისას ღია ტექსტის n-გრამა ($x_0,x_1,x_2,.....,x_{n1}$) იცვლება შიფრტექსტის n-გრამითი ($y_0,y_1,y_2,.....,y_{n1}$) შემდეგი წესის გამოყენებით: ??

სადაც j არის ღია ტექსტის ასოს რიცხვითი კოდი; j+k - შრიფტექსტის ასოს რიცხვითი კოდს აკლდება k და მიიღება ღია ტექსტის ასოს რიცხვითი კოდი.

თუ t რიცხვითს შესაბამისი ასო შეიცვლება ასოთი, რომლის რიცხვითი კოდია (at+b) და მოდულით, ე.ი.

$E_{a,b}$ (t)=(at+b)(modn).

სადაც a,b - მთელი რიცხვებია, 0≤a, b<n, a და n რიცხვების უდიდესი საერთო გამყოფი (უსგ) ტოლია ერთის, მაშინ მიიღება დაშიფვრის სისტემა, რომელიც ცნობილია ცეზარის ჩასმების აფინური სისტემის სახელწოდებით.

მაგალითად, თუ n=26, a=3 და b=5, მაშინ ცხადია, რომ უსგ (3,26)=1 და მიიღება ასოების რიცხვით კოდებს შორის შემდეგი შესაბამისობა:

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
3t+5	5	8	11	14	17	20	23	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2

თუ ეს რიცხვები შეიცვლება ინგლისური ალფაბეტის ასოებით, მაშინ ღია და შიფრტექსტის ასოების შორის იქნება შემდეგი შესაბამისობა:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z	C

ღია ტექსტი HOPE შეიცვლება შიფრტექსტით AVYR.

გაშიფვრისას იფრტექსტის ასო მოიძებნება ცხრილის ქვედა სტრიქონში და იგი შეიცვლება ზედა სტრიქონში მოთავსებული ასოთი.

დაშიფვრის ცეზარის სისტემისა და სიტყვა-გასაღების გამოყენებით მიიღება ერთალფაბეტიანი ჩასმის სისტემა. შიფრის გასაღების როლს ასრულებს სიტყვა ან მოკლე ფრაზა (სასურველია რომ გასაღების ყველა ასო იყოს სხვადასხვა).

დაშიფვრის მეთოდიკა განვიხილოთ ინგლისური ალფაბეტისთვის. ვთქვათ, სიტყვა-გასღებია DIPLOMAT. ვარჩევთ რომელიღაც k=5 რიცხვს (0≤ k<25). სიტყვა-გასაღები იწერება ინგლისური ალფაბეტის ქვეშ დაწყებული იმ ასოდან, რომლის რიცხვითი კოდი ემთხვევა K მნიშვნელობას:

```
0 1 2 3 4 5 6        10             15          20            25
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z.
          D I P L O M A T
```

ალფაბეტის დანარჩენი ასოები, რომლებიც არ სედიან გასარებში, იწერება სიტყვა-გასაღების შემდეგ ალფაბეტის თანმიმდევრობით:

```
                5
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z.
V W X Y Z D I P L O M A T B C E F G H J K N Q R S U.
```

ღია ტექსტი: S E N D M O R E M O N E Y.

შიფრტექსტი: H Z B Y T C G Z T C B Z S.

თუ სიტყვა-გასაღები შეიცავს ერთნაირ ასოებს, მაშინ ესსიტყვა დაუწერება ალფაბეტის ქვეშ განმეორებადი ასოების გარეშე.

მაგალითად, თუ გასაღებია რუსული ფრაზა

КАК ДЫМ ОТЕЧЕСТВА НАМ СЛАДОК И ПРИЯТЕН და k=3, მაშინ მიიღება:

0 1 2 3
А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я
Ъ Э Ю К А Д Ы М О Т Е Ч С В Н Л И П Р Я Б Г Ж З Й У Ф Х Ц Ш Щ Ь

ღია ტექსტი: ПРИЛЕТАЮ ВОСЬМОГО.

შიფრტექსტი: ЛИОЧДРЪЩ ЮНПФСНКН.

ცეზარის დაშიფვრის სამივე მეთოდის გამოყენებით დავშიფროთ ქართული ფრაზა «შენი ცოდნა შენსა ქვეყანას გამოადგება“.

- K პოზიციით გადაადგილდება ალფაბეტისგასწვრივ. თუ K=3, მაშინ ალფაბეტის გარდაქმნილი ცხრილი იქნება.

ნახ.3.20.

შ ე ნ ი ც ო დ ნ ა შ ე ნ ს ა ქ ვ ე ყ ა ნ ა ს გ ა მ ო ა დ გ ე ბ ა.
ძ თ ჟ მ ჭ რ ზ ჟ დ ძ თ ჟ ფ დ შ ით ც დ ჟ დ ფ ვ დ პ რ დ ზ ვ თ ე დ.

- ჩასმები აფინური სისტემა.

?????? და b=3 ცხადია, რომ უსგ (5,33)=1. ღია და შიფრტექსტის ასოებს შორის იქნება შემდგეი შესაბამისობა:

	ა	ბ	გ	დ	ე	ვ	ზ	თ	ი	კ	ლ	მ	ნ	ო	პ	ჟ	რ	ს	ტ	უ	ფ	ქ	ღ	ყ	შ	ჩ	ც	ძ	წ	ჭ	ხ	ჯ	ჰ
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
	1	8	13	18	23	28	0	5	10	15	20	25	30	2	7	12	17	22	27	32	4	9	14	19	24	29	1	6	11	16	21	26	31
			ო	ტ	ყ	წ	ა	ვ	ლ	ჟ	ფ	ჩ	ხ	გ	თ	ნ	ს	ღ	ძ	პ	ე	კ	პ	უ	შ	ჭ	ბ	ზ	მ	რ	ქ	ც	ჯ

შ ე ნ ი ც ო დ ნ ა შ ე ნ ს ა ქ ვ ე ყ ა ნ ა ს გ ა მ ო ა დ გ ე ბ ა.
შ ყ ხ ლ ბ გ ტ ხ დ შ ყ ხ ღ დ კ წ ყ უ დ ხ დ ღ ო დ ჩ გ დ ტ ო ყ ი დ.

- ერთალფაბეტიანი ჩასმის სისტემა.

k=6 და სიტყვა-გასაღები კონიუნქცია.

0 1 2 3 4 5 6
ა ბ გ დ ე ვ ზ თ ი კ ლ მ ნ ო პ ჟ რ ს ტ უ ფ ქ ღ ყ შ ჩ ც ძ წ ჭ ხ ჯ ჰ,
კ წ ჭ ხ ჯ ჰ კ ო ნ ი უ ქ ც ა ბ გ დ ე ვ ზ თ ლ მ პ ჟ რ ს ტ ფ ღ ყ შ ჩ;

შ ე ნ ი ც ო დ ნ ა შ ე ნ ს ა ქ ვ ე ყ ა ნ ა ს გ ა მ ო ა დ გ ე ბ ა.
ჟ ჯ ც ნ ს ა ხ ც ე ჟ ჯ ც ე ძ ლ ჰ ჯ პ ძ ც ძ ე ჭ ძ ქ ა ძ ხ ჭ ჯ წ ძ.

1508 წელს გერმანელმა აბატმა იოჰან ტრისემუსმა გამოაქვეყნა ნაშრომი კრიპტოლოგიში სახელწოდებით „პოლიგრაფია“. ამ ნაშრომში მან აღწერა ალფაბეტში შემავალი ასოების შემთხვევითი თანმიმდევრობით შევსებული ცხრილების გამოყენება ღია ტექსტის დასაშიფრად. შიფრის მისარებად მან გამოიყენა ცხრილი, რომელშიც თავდაპირველად (პირველი სტრიქონიდან) დაწყებული) იწერება სიტყვა-გასაღები განმეორებადი ასოების გარეშე, ხოლო ხოლო შემდეგ ცხრილის დარჩენილი თავისუფალი უჯრები ივსება ალფაბეტის იმ ასოებით (თანმიმდევრულად), რომლებიც სიტყვა-გასაღებში არ მონაწილეობენ.

დაშიფრვის ამ მეთოდის ასხსნელად განვიხილოთ რუსული ალფაბეტის შესაბამისი ცხრილი 4x8 და სიტყვა-გასაღებად ავიღოთ სიტყვა БАНДЕРОЛЬ (ნახ.3.21.).

Б	А	Н	Д	Е	Р	О	Л
Ь	В	Г	Ж	З	И	Й	К
М	П	С	Т	У	Ф	Х	Ц
Ч	Ш	Щ	Ы	Ъ	Э	Ю	Я

ნახ. 3.21.

ღია ტექსტში შემავალი ასო იცვლება იმ ასოთი, რომელიც მოთავსებულია შესაცვლელი ასოს ქვემოთ იმავე სვეტში. თუ შესაცველი ასო მდებარეობს სვეტის ბოლოში, მაშინ აიღება იმავე სვეტის დასაწყისში მოთავსებული ასო.

ღია ტექსტი: В Ы Л Е Т А Е М П Я Т О Г О.
შიფრტექსტი: П Д К З Ы В З Ч Ш Л Ы Й С Й

პოლიბის, ცეზარის და ტრისემუსის შიფრები მიეკუთვნებიან მონოალფაბეტურ შიფრებს. ეს შიფრები გამოირჩევიან დაბალი კრიპტომედეგობით. კრიპტოანალიტიკოსი ამ შიფრების გასახსნელად იყენებს ინფორმაციას იმ დამახასიათებელი ნიშანთვისებების შესახებ, რომლებითაც ხასიათდებიან ამა თუ იმ ალფაბეტის ასოებით შედგენილი ტექსტები. კერძოდ, თუ სეტყობინება გრძელია, მაშინ გამოიყენება ტექსტში სხვადსხვა ასოების გამოჩენის სიხშირეების განსაზღვრის მეთოდი და ამ სიხშირეების შედარება შესაბამის ენაზე შესრულებულ ტექსტებში ასოების გამოჩენის ფარდობით სიხშირესთან. 3.22 ნახ-ზე ნაჩვენებია ასოების გამოჩენის ფარდობითი სიხშირეების მნიშვნელობები (საშუალო სტატისტიკური) ინგლისური ალფაბეტისათვის.

ნახ.3.22.

რადგან მონოალფაბეტურ შიფრებში თითოეული ასო იცვლება ერთი და იგივე შესაბამისი ასოთი, ამიტომ სტატისტიკური მონაცმების ცოდნით ადვილად შეიძლება ამ შიფრების გახსნა და საწყისი ტექსტის სტრუქტურის დადგენა.

ამ ნაკლის აღმოსაფხვრელად საჭირო გახდა ისეთი შიფრების შექმნა, რომლებშიც გამოიყენება არა ცალკეული ასოს შეცვლა შესაბამისი ასოთი, არამედ რამდენიმე ასოს კომბინაციების შეცვლა შესაბამისი ასოების კომბინაციით ან დაშიფვრისას რამდენიმე ალფაბეტის ერთდროულად გამოყენება (n-გრამა შიფრი).

ტრისემუსმა აღმოაჩინა, რომ მის მიერ გამოყენებულ დამშიფრავი ცხრილითშესაძლებელია ორ-ორი ასოს დაშიფვრა.

1854 წელს პლეიფეირმა განავითარა ტრისემუსის აღმოჩენა და შეადგინა შიფრი ოორი ასოს დაშიფვრით. ეს სიფრი ცნობილია პლეიფეირის ბიგრამული შიფრის სახელწოდებით. ამ შიფრს იყენებდა ინგლისი პირველი მსოფლიო ომის მსვლელობისსას. დამშიფრავი ცხრილი ტრისემუსის ცხრილის ანალოგიური. დაშიფვრის პროცესი მიმდინარეობს შემდეგნაირად:

1. ღია ტექსტი, რომელიც აუცილებლად უნდა შეიცავდეს ლუწი რაოდენობის ასოს, იყოფა ორ-ორ სიმბოლოდ (ბიგრამებად). ამასთან, თითოეული ბიგრამა უნდა შეიცავდეს განსხვავებულ ასოებს. თუ ეს მოთხოვნა

არ კმაყოფილდება, მაშინ ხდება ღია ტექსტის მოდიფიცირება უმნიშვნელო ორთოგრაფიული შეცდომების დაშვებით.

2. ღია ტექსტის ბიგრამების მიმდევრობა დამშიფრავი ცხრილის მეშვეობით იშიფრება შიფრტექსტის ბიგრამებად შემდეგი წესის გამოყენებით (ნახ. 3.21):

ა) თუ ღია ტექსტის ბიგრამში შემავალი ორივე ასო არ მდებარეობს ერთ სტრიქონში ან ერთ სვეტში (მაგ. ასოები А და Й), მაშინ აიღება ის ასოები, რომლებიც ღია ტექსტის ასოებთან ერთად ადგენენ მართკუთხედს (АЙ ასოების წყვილი აისახება ОВ წყვილში, ЕТ ДУ-ში, ЕС НУ-ში, ТЯ ЦЫ-ში და ა.შ.). ღია და შიფრტექსტის შესაბამისი ბიგრიმები იწყება ერთი და იგივე სტრიქონის ასოებით;

ბ) თუ ღია ტექსტის ბიგრამაში შემავალი ორივე ასო მიეკუთვნება ცხრილის ერთ სვეტს, მაშინ ????? იმავე სვეტში და ამ ასოების ქვემოთ მოტავსებული ასოები. თუ შესაცვლელი ასო მდებარეობს ქვედა ბოლო სტრიქონში, მაშინ აიღება იმავე სვეტის ზედა (პირველ) სტრიქონში მოთავსებული ასო (НС წყვილი აისახება ГЩ-ში, ВШ ПА-ში, ЖТ ТЫ-ში, МЧ ЧБ-ში და ა.შ.).

გ) თუ ღია ტექსტის ბიგრამაში შემავალი ასოები მიეკუთვნება ერთ სტრიქონს, მაშინ შიფრტექსტის ბიგრამაში აიღება მათ მარჯვნივ მდებარე ასოები. თუ შესაცვლელიასო მდებარეობს განაპირა მარჯვენა სვეტში, მაშინ აიღება იმავე სტრიქონის, ოღონდ განაპირა მარცხენა სვეტში მოთავსებული ასო (ВИ წყვილი აისახება ГЙ-ში, ТУ УФ-ში, АЛ НБ-ში და ა.შ.).

განვიხილოთ მაგალითი, ვთქვათ, ღია ტექსტია:

ВСЕ ТАЙНОЕ СТАНЕТ ЯВНЫМ.

ბიგრამებად დაყოფის შემდეგ მიიღება:

ВС ЕТ АЙ НО ЕС ТА НЕ ТЯ ВН ЫМ.

შიფრტექსტის შესაბამისი ბიგრამები იქნება:

ГП ДУ ОВ ДЛ НУ ПД ДР ЦЫ ГА ЧТ.

პელიფერის მეთოდით დაშიფვრისას გამოიყენება აგრეთვე 25 ასოს შემცველი ინგლისური ალფაბეტის ნებისმიერი გადანაცვლებით შევსებული 5x5 კვადრატული ცხრილი (ასო j გამოტოვებულია და თუ ეს ასო მონაწილეობს ღია ტექსტში, მაშინ იგი შეიცვლება i-ით). ცხრილში ასოების განლაგება წარმოადგენს გასაღებს.

L	Z	Q	C	P
A	G	N	O	U
R	D	M	I	F
K	Y	H	V	S
X	B	T	E	W.

ამ ცხრილის მიხედვით, მაგალითად, АС წყვილი აისახება OL-ში, QM-NH-ში, YB- BZ-ში, EW-WX-ში, DI-MF-ში.

ამ ცხრილის სტრიქონებისა და სვეტების დანომვრით შესაძლებელია ასოების გადაყვანა ორნიშნა რიცხვში.

	0	1	2	3	4
0	L	Z	Q	C	P
1	A	G	N	O	U

2	R	D	M	I	F
3	K	Y	H	V	S
4	X	B	T	E	W.

ამ შემთხვაში, მაგალითად, B ასოს შეესაბამება 41 ან 14 და B Q წყვილი გამოისახება 41 02 ან 14 20-ით.

1854 წელს ინგლისელმა ჩარლზ უიტსტონმა დაამუშავა ბიგრამების დაშიფვრისახალი მეთოდი. ამ მეთოდით მიღებული შიფრი ცნობილია სახელწოდებით უიტსტონის შიფრი „ორმაგი კვადრატი“. ეს შიფრი გამოიყენებოდა გერმანიაში მეორე მსოფლიო ომის დროს.

И	Ч	Г	Я	Т
,	Ж	Ь	М	О
З	Ю	Р	В	Щ
Ц	:	П	Е	Л
Ъ	А	Н	.	Х
Э	К	С	Ш	Д
Б	Ф	У	Ы	Й

შიფრის მისაღებად აიღება ერთ ჰორიზონტალზე განლაგებული ორი ცხრილი შევსებული ერთი და იგივე ალფაბეტის სიმბოლოების შემთხვევითი განლაგებით (ნახ. 3.23).

Ж	Щ	Н	Ю	Р
И	Т	Ь	Ц	Б
Я	М	Е	.	С
В	Ы	П	Ч	Й
:	Д	У	О	К
З	Э	Ф	Г	Ш
Х	А	,	Л	Ъ
Е	?	Р	Y	Н
О	J	G	Z	С
К	В	R	N	.
Х	W	L	,	F
М	I	V	D	Q
Т	U	А	:	S
V	Т	W	L	F
S	D	.	М	Х
I	Z	А	:	U
N	Q	Y	С	J
В	О	?	G	R
Н	,	Е	Р	К

ბ	ც	ფ	ლ	ჩ
ქ	თ	წ	ჟ	ე
მ	შ	ა	ძ	ო
ვ	ჭ	ტ	ნ	ყ
რ	პ	ჰ	დ	ჯ
ზ	ღ	ი	ხ	ს
,	კ	.	ზ	უ
დ	ძ	პ	ღ	ზ
ხ	ს	ბ	ჭ	რ
ჯ	ვ	ჰ	ი	მ
უ	.	კ	,	ბ
ო	ე	წ	ფ	ქ
ჩ	ჟ	თ	ც	ტ
ლ	შ	ნ	ა	ყ

ნახ. 3.23.

დაშიფვრის წინ ღია ტექსტი იყოფა ბიგრამებად. შესაცვლელ ბიგრამაში შემავალი პირველი ასო მოიძებნება მარცხენა ცხრილში, ხოლო მეორე ასო - მარჯვენა ცხრილში . დაშიფვრა მიმდინარეობს შემდეგნაირად:

1) თუ ღია ტექსტის ბიგრამაში შემავალი ასოები მოთავსებულია სხვადსხვა სტრიქონში, მაშინ მათზე აზრობრივად აიგება მართკუთხედი და შიფრტექსტის ასოებად აიღება ის ასოები, რომლებიც მდებარეობენ ამ მართხკუთხედის წვერეობზე პლეიფეირის მეთოდით (ИЛ წყვილი აისახება ОВ-ში, МЕ ВЫ-ში, ДЯ Щ-ში,МК ЮЭ-ში და ა.შ.).

2) თუ ღია ტექსტის ბიგრამაში შემავალი ასოები მდებარეობენ ერთ სტრიქონში, მაშინ შიფრტექსტის ასოები აიღება იმავე სტრიქონიდან. კერძოდ, პირველი ასო აიღება მარცხენა ცხრილის იმ სვეტიდან, რომელიც შეესაბამება შესაცვლელ ბიგრამაში შემავალ მეორე ასოს, ხოლო მეორე ასო აიღება მარჯვენა ცხრილის იმ სვეტიდან, რომელიც შეესაბამება შესაცვლელ ბიგრამაში შემავალ პირველ ასოს (ТО წყვილი აისახება БЖ-ში,МВ Ю-ში, ЭШ ГК-ში და ა.შ.).

3) თუ ღია ტექსტის ბიგრამაში შემავალი ასოები მდებარეობენ ერთ სტრიქონში და ერთ სვეტში, მაშინ შიფრტექსტის ბიოგრამა იგივე დარჩება.

განვიხილოთ მაგალითი, ვთქვათ, ღია ტექსტია:

ВСЕ ТАЙНОЕ СТАНЕТ ЯВНЫМ.

ბიგრამებად დაყოფის შემდეგ მიიღება:

ВС ЕТ АЙ НО ЕС ТА НЕ ТЯ ВН ЫМ.

შიფრტექსტის შესაბამისი ბიგრამები იქნება:

ПЗ ЩН ЪФ ТЬ РФ ЖД ЯП МЩ П: ЕТ.

ცეზარის შიფრის მოდიფიკაციას წარმოადგენს გრონსფილდის შიფრი. გასაღების როლს ამ შიფრში ასრულებს რიცხვი. დასაშიფრი შეტყობინების ქვეშ იწერება რიცხვითი გასაღების ციფრები. თუ გასაღები შეტყობინებაზე მოკლეა, მაშინ გასაღების ჩანაწერი ციკლურად ?????????? შიფრტექსტი მიიღება თითქმის ისე, როგორც ცეზარის შიფრში, ოღონდ შემცვლელი ასო აიღება ალფაბეტიდან არა მესამე ასო, არამედ ის ასო, რომელიც დაძრულია შესაცვლელი ????? მის ქვემოთ დაწერილი ციფრის შესაბამისად. მაგალითად, თუ გასაღებად აღებულია რიცხვი 2718 (ნეპერის e რიცხვის პირველი ოთხი ციფრი) და დასაშიფრი შეტყობინებაა ВОСТОЧНЫЙ ЕКСПРЕСС, მაშინ შიფრტექსტი მიიღება შემდგენაირად:

რუსული ალფაბეტი

??

А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я.

შეტყობინება: В О С Т О Ч Н Ы Й Е К С П Р Е С С.

გასაღები: 2 7 1 8 2 8 1 8 2 7 1 8 2 8.

შიფრტექსტი: Д Х Т Ь Р Ю Ю Г Л Д Л Щ С Ч Ж Щ У.

· ვიჟინერის დაშიფვრის სისტემა

დაშიფვრის ეს სისტემა გამოქვეყნდა ფრანგი დიპლომატის ვიჟინერის მიერ 1586 წელს და იგი მრავალალფაბეტიანი სისტემაა.

ვიჟინერმა შეადგინა ცხრილი, რომელიც გამოიყენა დაშიფვრის და გაშიფვრის განსახორციელებლად. 3.24 და 3.25 ნახაზებზე მოცემულია ვიჟინერის ცხრილები, შესაბამისად, ???????? და ინგლისური ალფაბეტისათვის.

ნახ. 3.24

ნახ. 3.25

ცხრილს აქვს ორი შესასვლელი. ცხრილის ზედა სტრიფონში განლაგებული ხაზგასმული ასოების ღია ტექსტის ასოებია, ხოლო მარცხენა სვეტში განლაგებული ასოები - გასაღების ასოები.

დაშიფვრისას სტრიქონში დაწერილ საწყისს შეტყობინებას ქვეშ მიეწერება სიტყვა-გასაღები განმეორებით. შიფრტექსტის ასოს მისარებად აიღება შეტყობინების ასოსა და მის ქვემოთ დაწერილი გასაღების ასოს გადაკვეთაზე მოთავსებული ასო. ე.ი. k=(i+j)modm, სადაც k,i,j შესაბამისად, შიფრტექსტის, ღია ტექსტის და გასაღების ასოებია, ხოლო (f) ალფაბეტში შემავალი ასოების რაოდენობა.

განვიხილოთ მაგალითი. ვთქვათ, გასაღებად არებული სიტყვაა АМБРОЗИЯ და დასაშიფრი შეტყობინებაა ПРИЛЕТАЮ СЕДЬМОГО. ე.ი. გვექნება:

შეტყობინება: П Р И Л Е Т А Ю С Е Д Ь М О Г О

გასაღები: А М Б Р О З И Я А М Б Р О З И Я

შიფრტექსტი: П Ъ ЙЫ УЩ И Э С С Е К Ь Х Л Н

ვიჟინერის ცხრილიდან გამომდინარეობს დაშიფვრის და გაშიფვრის გამარტივებული ალგორითმები. კერძოდ, თუ I,j და k წარმოადგენენ, შესაბამისად, ღია ტექსტს, სიტყვა-გასაღებისთვის და შიფრტექსტის ასოების სტანდარტულ ნომრებს ალფაბეტის მიხედვით, მაშინ დაშიფვრისას შიფრტექსტის ასოს ნომერი გამოითვლება შემდეგნაირად: k=i+j, როცა m>i+j და k=(+)·m, როცა m≤i+j, სადაც m ალფაბეტში შემავალი ასოების რაოდენობაა.

გაშიფვრისას ღია ტექსტის ასოს სტანდარტული ნომერი გამოითვლება შემდგენაირად: i=k+j, როცა k>j და i=k-j+m, როცა k<j.

ზემოთ განხილული მაგალითისათვის გვექნება:

დაშიფვრა

	15 16 08 11 05 18 00 30 17 05 04 26 12 14 03 14
ღია ტექსტი (i):	П Р И Л Е Т А Ю С Е Д Ь М О Г О
	00 12 01 16 14 07 08 31 00 12 01 16 14 07 08 31
გასაღები (j):	А М Б Р О З И Я А М Б Р О З И Я
	15 28 09 27 19 25 08 29 17 17 05 10 26 21 11 13
შიფრტექსტი(k):	П Ъ Й Ы У Щ И Э С С Е К Ь Х Л Н

გაშიფვრა

	15 28 09 27 19 25 08 29 17 17 05 10 26 21 11 13
შიფრტექსტი(k):	П Ъ Й Ы У Щ И Э С С Е К Ь Х Л Н
	00 12 01 16 14 07 08 31 00 12 01 16 14 07 08 31
გასაღები (j):	А М Б Р О З И Я А М Б Р О З И Я
	15 16 08 11 05 18 00 30 17 05 04 26 12 14 03 14
ღია ტექსტი (i):	П Р И Л Е Т А Ю С Е Д Ь М О Г О

ამ ალგორითმის გამოყენებით შესაძლებელია შიფრტექსტის გაგზავნა რიცხვების სახით. ПЪЙЫУЩИЭССЕКЬХЛН 15280927170510262111113

ზოგჯერ გამოიყენება თანამედროვე დაშიფრვა მარტივი შეცვლით და შემდეგ დაშიფრვა ვიჟინერის მეთოდით ან პირიქით.

თუ ვიჟინერის მეთოდით დაშიფრვისას ნამდვილ გასაღებს გამოვიყენებთ მხოლოდ ერთხელ, ხოლო შემდეგ გასაღების როლს შევასრულებინებთ ღია ტექსტს ან კრიპტოგრამას, მაშინ მიიღება შრიფტი ავტოგასაღებით.

მაგალითად, ვთქვათ, გასაღებია COMET და შეტყობინება SENDSUPPLIES…., მაშინ შეტყობინების (ღია ტექსტის) გასაღებად გამოყენების შემთხვევაში მიიღება:

შეტყობინება:	S E N D S U P P L I E S….,
გასაღები:	C O M E T S E N D SU P…..
კრიპტოგრამა:	U S Z H LMT C O A Y H….

ხოლო კრიპტოგრამის გასაღებად გამოყენების შემთხვევაში კი:

შეტყობინება:	S E N D S U P P L I E S….,
გასაღები:	C O M E T U S Z H LO H…..
კრიპტოგრამა:	U S Z H L O H O S T T S….

დაშიფრვისა და გაშიფრვის პროცესებიდ გასამარტივებლად გამოიყენება სპეციალური დამშიფრავი სახაზავი. სახაზავი შედგება მოძრავი და უძრავი ნაწილებისგან (ნახ. 3.26.).

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ

უძრავი ნაწილი საწყისი ალფაბეტი მოძრავი ნაწილი

ნახ. 3.26

გასაღების ასო, რომელიც მდებარეობს მოძრავ ნაწილზე, მოძრავი ნაწილის გადაადგილებით შეუთავსდება უძრავ ნაწილზე მოთავსებულ A ასოს და უძრავ ნაწილზე მოთავსებულ დასაშიფრი ტექსტის ასოს თავზე, მოძრავ ნაწილზე წაიკითხება შრიფტექსტის შესაბამისი სიმბოლო.

ვიჟინერის ცხრილის გამოყენებით შესაძლებელია დაშიფრვის განხორციელება სხვა მეთოდით, ნულოვან სტრიქონში მოთავსებული ღია ტექსტის X_i სიმბოლო იცვლება მის ქვემოთ i-ურ სტრიქონში მოთავსებული სიმბოლოთი (i=1,2,3…). მაგალითად, თუ საწყისი ტექსტია NOW IS THE TIME, მაშინ მიიღება:

	1	2	3	4	5	6	7	8	9	10	11	12
შაწყისი ტექსტი:	N	O	W	I	S	T	H	E	T	I	M	E
შიფრტექსტი:	O	Q	Z	M	X	Z	O	M	C	S	X	Q.

ამ მეთოდს ეწოდება ტრისემუსის პროგრესული გასაღების გამოყენების მეთოდი. თუ ამ შემთხვევაში ღია ტექსტში შემავალ ასოს რიგითი ნომერის ტექსტის მიხედვით არის i ხოლო ალფაბეტის მიხედვით χ ,მაშინ შრიფტექსტის შესაბამისი ასოს ნომერი ალფაბეტის მიხედვით იქნება (i+j)modm. Gანხილულ მაგალითში ღია ტექსტის T ასოს რიგითი ნომერი ტექსტის მიხედვით არის 9, ხოლო ალფაბეტის მიხედვით 19. ამიტომ შრიფტექსტში შემავალი შესაბამისი ასოს რიგითი ნომერი ალფაბეტის მიხედვით იქნება (9+19)modm26=2. ე.ი. საძებნი ასოა C.

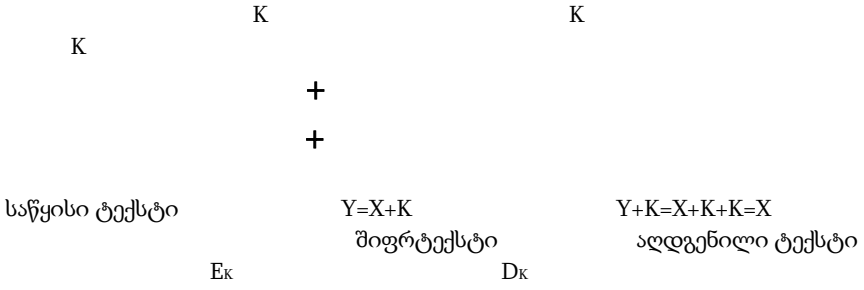
გაშიფრვის შემთხვევაში შრიფტექსტში შემავალი ასოს რიგით ნომერს ალფაბეტის მიხედვით აკლდება იგივე ასოს რიგითი ნომერი შრიფტექსტის მიხედვით და მიიღება ღია ტექსტის ასო ალფაბეტის მიხედვით. ე.ი. (j+i)modm შრიფტში შემავალი C-ს ნომერია ალფაბეტის მიხედვით 2, ხოლო შრიფტექსტის მიხედვით 9, ამიტომ ღია ტექსტში შემავალი შესაბამისი ასოს ნომერი ალფაბეტის მიხედვით იქნება (2-9)mod26=7mod26=19mod26. ე.ი. მიიღება 19, რომელსაც შეესაბამება ასო T.

3.5. დაშიფრვის ვერნამის მეთოდი

ჟილბერტ ვერნამმა 1926 წელს გამოაქვეყნა დაშიფრვის მეთოდი, რომელშიც გამოიყენებოდა ინგლისური ალფაბეტის ასოების და ექვსი დამხმარე სიმბოლოს წარმოდგენა ?????? ორობითი სიმბოლოების სახით (ბოდის კოდი). დაშიფრვისას ორობითი კოდური კომბინაციის სახით წარმოდგენილი ღია ტექსტი ორის მოდულით იკრიბება გასაღების შესაბამის ორობით კოდურ კომბინაციასთან. გაშიფრვისას მიღებულ χამს ემატება ორის მიხედვით გასაღების შესაბამისი იგივე კოდური კომბინაცია და მიიღება საწყისი ტექსტი.

დაშიფრვისა და გაშიფრვის სქემა ნაჩვენებია 3.27 ნახ-ზე.

K გასაღების მიმდევრობა



ნახ.3.27

თუ დასაშიფრია მაგალითად ასო A=10001 და გასაღებია 01100 მაშინ დაშიფრული კომბინაცია იქნება 10001 ????01100=11101.

გაშიფრვის შედეგად მიიღება: 11101+01100=10001.

ვერნამის დაშიფრვის სქემაში გამოიყენება გასაღების ციკლური განმეორება (რგოლური ლენტი) მაგალითად, თუ დასაშიფრია D35B7H-ის შესაბამისი ორობითი კომბინაცია 00100101101 გასაღებით, მაშინ:

1 1 0 1 0 0 1 1 0 1 0 1 1 0 1 1 0 1 1 1
1 1 0 1 0 0 1 0 1 1 0 1 1 1 0 1 0 0 1 0
0 0 0 0 0 0 0 1 1 0 0 0 0 1 1 0 0 1 0 1.

გაშიფვრის შედეგად მიიღება:

0 0 0 0 0 0 0 0 1 1 0 0 0 0 1 1 0 0 1 0 1.
1 1 0 1 0 0 1 0 1 1 0 1 1 1 0 1 0 0 1 0
1 1 0 1 0 0 1 1 0 1 0 1 1 0 1 1 0 1 1 1.

ცხადია, რომ ვერნამის მეთოდით დაშიფრული ტექსტი მით უფრო კრიპტომედეგია, რაც უფრო გრძელია გასაღები (ე.ი. რაც უფრო დიდია გასაღების გამეორების პერიოდი), რადგან მოკლე გასაღების შემთხვევაში, შრიფტექსტის გრძელი ფრაგმენტისა და ღია ტექსტის ცალკეული ფრაგმენტების ცოდნით კრიპტოანალიტიკოსს შეუძლია შიფრის გახსნა.

ჟოზეფ მობრნმა განავითარა ვერნამის მეთოდი შეტყობინების სიგრძის ტოლი გასაღების შემოტანით. ე.ი. ამ შემთხვევაში გამოიყენება გასაღების ერთჯერადი ლენტი, რომელიც მიიღება შემთხვევითი რიცხვების გენერატორის მეშვეობით. ასეთი შიფრის გახსნა შეუძლებელია, რადგან შრიფქტესტი არ იძლევა არავითარ ინფორმაციას ღია ტექსტის შესახებ. ამ მეთოდის ნაკლს წარმოადგენს ის, რომ გადამცემ და მიმღებ მხარეებს უნდა გააჩნდეთ ერთი და იგივე სიგრძის შემთხვევითი გასაღების მაფორმირებელი გენერატორები, რისი განხორციელებაც პრაქტიკულად შეუძლებელია.

3.6. მრავალალფაბეტიანი შიფრი

მრავალალფაბეტიანი შიფრი, რომლის ავტორია კრიფტოგრაფიის მეცნოიერების ფუძემდებელი ლეონ ალბერტი, წარმოადგენს შიფრს რთული შეცვლით. ასეთ შიფრში საწყისი შეტყობინების თითოეული სიმბოლოს

დასაშიფრად გამოიყენება შიფრი მარტივი შეცვლით და თანაც გამოყენებული ალფაბეტი იცვლება თანმიმდევრულად და ციკლურად.

თუ მოცემულია r რაოდენობის ალფაბეტი, ($B_0,B_1….B_{r-1}$) მაშინ საწყისი შეტყობინების X_0 სიმბოლო იცვლება B_0 ალფაბეტის Y_0 სიმბოლოთი, X_1-B_1 ალფაბეტის Y_1 სიმბოლოთი და ა.შ. X_{r-1}– B_{r-1} ალფაბეტის $_{r-1}$ სიმბოლოთი, X_r -B_r ალფაბეტის $_r$, სიმბოლოთი და ა.შ. თუ r=4, მაშინ დასაშიფრ სქემას ექნება 3.28 ნახ.-ზე ნაჩვენები სახე.

საწყისი ტექსტის სიმბოლო X_0 X_1 X_2 X_3 X_4 X_5 X_6 X_7 X_8 X_9 X_{10}

B_0 B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8 B_9 B_{10}

შემცვლელი სიმბოლო

ასეთი დაშიფრვისას საწყისი ალფაბეტის კონკრეტული სიმბოლო შეიძლება შეიცვალოს დამშიფრავი ალფაბეტის სხვადასხვა სიმბოლოებით.

მრავალალფაბეტიანი შიფრის გამოყენების ეფექტურობა იმაში მდგომარეობს, რომ იგი უზრუნველყოფს საწყისი ენის ბუნებრივი სტატისტიკის შენიღბვას. Mრავალალფაბეტიანი შიფრის მიღება შეიძლება, აგრეთვე, იმ შემთხვევაში, თუ საწყისი ალფაბეტის ყოველი სიმბოლოსთვის შეიქმნება გარკვეული სიმბოლოებისაგან შედგენილი M სიმრავლე, ასეთი შიფრისთვის საწყისი ალფაბეტის განსხვავებული სიმბოლოების ($\alpha\neq\beta$) შესაბამისმა სიმრავლეებმა უნდა დააკმაყოფილოს შემდეგი პირობა $M\alpha \cap M\beta=ø$.

M სიმრავლის შექმნა შეიძლება: რიცხვებისგან, სხვადასხვა ალფაბეტში შემავალი სიმბოლოებისგან, სასვენი ნიშნებისგან, მათემატიკური ოპერაციების აღმნიშვნელი სიმბოლოებისგან და სხვ.

მაგალითად, თუ M სიმრავლეები წარმოადგენენ 3.29 და 3.30 ნახაზებზე ნაჩვენებ ცხრილებს.

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
21	37	20	13	14	22	59	25	01	24	75	35	62	43	19	73
40	26	52	39	63	47	07	49	31	83	33	60	88	85	58	30
10	03	89	67	71	82	93	76	15	70	18	84	11	51	87	55

Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я
46	23	29	06	12	08	65	74	97	53	48	96	36	28	04	16
69	91	80	50	72	32	34	17	77	68	56	09	78	64	44	41
90	69	66	81	38	61	92	42	54	98	79	27	86	05	45	57

ნახ. 3.29

A	B	C	D	E	F	G	H	I	J	K	L	M
1	?	#	$	3	&	·	(	)	*	+	7	-
99	/	:	;	=	<	>	?	@	8	\	]	^
{	|	}	~	?	2	:	§	©	1	9		

N	O	P	Q	R	S	T	U	V	W	X	Y	Z

+ µ 23 . ® 5 □ % [11 « ¬
Œ Ž » § ¿ € † ¢ ä ¾ © ¥
B Æ „ Ô à ‰ Ŝ ¬ i 32 , ¶

ნახ. 3.30

ხოლო დასაშიფრი ტექსტებია: ОРГАНИЧЕСКИЙ ДИЭЛЕКТРИК და ORGANIC HISULATOR, მაშინ შესაბამისი შრიფტექსტების სახეობები იქნება:

1 О Р Г А Н И Ч Е С К И Й Д И Э Л Е К Т Р И К
1.1 19 46 13 21 43 01 74 22 23 75 31 24 14 15 28 35 47 33 29 46 31 18
1.2 87 02 67 10 85 31 42 22 91 18 01 83 71 15 64 84 82 33 80 90 15 75
1.3 88 90 39 40 81 15 17 47 69 33 15 70 63 31 05 60 82 75 66 02 01 18

2. O R G A N I C H I S U L A T O R
2.1 + . , ! °) #) ° ® □ 7 ! 5 ± .
2.2 § > 99 ‡ @ : @ ‡ ¿ †] 99 € Œ §

3.7 დაშიფრვის ჰილის მეთოდი

დაშიფრვის ეს მეთოდი დამუშავებულია ლესტერ ჰილის მიერ 1929 წელს. დაშიფრვის ალგორითმი შემდეგში მდებარეობს:

თუ საიდუმლო Z გასაღები წარმოადგენს nxn განზომილების მქონე K მატრიცას, ხოლო დასაშიფრი ღია ტექსტი –n სიგრძის P ვექტორს, მაშინ m რაოდენობის სიმბოლოს შემცველი ალფაბეტისათვის n განზომილების მქონე შრიფტექსტის C ვექტორის ელემენტები გამოითვლება $C_j=(Kij\cdot Pj) \mathrm{mod} m$ გამოსახულების გამოყენებით.

მაგალითად, თუ n=3 და

K= P=

მაშინ

C=

სადაც

$$C_1=(K_{11}P_1+K_{12}P_2+K_{13}P_3) \mathrm{mod} m$$
$$C_2=(K_{21}P_1+K_{22}P_2+K_{23}P_3) \mathrm{mod} m$$
$$C_3=(K_{31}P_1+K_{32}P_2+K_{33}P_3) \mathrm{mod} m$$

გაშიფრვის დროს შრიფტექსტის C ვექტორი მრავლდება K მატრიცის შებრუნებულ K^{-1} მატრიცაზე ე.ი.

$$C\cdot K^{-1}=K\cdot P\cdot K^{-1}=EP=P,$$

სადაც E ერთეულოვანი მატრიცაა.

შებრუნებული K^{-1} მატრიცა გამოითვლება (თუ K მატრიცა არაგანსაკუთრებულია, ე.ი. მისი დეტერმინანტი ნულისაგან განსხვავებულია) შემდეგნაირად:

$$K^{-1}=[K^{-1}]=(-1)^{i+j}(Mij)/\det(K),$$

სადაც $(-1)^{i+j}M_{ij}$ ალგებრული დამატებაა, det(K)- მატრიცის დეტერმინანტი, ხოლო M_{ij} – მინორი, რომელიც შეიცავს K მატრიცის ელემენტებს i სტრიქონისა და j სვეტის გარეშე.

განვიხილოთ მაგალითი, ვთქვათ, დასაშიფრია ინგლისურენოვანი ტექსტის (m=26) სამი ასო PAY. ამ ასოების რიგითი ნომრები ინგლისური ალფაბეტის მიხედვით, შესაბამისად ტოლია 15, 0 და 24 რიცხვების ე.ი.

P=

თუ

K=

მაშინ:

$$C_1=(17\cdot15+17\cdot0+5\cdot24)\bmod26=11$$
$$C_2=(21\cdot15+18\cdot0+21\cdot24)\bmod26=13$$
$$C_3=(2\cdot15+2\cdot0+19\cdot24)\bmod26=18$$

მაშასადამე, შრიფტექსტი C=(11,13,18) LNS.

გაშიფრვის პროცესის ჩასატარებლად საჭიროა შებრუნებული K^{-1} მატრიცის გამოთვლა.

გაშიფრვის რეზულტატი იქნება:

Cs შეტყობინების ცოდნით შეუძლებელია გამოყენებული Kj გასაღებისა და Mi შეტყობინების გამოცნობა.

თუ რომელიმე პირობა დაირღვევა, მაშინ რომელიღაც i და j-სთვის $P(M_i|C_j)=0$ და კრიპტოანალიზის შედეგად შესაძლებელია შიფრის გახსნა.

მაგალითის სახით განვიხილოთ ცეზარის დაშიფრვის სისტემით (ღია ტექსტის სიმბოლო შეცვლილია მისგან K პოზიციით დაშორებული სიმბოლოთი) მიღებული შრიფტექსტიდან საწყისი ტექსტის აღდგენა კრიპტოანალიზის მეთოდით.

ვთქვათ, შრიფტექსტი შეიცავს 29 სიმბოლოს

G R O B O K B O D R O R O B Y O C Y P I O C D O B I O K B.

რადგან $1\le K\le25$ და K ნაკლებია 29 სიმბოლოსგან მიღებული გააზრებული და შესაძლებელი შეტყობინებების რაოდენობაზე, ამიტომ სრულყოფილი საიდუმლოების პირობები დარღვეულია და ეს შრიფტექსტი ადვილად გასაშიფრია K-ს მნიშვნელობის არცოდნის შემთხვევაში. მართლაც, თუ შევადგენთ ცხრილს (ნახ.3.32), რომლის ნულოვან სტრიქონში ჩაიწერება შრიფტექსტი, ხოლო თითოეულ სვეტში ალფაბეტის ყველა ასო დაწყებული შრიფტექსტის ასოდან წრიული მიმართულებით მარჯვნიდან მარცხნივ, მაშინ შევამჩნევთ, რომ გააზრებული ტექსტი მიიღება მეათე სტრიქონში.

W H E R E A R E T H E H E R O E S O F Y E S T E R Y E A R
WHERE ARE THE HEROES OF YESTERDYEAR.

გასაღები	ტექსტი
0	G R O B O K B O D R O R O B Y O C Y P I O C D O B I O K B.
1	F Q N A N J A N C Q N Q N A X N B X O H N B C N A H N J A
2	E P M Z M I Z M B P M P M Z W M A W N G M A B M Z G M I Z
3	D O L Y L H Y L A O L O L Y V L Z V M F L Z A L Y F L H Y
4	C N K X K G X K Z N K N K X U K Y U L E K Y Z K X E K G X
5	B M J W J F W J Y M J M J W T J X T K D J X Y J W D J F W
6	A L I V I E V I X L I L I V S I W S J C I W X I V C I E V
7	Z K H U H D U H W K H K H U R H V R I B H V W H U B H D U
8	Y J G T G C T G V J G J G T Q G U Q H A G U V G T A G C T
9	X I F S F B S F U I F I F S P F T P G Z F T U F S Z F B S
10	W H E R E A R E T H E H E R O E S O F Y E S T E R Y E A R

11
12
13
14
15
16
17
18
19
20

ნახ.3.32

თუ აღდგენილ ტექსტს დავშიფრავთ ცეზარის დაშიფვრის სისტემით, როცა K=10, მივიღებთ მოცემულ შრიფტექსტს.

განვიხილოთ ქართულ ენაზე სესრულებული შრიფტექსტი, რომელიც შეიცავს შვიდ ასოს (შითცდჟდ).

შ ი თ ც დ ჟ დ
ყ თ ზ ჩ გ ა გ
ღ ზ ვ შ ბ ო ბ
ქ ვ ე ყ ა ნ ა
ფ ე დ ღ ჰ მ ჰ
უ დ გ ქ ჯ ლ ჯ
თ გ ბ ფ ხ კ ხ
ს ბ ა უ ჭ ი ჭ

რადგან გააზრებული ტექსტი მიიღება მესამე სტრიქონში (ქვეყანა), მაშასადამე, შეგვიძლია ვთქვათ რომ K-3 თუ აღდგენილ ტექსტს დავშიფრავთ ცეზარის დაშიფვრის სისტემით, როცა ????? მივიღებთ მოცემულ შრიფტექსტს.

ადვილი გასაშიფრია, აგრეთვე, შრიფტექსტი, რომელიც მიღებულია ტრისემუსის პროგრესული გასაღების გამოყენების მეთოდით. ვთქვათ, შრიფტექსტი შეიცავს 12 სიმბოლოს და მას აქვს შემდეგი სახე:

O Q Z M X Z O M C S X Q.

თუ შევადგენთ ცხრილს წინა შემთხვევის ანალოგიურად, მივიღებთ:

სტრიქონების დანომვრა იწყება 0-დან, ხოლო სვეტების 1-დან და რიგრიგობით ამოიკრიფება ის ასოები, რომლებიც განლაგებულია იმ პოზიიციებზე რომელთათვის სტრიქონისა და სვეტის ნომერი ერთი და იგივეა.

პოზიცია:

11-N, 77-H,
22-O, 88-E,
33-W, 99-T<
44-I, AA-I,
55-S, BB-M,
66-T, CC-E,

მეორე ოპერაციის დროს P რეგისტრში ჩაწერილი მიმდევრობა მარცხნივ ციკლურად დაიძვრება 11 თანრიგით.

P რეგისტრის გამოსასვლელებზე მიღებული მიმდევრობა და L(0) მიმდევრობა CM_2 ამჯამავით იკრიბება 2^{32} მოდულით. CM_2-ის გამოსასვლელზე მიღებული R(1) მიმდევრობა ჩაიწერება N_1 დამგროვებელში, ხოლო N_1-ში ჩაწერილი წინა R(0) მიმდევრობა გადადის N_2-ში. ამით პირველი ციკლი მთავრდება.

ანალოგიურად მიმდინარეობს დანარჩენი 31 ციკლი, ოღონდ 1-8, 9-16, 17-24 ციკლებში Z გასაღების ბაიტები მონაწილეობენ შემდეგი თანმიმდევრობით $Z_0, Z_1, Z_2, Z_3, Z_4, Z_5, Z_6, Z_7$, ხოლო 25-32 ციკლებში – $Z_7, Z_6, Z_5, Z_4, Z_3, Z_2, Z_1, Z_0$ თანმიმდევრობით და ოცდამეთორმეტე ციკლის ბოლოს CM_2-ის გამოსასვლელზე მიღებული მიმდევრობა ჩაიწერება N_2-ში, ხოლო N_1-ში რჩება ჩაწერილი წინა R(31).

დაშიფვრის პროცესის ამსახველი განტოლებებია:

დაშიფრული $Q_ш$ ბლოკი მიიღება N_1 და N_2-ში ჩაწერილი მიმდევრობების წაკითხვით დაწყებული დაბალი თანრიგიდან, ე.ი.

$Q_ш=(a_1(32), a_2(32)…., a_{32}(32), b_1(32)\ b2(32)… b_{32}(32))$

გაშიფვრისას $Q_ш$ ბლოკის სესაბამისი მიმდევრობა იყოფა ორ ოცდათორმეტბიტიან მიმდევრობებად:

$L(32)=(b_{32}(32), b_{31}(32)…, b_1(32))$ და $R(32)=(a32(32), a_{31}(32)…., a_1(32))$

L(32)-ით შეივსება N_2, ხოლო R(32)-ით – N_1 და დაიწყება გაშიფვრის ოცდათორმეტციკლიანი პროცესი.

1-8 ციკლების დროს გამოიყენება Z გასარების ბაიტები შემდეგი თანმიმდევრობით $Z_0, Z_1, Z_2, Z_3, Z_4, Z_5, Z_6, Z_7$, ხოლო 9-16,

17-24 და 25-32 ციკლებში - $Z_7, Z_6, Z_5, Z_4, Z_3, Z_2, Z_1, Z_0$ თანმიმდევრობით.

გაშიფვრის განტოლებებს აქვთ შემდეგი სახე:

32 ციკლის შემდეგ N_1 და N_2 დამგროვებლებში ცაწერილი მიმდევრობები წაიკითხება დაწყებული დაბალი თანრიგიდან და მიიღება ღია ტექსტის ბლოკი.

$Q_ღ=(a_1(0), a_2(0),…,\ a_{32}(0), b_1(0), b_2(0),\ b_{32}(0)$

ამ ლოგარითმის მცირეოდენი გადაკეთებით შესაძებელია გამირების რეჟიმში მომუშავე კრიფტოგრაფიული ალგორითმის მიღება (ნახ. 5.16)

ნახ. 5.16

სამოცდაოთხთანრიგა $Q_{ღ}^{(1)}$, $Q_{ღ}^{(2)}$,…, $Q_{ღ}^{(m)}$ ბლოკებად დაყოფილია ღია ტექსტი იკრიბება ორის მოდულით სამოცდაოთხი ბიტის შემცველ გამა შიფრის $გ_{ჭ}^{(1)}$, $გ_{ჭ}^{(2)}$,…., $გ_{ჭ}^{(m)}$ ბლოკებთან, ე.ი.

$Q_{ჭ}^{(1)}=A(Ŝ)\ Q_{ღ}^{(1)}=გშ^{(1)}\ Q_{ღ}^{(1)}$

თუ $Q_{ღ}^{(m)}$ ბლოკში თანრიგების რიცხვი ნაკლებია 64-ზე, მაშინ $გ_{ჭ}^{(m)}$ –ს ზედმეტი თანრიგები ჩამოშორდება.

გამა შიფრის $გ_{ჭ}^{(1)}$ ბლოკის მისაღებად N_1 და N_2 დამგროვებლებში თავდაპირველად იწერება სამოცდაოთხბიტიანი სინქროკოდი Ŝ (S_1, S_2,…, S_{64}), ხოლო $გ_{ჭ}^{(2)}$, $გ_{ჭ}^{(3)}$,…., $გ_{ჭ}^{(m)}$ ბლოკების მისაღებად კი, შესაბამისად, $Q_{ჭ}^{(1)}$, $Q_{ჭ}^{(2)}$,….., $Q_{ჭ}^{(ϑ-1)}$ბლოკები.

კავშირის არხში გადაიცემა S სინქროკოდი და დაშიფრული მონაცემების $Q_{ჭ}^{(1)}$ ბლოკები. გაშიფვრისას CM3 ამჯამავით ხდება $Q_{ჭ}^{(1)}$ და $გ_{ჭ}^{(1)}$ ბლოკების შეკრება ორის მოდულით, ე.ი. $Q_{ღ}^{(1)}=A(Ŝ)\ Q_{ჭ}^{(1)}= გ_{ჭ}^{(1)}\ Q_{ჭ}^{(1)}$.

6. ასიმეტრიული კრიპტოსისტემები

ღია გასარებიანი ასიმეტრიულ კრიპტოგრაფიულ სისტემებში ძირითადად გამოიყენება ერთმიმართული (შეუქცევადი) ფუნქციებით დაშიფვრის ბლოკური მეთოდები.

F:x y ფუნქცია წარმოადგენს ერთმიმართულს, თუ ნებისმიერი x და y სიმრავლეების შემთხვევაში ყოველი x∈X მნიშვნელობისთვის მისი გამოთვლა ეფექტური ალგორითმების მეშვეობით ადვილად ხორციელდება (y=f(x), y∈Y), ხოლო y-ის მნიშვნელობით x-ის მიშვნელობის აღდგენა თითქმის განუხორციელებელია.

ერთმიმართულ ფუნქციებს მიეკუთვნება: ორი დიდი მთელი რიცხვის გამრავლება, მოდულური ექსპონენტი, ჰეშ-ფუნქცია და სხვ.

1.ორი დიდი მთელი P და Q რიცხვების გამრავლება.

N=P·Q ნამრავლის გამოანგარიშება ეგმ-თვის პრობლემას არ წარმოადგენს, ხოლო N-ს მნიშვნელობის მიხედვით P და Q მნიშვნელობების აღდგენა (P და Q გამყოფების პოვნა) პრაქტიკულად გადაუწყვეტელი ამოცანაა. მაგალითად თუ $N=2^{564}$ და P=Q, მაშინ N-ის დასაშლელად ეგმ-ზესაჭიროა დაახლოებით 10^{23} ოპერაციის შესრულება.

2.მოდულური ექსპონენტი.

თუ A და N მთელი რიცხვებია (1≤A≤N), ხოლო Z_N არის არაუარყოფითი მთელ რიცხვთა შემდეგი სიმრავლე Z_N =(0,1,2,…, N-1), მაშინ მოდულური ექსპონენტი A ფუძით და N მოდულით წარმოადგენს ფუნქციას:

$f_{AN}:Z_N \quad Z_N$

$f_{AN}(x)=A^x(modN)$,

სადაც x მთელი რიცხვია,(1< x <N-1),

$f_{AN}(x)$-ის მნიშვნელობის სწრაფად გამოთვლა შესაძლებელია სხვადასხვა ეფექტური ალგორითმების მეშვეობით.

თუ $y=A^x$, მაშინ $x=\log_a y$.

$f_{AN}(x)$-ის მნიშვნელობიდან x-ის მნიშვნელობის აღდგენა წარმოადგენს დისკრეტული ლოგარითმის მოძებნის ამოცანას, ე.ი. A, N, y მნიშვნელობების ცოდნით საჭიროა ისეთი x მნიშვნელობის მოძებნა, რომელიც აკმაყოფილებს ტოლობას Ax(modN)=y, ასეთი გამოთვლის შესრულება საჭიროებს დიდი რაოდენობის ოპერაციის ჩატარებას, მაგალითად, თუ $A=2^{664}$ და $N=2^{664}$, მაშინ x მნიშვნელობის მოძებნა მოითხოვს დაახლოებით 10^{26} ოპერაციის ჩატარებას.

3.ჰეშ-ფუნქცია.

ჰეშ-ფუნქცია წარმოადგენს თვლის ორობით სისტემაში წარმოდგენილი ნებისმიერი სიგრძის M შეტყობინების შეკუმშულ ასახვას ფიქსირებული სიგრძის H შეტყობინებაში (H<<M), ე.ი. H=ჰ(M). ჰეშ-ფუნქციის H მნიშვნელობიდან M შეტყობინების აღდგენა გამოთვლითი პროცესების ჩატარებით შეუძლებელია.

ერთმიმართული ჰეშ-ფუნქციის მიღების მეთოდის ერთი ბიჯი ნაჩვენებია 6.1. ნახ-ზე.

ნახ. 6.1

სადაც $H_1=f(M_1H??)$ არის H_1 ჰეშ-ფუნქციის ბლოკი M –შეტყობინების ბლოკი, H_1 – ჰეშ-ფუნქციის ბლოკი წინა ბიჯზე. უნდა აღინიშნოს, რომ M????? H?? და H?? ბლოკები წარმოადგენენ ერთი და იგივე ნ სიგრძის შეტყობინებებს და ??????/ შემთხვევითი საწყისი მნიშვნელობაა.

უსაფრთხო ჰეშ-ფუნქციების მიღების ალგორითმებია:

ა)ჰეშ-ფუნქცია MD4(Message Didest 4)

ბ)ჰეშ-ფუნქცია MD5(Message Didest 5)-ის ალგორითმი;

გ) ჰეშ-ფუნქცია SHA(Secure Hash Algorithm)-ის ალგორითმი;

დ) სიმეტრიული ბლოკური ალგორითმი.

MD5 ჰეშ-ფუნქცია არის MD4 ჰეშ-ფუნქციის გაუმჯობესებული ვერსია განვიხილოთ MD5 ალგორითმი.

512 ბიტის შემცველი მონაცემების ბლოკი, რომელიც იშლება 16 ოცდათორმეტბიტიან M ქვებლოკებად (0<i <15), განიცდის გარდაქმნას შემდეგი ოთხი ოპერაციის გამყენებით:

FF(a,b,c,d,M,s,t,) a=b+((b,c,d)+M,+t)<<<s).

GG(a,b,c,d,M,s,t,) a=b+((a+G(b,c,d)+M,+t)<<<s).

HH(a,b,c,d,M,s,t,) a=b+((a+H(b,c,d)+M,+t)<<<s).

II(a,b,c,d,M,s,t,) a=b+((a+I(b,c,d)+M,+t)<<<s).

სადაც a,b,c და d დამხმარე ცვლადებია გარკვეული საწყისი მნიშვნელობით:

a A=67452301

b B=EFCDAB89

c C=98BADCEF

d D=10325476

F, G, H და I - სამი ცვლადის შემცველი შემდეგი არაწრფივი ფუნქციები:

t, - კონსტანტა, რომელიც წარმოადგენს i-ურ ეტაპზე 2^{32} sin(i) გამოსახულების მთელი ნაწილის (iიზომება რადიანებში);

<<<s - მონაცემების S რაოდენობის ბიტით მარცხნივ დაძვრის აღმნიშვნელი.

6.2 ნახ-ზე ნაჩვენებია MD5 ალგორითმის მთავარი ციკლის სქემა.

ნახ.6.2

მთავარი ციკლი მოიცავს ოთხ ეტაპს. თითოეულ ეტაპზე 16-ჯერ სრულდება ზემოთ მოცემული ოპერაციებიდან (FF,GG,HH,II) ერთ-ერთი 6.3 ნახ.-ზე ნაჩვენებია ამ ოპერაციების ზოგადი სქემა.

ნახ. 6.3

თითოეულ ეტაპზე შესრულებული ოპერაციებია:

ეტაპი 1:	ეტაპი2:
FF(a,b,c,d,M0,7,d76aa478)	GG(a,b,c,d,M1,5,f61e2562)
FF(a,b,c,d,M1,12,e8c7b756)	GG(a,b,c,d,M6,9,c040b340)
FF(a,b,c,d,M2,17,242070db)	GG(a,b,c,d,M11,14,265e5a51)
FF(a,b,c,d,M3,22,c1bdceee)	GG(a,b,c,d,M0,20,e9b6c7aa)
ეტაპი:	ეტაპი:

??

MD4 ალგორითმი იმით განსხვავდება MD5 ალგორითმისაგან, რომ იგი მოიცავს მხოლოდ სამ ეტაპს და არაწრფივ ფუნქციებს აქვთ შემდეგი გამოსახულება:

$$F(x,y,z)\text{-}(x\cdot y)+(x\cdot z)$$
$$Q(x,y,z)=((x\cdot y)+(y\cdot z)$$
$$H(x,y,z,)=???$$

MD4 და MD5 ალგორითმების გამოსასვლელზე მიიღება 128 ბიტის (ოთხი ოცდათორმეტბიტიანი ბლოკი) შემცველი ჰეშ-ფუნქცია.

SHA ალგორითმი ახდენს შეტყობინების 512 ბიტის შემცველი ბლოკების შეკუმშვას 160 ბიტის შემცველ შეტყობინებად. MD5 ალგორითმისაგან განსხვავებით, ამ ალგორითმში გამოიყენება ხუთი ცვლადი სიდიდე და 512 ბიტის შემცველი შეტყობინება განიცდის გარდაქმნას ოთხ ეტაპად, თითოეულ ეტაპზე ოცი ოპერაციის განხორციელებით. ხუთი ცვლადი სიდიდე დამხმარე ცვლადებია საწყისი მნიშვნელობებით:

a A=67452301,
b B=EFCDAB89,
c C=98BADCEF,
d D=10325476,
e E=C3D2E1F0.

ამ ცვლადების გარდაქმნა ხდება შემდეგი ოპერაციების განხორციელებით:

$a,b,c,d,e \quad b,c,S^{30}(d),\ e,\ [a+F(b,c,d)+S^{5}(e)+W_t+K_t],$

სადაც F არის არაწრფივი ფუნქცია, W_t – შეტყობინების გარდაქმნილი ბლოკი, K_t – კონსტანტა, S – მარცხნივ დაძვრის აღმნიშვნელი.

შამცვლადიანი არაწრფივი ფუნქციის რეალიზაცია მიმდინარეობს შემდეგი გამოსახულებების გამოყენებით:

$Ft(x,y,z)=(x\cdot y)+(x\cdot z), \quad 0\le t\le 19,$
$Ft(x,y,z)=x\ y\ z, \quad 20\le t\le 39,$
$Ft(x,y,z)=x\cdot y+x\cdot z+y\cdot z, \quad 40\le t\le 59,$
$Ft(x,y,z)=x\ y\ z, \quad 60\le t\le 79,$

სადაც t ოპერაციის ნომერია ($0\le t\le 79$).

შეტყობინების ბლოკი გარდაქმნის თექვსმეტ ოცდათორმეტბიტიან სიტყვას ($M_0 \div M_{15}$) ოთხმოც ოცდათორმეტბიტიან სიტყვად შემდეგი ალგორითმის მიხედვით:

$Wt=Mt, \quad 0\le t\le 15,$
$Wt=(W_{t-3}\ W_{t-8}\ W_{t-14}\ W_{t-16})\cdot S^{1} \quad 16\le t\le 79.$

ალგორითმში გამოყენებულია ოთხი მუდმივა წარმოდგენილი თექვსმეტობითი სახით. თითოეული არის $\sqrt{n}\cdot 2^{30}$ ($n=2,3,5,10$) გამოსახულების მთელი ნაწილი, კერძოდ:

6.4ნახ-ზე ნაჩვენებია SHA ალგორითმის ერთი ოპერაციის შესასრულებელი სქემა.

სიმეტრიული ბლოკური ალგორითმების გამოყენებით ერთმიმართული ჰეშ-ფუნქციის ფორმირებისას გამოიყენება სამი ცვლადი A,B და C (ნახ. 6.5).

$Hi=E_A(B)$ C, $H_0=I_0$(I_0 შემთხვევითი საწყისი მნიშვნელობაა).

A, B და C ცვლადებს შეუძლია მიიღოს ოთხი შესაძლო მნიშვნელობიდან (M_i, H_{i-1}, M_i, H_{i-1}, t_i –კონსტანტა) ერთ-ერთი.

6.6 ნახ-ზე ნაჩვენებია ოთხი უსაფრთხო ჰეშ-ფუნქციის ჰეშირების სქემა.

4) ერთმიმართული ფუნქცია „ფარული სვლა”.

ვთქვათ, მოცემულია N რაოდენობის a_1 დადებითი რიცხვების A სიმრავლე $A=\{a_1, a_2, a_3,\ldots, a_N\}$ და ერთი დადებითი რიცხვი Z.

ამოცანა მდგომარეობს შემდეგში: საჭიროა A სიმრავლეში შემავალი რიცხვებიდან მოიძებნოს ისეთი a_j რიცხვები, რომელთა ჯამი z-ის ტოლია. ეს ამოცანა ცნობილია, როგორც ზურგჩანთის ჩალაგების ამოცანა (z წარმოადგენს ზურგჩანთის ზომას, ხოლო a_i საგნის ზომას და ასეთი საგნების ნაკრებმა უნდა შეავსოს ზურგჩანთა).

ნახ.6.4

ნახ.6.5

ნახ.6.6

საილუსტრაციოდ განვიხილოდ ათი რიცხვისგან შედგენილი სიმრავლე: $A=\{43,129,215,473,903,302,561,1165,697,1523\}$ და z=3231

ზურგჩანთა ივსება მხოლოდ ერთი ვარიანტის შერჩევით (ნახ.6.7) და ეს ვარიანტია 3231=129+473+903+561+1165.

ზურგჩანთაში ჩასალაგებელი საგნის სიმრავლე

ნახ.6.7

ამ ერთი ვარიანტის შესარჩევად საჭიროა 2^{10}=1024 რაოდენობის ქვესიმრავლეების განხილვა (ცარიელი სიმრავლის ჩათვლით). ე.ი. ათი რიცხვის შემთხვევაში დასმული ამოცანა ადვილად გადასაწყვეტია. მაგრამ, თუ აღებულია 300 რიცხვი, მაშინ 20^{300} რაოდენობის ქვესიმრავლის განხილვა და სწორი გადაწყვეტილების მოძენა პრაქტიკულად შეუძლებელია.

ასეთი ერთმიმართული ფუნქციის შესადგენად საჭიროა თავდაპირველად შედგეს ზურგჩანთის ვექტორი და მონაცემთა ვექტორი. ზურგჩანთის ვექტორი წარმოადგენს სხვადასხვა მთელი რიცხვებისგან შედგენილ n კორტეჟს ($a=a_1,a_2,\ldots a_n$), ხოლო მონაცემთა ვექტორი - ორობითი სიმბოლოების n კორტეჟს ($x=x_1,x_2,\ldots x_n$). ზურგჩანთა S წარმოადგენს ზურგჩანთის ვექტორის კომპონენტების ქვესიმრავლეს.

S=???????????????? სადაც x_1=0,1.

ერთმიმართული X ფუნქცია განისაზღვრება ცნობილი S და a მნიშვნელობებით. X-ის განსაზღვრის ალგორითმი შემდეგია: a ვექტორი ლაგდება სწრაფად ზრდადი მიმდევრობის სახით. სწრაფად ზრდადი მიმდევრობა ეს ისეთი მიმდევრობაა, რომლის ყოველი კომპონენტი მეტია მის წინ განთავსებულ ყველა კომპონენტის ჯამზე, ე.ი.

a_1 >?????????????????????? i=2,3…,n. (1)

თუ a ვექტორი სწრაფად ზრდადია, მაშინ X-ის პირველი ელემენტი $x_n=1$, როცა $S \geq a_n$ და $x_n = 0$, როცა $S < a_n$. რაც შეეხება X ვექტორის დანარჩენ კომპონენტებს, ისინი გამოითვლებიან შემდეგი თანაფარდობიდან:

x1 = ??????????????? როცა S- ?????????? (2)

სხვა შემთხვევაში,

სადაც, i=n-1, n-2,…1.

განვიხილოთ მაგალითი:

ვთქვათ, a=171,197,459,1191,2410,4517 და S=aX=3798. ვიპოვოთ X.

რადგან a ვექტორი წარმოადგენს სწრაფად ზრდად მიმდევრობას, ამიტომ ის აკმაყოფილებს (1) უტოლობას, რადგან $S<a_6$ (3798<4517), ამიტომ $x_6 = 0$, ხოლო დანარჩენი x კომპონენტისათვის, (2)-ის თანახმად, გვექნება:

$x_5 = 1$, $x_4 = 1$, $x_3 = 0$, $x_2 = 1$ და $x_1 = 0$, ე.ი. X =010110.

მართლაც, 197+1191+2410=3798,

რადგან ა ვექტორის საშუალებით ხდება ერთმიმართული X ფუნქციის მნიშვნელობიდის განსაზღვრა, ამიტომ a ვექტორს დაარქვეს „ფარული სვლის" ვექტორი.

თუ a ვექტორი არ წარმოადგენს სწრაფად ზრდად მიმდევრობას, მაშინ ერთმიმართული X ფუნქციის განსაზღვრისათვის გამოიყენება მერკლ-ჰერმანის ღია გასაღებიანი კრიპტოსისტემა. ამ კრიპტოსისტემის ალგორითმი შემდეგია:

თავდაპირველად ხდება a^1 ვექტორის შედგენა ისეთი რიცხვების მეშვეობით, რომლებიც წარმოადგენენ სწრაფად ზრდად მიმდევრობას, შემდეგ შეირჩევა მარტივი რიცხვი M და შემთხვევითი რიცხვი W შემდეგი პირობების გათვალისწინები:

M>????????????? 1<W<M, $W \cdot W^1 (\text{მოდმ}) = 1$.

a^1,M,W და W^{-1} მნიშვნელობები შეინახება საიდუმლოდ a^1 ვექტორისა და W,M რიცხვების საშუალებით ხდება a ვექტორის განსაზღვრა შემდეგი თანაფარდობის გამოყენებით:

$$a_i=(W \cdot a^1{}_i) \text{mod} M$$

a ვექტორი წარმოადგენს ზურგჩანთის ვექტორს და მისი მნიშვნელობა არ წარმოადგენს საიდუმლოს.

a და X ვექტორებით განისაზღვრება ზურგჩანთის S ვექტორი:

S=aX=???????????????????????????

S-ის მნიშვნელობა ეგზავნება კანონიერ მომხმარებელს, რომელიც გარდაქმნის S-ს S'-ად შემდეგი გამოსახულებით.

??
??/

S'-სა და a'-ის მნიშვნელობებით მომხმარებელი განსაზღვრავს X-ს (1) და (2) თანაფარდობების მიხედვით.

განვიხილოთ მაგალითი, ვთქვათ, ა'=(171, 197, 450, 1101, 2410, 4517)

??

შევირჩევთ M-9109, W-2251.

(2251·W-1)mod 9109 და $a_i=(a_i' \cdot 2251) \text{mod} 9109$ შედარებებიდან გამოვთვლით W-1=1388, და a=2343, 6215, 3892, 2895, 5055, 2123.

ვთქვათ, კანონიერ მომხმარებელს ეგზავნება S=aX-14165, მომხმარებელი გამოთვლის S'=(W-1·S)modM=(1388·14165)mod9109=3708 და a' ვექტორის გამოყენებით განსაზღვრავს X-ს.

3798=2410+1191+197 და X=010110

X-ის განსაზღვრა S'-ით და სწრაფად ზრდადი ა' ვექტორით განხილულია პირველ მაგალითში.

ერთმიმართული ფუნქციები გამოიყენება დაშიფვრის ისეთ სისტემებში, როგორიცაა: RSA კრიპტოსისტემა, ელ-გამალის დაშიფვრის სქემა და ს ხვ.

6.1. მონაცემების დაშიფვრის RSA კრიპტოსისტემა.

RSA კრიპტოსისტემაში საიდუმლო გასაღები $Z_ს$, ღია გასაღები $Z_ღ$, შეტყობინება x და კრიპტოგრამა y მიეკუთვნებიან მთელ რიცხვთა (0,1,2…., N-1) სიმრავლეს, სადაც N მოდულია

$$N=P\cdot Q$$

P და Q შემთხვევითი დიდი მარტივი რიცხვებია, მაქსიმალური უსაფრთხოების უზრუნველსაყოფად P და Q შეირჩევა ერთნაირი სიგრძის და ინახება საიდუმლოდ.

ღია გასაღების მნიშვნელობა შეირჩევა შემთხვევით შემდეგი პირობების გათვალისწინებით:

$$1<Z_ღ\le\varphi(N),\ \text{უსგ}((Z_ღ, \varphi=(N))=1,$$
$$\varphi(N)=(P-1)(Q-1)$$

სადაც φ(N) ეილერის ფუნქციაა.
საიდუმლო გასაღების მნიშვნელობა გამოითვლება ევკლიდეს ალგორითმით:

$$z_ს\cdot z_ღ=1(\text{mod }\varphi=(N))$$
$$\text{ან}\quad z_ს=z_ღ-1=(\text{mod}(P-1)(Q-1))$$

ღია გასაღები გამოიყენება მონაცემების დასაშიფრად, ხოლო საიდუმლო გასაღები შრიფტექსტის გასაშიფრად.
დაშიფვრისას კრიპტოგრამა მიიღება $y=Ez_ღ(x)=x^{z}{}_ღ(\text{mod}N)$ გამოსახულებით, ხოლო ამ უკანასკნელის გაშიფვრა ხდება $x=Dz_ს(y)=yz_ს(\text{mod}N)$გამოსახულებით.

x-ის განსაღვრა, როცა ცნობილია $y,z_ღ$ და N(N=2512), პრაქტიკულად შეუძლებელია.

დაშიფვრისა და გაშიფვრის პროცესების მიმდინარეობის საცვენებლად გვიხილოტ ორი A და B მომხმარებელი. დავუსვათ, რომ A მომხმარებელს სურს გადასცეს დაშიფრული შეტყობინება B მომხმარებელს. ამ შემთხვევაში მომხმარებელი A შეტყობინების გამგზავნია, ხოლო B – შეტყობინების მიმღები. კრიპტოსისტემას აფორმირებს შემდეგი სეტყობინების მიმღები, ე.ი. ამ შემთხვევაში B მომხმარებელი. განვიხილოთ B და A მომხმარებლის მიერ შესასრულებელი ოპერაციების თანმიმდევრობა.

1. B მომხმარებელი შეარჩევს ორ დიდ მარტივ P და Q რიცხვს;
2. B მომხმარებელი გამოთვლის მოდულის მნიშვნელობას N=P·Q;
3. B მომხმარებელი გამოთვლის ეილერის ფუნქციას φ=(N) = (P-1)(Q-1) და შეირჩევს ღია $z_ღ$ გასაების შემთხვევით მნიშვნელობას შემდეგი პირობებით:

$$1<z_ღ\le\varphi=(N),\ \text{უსგ}(z_ღ, \varphi=(N))=1;$$

4. B მომხმარებელი გამოთვლის საიდუმლო გასაღების მნიშვნელობას
$z_ს=z_ღ-1(\text{mod}\varphi=(N))$;
5. B მომხმარებელი გააგზავნის N და $z_ღ$ მნიშვნელობებს დაუცველი არხით A მომხმარებელთან.

თუ A მომხმარებელს სურს გადასცეს B მომხმარებელს შეტყობინება, მაშინ იგი ასრულებს შემდეგ ოპერაციებს:

6. A მომხმარებელი ახდენს საწყისი ღია ტექსტის დაყოფას ბლოკებად. თითოეული ბლოკე წარმოდგენილი უნდა იყოს რიცხვის სახით x_i=0,1,2,…., N-1);
7. A მომხმარებელი შიფრავს x_i რიცხვების მიმდევრობას $y=x^{z}{}_ღ(\text{mod}N)$ გამოსახულების სესაბამისად და გააგზავნის $y_1,y_2,y_3,….,y_i$ კრიპტოგრამას B მომხმარებლებთან;
8. B მომხმარებელი გაშიფრავს მიღებულ კრიპტოგრამას საიდუმლო გასაღების გამოყენებით, ე.ი. $xi=yi^{z}{}_ს(\text{mod}N)$.

განვიხილოთ მაგალითი მცირე რიცხვების შემთხვევაში.

1. P=3 და Q=11.
2. N=P·Q=3·11=33
3. φ=(N)= φ=(33)=(P-1)(Q-1)=2·10=20

$1<z_{ღ}\leq 20$, უსგ $(z_{ღ},20)=1$

დავუშვათ $z_{ღ}=7$

4. $Z_{ს}=Z_{ღ}$ -1(mod φ=(N))=7^{-1}(mod20)=7 $^{φ=(N)\ 1}$(mod20)=$7^{φ=(33)1}$ (mod20) =7^{20-1} (mod20) =7^{19} (mod20)= (716(mod20)*7^{3} (mod20))mod20 =(7^{4}(mod20))^{4}·7^{3}(mod20)=1·3=3
5. B მომხმარებელი გააგზავნის A –სთან (N=33,$z_{ღ}$=7)
6.
7.
8.

განვიხილოთ ტექსტის დასიფვრა RSA კრიპტოსისტემით. ვთქვათ, დასაშიფრი ტექსტია ITS ALL GREEK TO ME. თუ დავუშვებთ, რომ P=47, Q=59 და ზღ=157, მაშინ N=47·59=2773, Φ(N)=46·58=2668, ზს=157-1(მოდ2668)=17.

თუ დასაშიფრი ტექსტის ასოებს შევცვლით ნომრებით (01,26) შუალედიდან, ხოლო სიტყვებს შორის ინტერვალს წარმოადგენთ 00-სახიტ, მაშინ ოთციფრა ბლოკებით წარმოდგენილი ღია ტექსტი მიირებს სემდეგ სახეს:

0920 1900 0112 1200 0718 0505 1100 2015 0013 0500.

თითოეული ბლოკი დაიშიფრება $y_i=x_i^{z_ღ}$ (modN) გამოსახულებით.

ე.ი.:

6.2. დაშიფვრა ღია გასაღებით

ღია გასაღებით დაშიფვრა ხდება შემდეგნაირად:

1. შეტყობინების მიმღები აფორმირებს ღია გასაღებს (N და E რიცხვების წყვილი) და საიდუმლო გასაღებს (რიცხვი D). ამისთვის: – შეირჩევა ორი დიდი მარტივი რიცხვი P და Q;
- განისაზრვრება ღია გასარების პირველი ნაწილი N=P·Q;
- განისაზღვრება ღია გასაღების მეორე ნაწილი. კერძოდ, შეირჩევა კენტი რიცხვი E(E და (P-1)(Q-1) რიცხვები ურთიერთმარტივი რიცხვებია);
- განისაზღვრება საიდუმლო გასაღები: D=E-1მოდ ((P-1)(Q-1) ღია გასაღები (N,E) გაეგზავნება შეტყობინებების გამგზავნებს.

2. შეტყობინების გამგზავნი შიფრავს შეტყობინებას (საჭიროების შემთხვევაში შეტყობინება წინასწარ დაიყოფა S_i სიგრძის სიტყვებად და თითოეული სიტყვის თანრიგების რაოდენობა ნაკლებია $\log_2$N-ზე) $C_i=(S_i)^E$modN გამოსახულების მიხედვით და გააგზავნის მიღებულ სრიფტექსტს მიმღებთან.

3. მიმღები შრიფტექსტს გაშიფრავს საიდუმლო D გასაღების გამოყენებით:

$P_i=(C_i)^D$modN.

6.3. დიფი-ჰელმანის ალგორითმი

დავუშვათ, რომ A და B მომხმარებლებს სურთ დაცული საკომუნიკაციო არხის ორგანიზება. ამისათვის ორივე მხარე თანხმდება N მოდულისა და g რიცხვის შერჩევის შესახებ (ორივე რიცხვი უნდა იყოს მარტივი და დიდი, ამასთან, N=2g+1).

N და g მთელი რიცხვები სისტემის ყველა მომხმარებლისთვის საერთოა და ისინი საიდუმლოებას არ წარმოადგენენ.

A და B მომხმარებლები ერთმანეთისაგან დამოუკიდებლად ირჩევენ და საკუთარ საიდუმლო K_A და K_B (K_A და K_B – შემთხვევითი დიდი მთელი რიცხვებია) მნიშვნელობებს. ეს მნიშვნელობები ინახება საიდუმლოდ.

საიდუმლო გასაღებების შერჩევის შემდეგ A და B მომხმარებლები გამოთვლიან ღია გასაღებებს

$$Y_A=g^{K_A}(\text{mod } N),$$

$$YB=g^{K_B}(\text{mod } N)$$

და გასაღებების ამ მნიშვნელობებს გაცვლიან ერთმანეთში დაუცველი არხით.

მიღებული ღია გასაღების მნიშვნელობით თითოეული გამოთვლის საერთო საიდუმლო გასაღებს:

მომხმარებელი A: $K=(Y_B)^{K_A}=(\text{mod } N)$;

მომხმარებელი B: $K=(Y_A)^{K_B}=(g^{K_A})^{K_B}\ (\text{mod } N)$.

ამასთან, K=K', რადგან $(g^{K_A})^{K_A}=(g^{K_B})^{K_B}\ (\text{mod } N)$.

დიფი-ჰელმანის ალგორითმისს რეალიზაცია ნაჩვენებია 6.8 ნახ-ზე.

ორივე მხარე შიფრავს გადასაცემ M შეტყობინებას დაშიფვრის შემდეგი გარდაქმნის გამოყენებით:

$$C=E_K(M)=M^K(\text{mod } N).$$

გაშიფვრის შესასრულებლად მიმღები განსაზღვრავს გაშიფვრის K^* გასაღების მნიშვნელობას შემდეგი შედარების საშუალებით:

$$K\cdot K^*=1(\text{mod } N-1)$$

გაშიფვრის გასაღებით ხდება M შეტყობინების არდგენა:

$$M=D_K(C)=C^{K^*}(\text{mod } N)$$

მაგალითი. ვთქვათ, N=47 და g=23. დავუშვათ, რომ $K_A=12(\text{mod } 47)$ და $K_B=33(\text{mod } 47)$,

მაშინ: $Y_A=g^{K_A}(\text{mod } N)=23^{12}(\text{mod } 47)=27(\text{mod } 47)$,

$Y_B=g^{K_A}(\text{mod } N)=23^{33}(\text{mod } 47)=33(\text{mod } 47)$.

საერთო საიდუმლო გასაღები იქნება:

$K=(Y_B)^{K_A}(\text{mod } N)=(Y_A)^{K_B}(\text{mod } N)=33^{12}(\text{mod } 47)=27^{33}(\text{mod } 47)=25(\text{mod } 47)$,

თუ M =16, მაშინ: $C=M^K(\text{mod } 47)=16^{25}(\text{mod } 47)=21(\text{mod } 47)$

გაშიფვრის K^* გასაღების მნიშვნელობა იქნება:

$$K\cdot K^*=1(\text{mod } N-1)$$

$$25\cdot K^*=1(\text{mod } 46)$$

$$K^*=35\ (\text{mod } 46)$$

გაშიფრული შეტყობინებაა:

$$M=C^K(\text{mod } 47)=21^{35}(\text{mod } 47)=16\ (\text{mod } 47)$$

ნახ.6.8

გასაღებების გაცვლის ეს ალგორითმი შეიძლება გამოყენებულ იქნება იმ შემთხვევაშიც, როდესაც მომხმარებლის რაოდენობა ორზე მეტია.

ვთქვათ, მომხმარებლის რაოდენობაა სამი (A,B და C). თითოეული მათგანი შეირჩევს საკუთარ საიდუმლო გასაღებს (K_A, K_B და K_C) და გამოთვლის ღია გასაღებს:

$Y^A=g^{K_A}(\text{mod}N)$, $Y^B=g^{K_B}(\text{mod}N)$, $YC=g^{K_C}(\text{mod}N)$

ღია გასაღების გაცვლის თანმიმდევრობა ნაჩვენებია 6.9 ნახ-ზე.

ნახ.6.9

მიღებული ღია გასაღების მნიშვნელობა იშიფრება მიმღების საიდუმლო გასაღებით და დაშიფრული შეტყობინება გადაიცემა 6.10 ნახ.ზე ნაჩვენები სქემით.

ნახ.6.10

თითოეული მომხმარებელი გამოთვლის საერთო საიდუმლო K გასაღებს, კერძოდ:
A გამოთვლის $Y_B{}^{K_C K_A}(\text{mod } N)=(g^{K_B})^{K_C K_A}(\text{mod } N)=g^{K_A K_B K_C}(\text{mod } N)=K$;

B – $Y_c{}^{K_A K_B}(\text{mod } N)= g^{K_A K_B K_C}(\text{mod } N)=K$;
C – $Y_A{}^{K_B K_C}(\text{მოდ} N)= g^{K_A K_B K_C}(\text{mod } N)=K$.

6.4. ელ-გამალის დაშიფვრის სქემა

დაშიფვრის სქემაში გამოიყენება საიდუმლო x და ღია y გასაღებები, ამასთან, x გასაღების მნიშვნელობა შეირჩევა გარკვეული პირობების გათვალისწინებით , ხოლო y-ის მნიშვნელობა გამოითვლება.

თავდაპირველად შეირჩევა ორი დიდი მთელი რიცხვი P და G, ამასთან, P უნდა იყოს მარტივი და G<P (G და P რიცხვები ცნობილია მომხმარებლისათვის). შემდეგ შეირჩევა x გასაღების მნიშვნელობა, რომელიც უნდა იყოს მთელი და ნაკლები P-ზე. y გასაღების მნიშვნელობა გამოითვლება ტოლობით.

$$y=G^x(\text{mod } P).$$

M შეტყობინების დასაშიფრად საჭიროა ისეთი შემთხვევითი მთელი K რიცხვის შერჩევა, რომელიც აკმაყოფილებს შემდეგ პირობებს:

$$1<k<P-1,$$
$$\text{უსგ } (k,P-1)=1.$$

P,G,K,M და y მნიშვნელობებით ხდება ღია ტექსტის სესაბამისი სრიფტექსტის მიღება a და b რიცხვების წყვილის სახით:

$$a=G^k(\text{mod } P),$$
$$b=(y^kM)\text{mod } P.$$

(a,b) შრიფტექსტის გაშიფვრა ხდება შემდეგი ტოლობით:

??????????????????????????????????

რადგან
ვთქვათ, P=11,G=2 და ხ=8, მაშინ

$$y=G^x(\text{mod } 11)=2^8(\text{mod } 11)=256(\text{mod } 11)=3$$

ვთქვათ, სეტყობინებაა M=5, თუ k=9(1<9<10 და უსგ (9,11-1)=1), მაშინ a და b იქნება:

$$a=G^k(\text{mod } P)=29(\text{mod } 11)=512(\text{mod } 11)=6,$$
$$b=(y^k\cdot M)\text{mod } P=(39\cdot 5)\text{mod } 11=(19683\cdot 5)\text{mod } 11=98415(\text{mod } 11)=9.$$

შრიფტექსტი იქნება : (a,b)=(6,9).
მიღებული წყვილის გაშიფვრით მიიღება:

??

$$68M=9(\text{mod}11),$$
$$\text{ან} \quad 1679616\cdot M=9(\text{mod}11),$$
$$(1679616\cdot 9\cdot M)\ \text{mod}11=9,$$
$$((1679616\text{mod}11)\cdot(M\text{mod}11))\text{mod}11=9$$
$$(4M)\text{mod}11=9,$$
$$4M=9(\text{mod}11),$$

$4M=11k+9,$

როცა $k=1$, მაშინ $M=5$

7.ინფორმაციის დაკარგვის გამომწვევი ფაქტორები

შესაძლებელ ფაქტორებს, რომლებსაც მივყევართ ინფორმაციის დაკარგვასთან ან შეცვლასთან, მიეკუთვნებიან:

1. შემთხვევითი ფაქტორები:

ა) მომსახურე პერსონალის ან მომხმარებლის მიერ დაშვებული შეცდომები (საარქივო მონაცემების არასწორი შენახვა, მონაცემების შემთხვევითი განადგურება ან შეცვლა);

ბ) მოწყობილობის მუშაობის დროს წარმოქმნილი შეფერხებები (დისკური სისტემის შეფერხება, მონაცემთა საარქივო სისტემის შეფეხრება, შეფერხებების შეფერხებები სერვერის, მუშა სადგურის, ქსელური კარტის და სხვა მოწყობილობების მუშაობისას);

გ) ელექტროკვების შეფერხებები (კვების ძაბვისა და სიხშირის ცვლილება, კაბელური სისტემის დაზიანება);

დ) პროგრამული უზრუნველყოფის არაკორექტული მუშაობა ან მასში დაშვებული შეცდომები.

2. კომპიუტერული ვირუსებით დაბინძურება:

დესტრუქციული შესაძლებლობების მიხედვით ვირუსები იყოფა: უვნებ, არასაშიშ, საშიშ და ძალიან საშიშ ვირუსებად.

უვნები (უწყინარი) ვირუსები ამცირებენ თავისუფალ მეხსიერებას დისკზე.

არასაშიში ვირუსები ამცირებენ მეხსიერებას და იწვევენ გრაფიკულ ან ბგერით ეფექტებს.

საშიში ვირუსები იწვევენ კომპიუტერის მუშაობაში სერიოზულ შეფერხებებს.

ძალიან საშიში ვირუსები იწვევენ პროგრამის დაკარგვას, მონაცემთა განადგურებას, კომპიუტერის ნორმალური მუშაობისთვის საჭირო ინფორმაციის წაშლას.

ვირუსები, მათი ფუნქციონირების ალგორითმის თავისებურებების მიხედვით, შეიძლება დაიყოს შემდეგ ჯგუფებად:

ა)კომპანიონი (თანამონაწილე) ვირუსი;

ბ)ვირუსი “ჭია”;

გ) პარაზიტული ვირუსი;

დ) სტუდენტური ვირუსი;

ე) უჩინარი ვირუსი;

ვ) მრავალფორმიანი ვირუსი.

კომპანიონი ვირუსის პროგრამა არ ცვლის ფაილებს. ასეთი პროგრამების მუშაობის ალგორითმი მდგომარეობს იმაში, რომ ისინი კომპიუტერის მეხსიერებაში არსებული EXE ფაილებისთვის ქმნიან ე.წ. ფაილ-თანამგზავრებს იგივე სახელით და COM გაფართოებით (მაგალითად, XCOPY.EXE ფაილისათვის იქმნება XCOPY.ბOM ფაილი). ვირუსი იწერება COM ფაილში და არ ცვლის EXE ფაილს. ასეთი ფაილის გაშვებისას ოპერაციული სისტემა DOS პირველად აღმოაჩენს COM ფაილს, ე.ი. ვირუსს, რომელიც შემდეგ გაუშვებს EXE ფაილს.

ვირუსები “ჭია” ვრცელდებიან კომპიუტერულ ქსელებში. ეს პროგრამები არ ცვლიან ფაილებს ან სექტორებს დისკზე. კომპიუტერული ქსელით ვირუსები შედიან კომპიუტერის მეხსიერებაში, ადგენენ სხვა კომპიუტერების ქსელურ მისამართებს და აგზავნიან ამ მისამართებზე თავიანთი პროგრამირების ასლებს. ეს ვირუსები ზოგჯერ ქმნიან მუშა ფაილებს სისტემის დისკებზე.

პარაზიტული ვირუსები თავიანთი პროგრამების ასლების გავრცელებისას აუცილებლად ცვლიან დისკურ სექტორებზე ან ფაილებში შენახულ ინფორმაციას. ამ ჯგუფს მიეკუთვნება ყველა ის ვირუსი, რომელიც არ წარმოადგენს ცომპანიონ და “ჭია” ვირუსს.

სტუდენტური ვირუსები წარმოადგენენ პრიმიტიულ, ხშირ შემთხვევაში არარეზიდენტულ ვირუსებს და ხასიათდებიან შეცდომების დიდი რაოდენობით

უჩინარი ვირუსები წარმოადგენენ სრულყოფილ პროგრამებს. ისინი ხელთ იგდებენ DOS-ის მიმართვებს დაზიანებულ ფაილებთან ან დისკების სექტორებთან და თავიანთი თავის მაგივრად წარადგენენ ინფორმაციის

დაუზიანებელ უბნებს. გარდა ამისა, ასეთ ვირუსებს, ფაილებთან მიმართვისას საკმარისად ორიგინალური ალგორითმების გამოყენებით, შეუძლიათ შეცდომაში შეიყვანონ რეზიდენტური ანტივირუსული მონიტორები.

მრავალფორმიანი ვირუსები საკმაოდ ძნელად აღმოსაჩენი ვირუსებია, რადგან მა თარ გააჩნიათ სიგნატურე, ე.ი. არ შეიცავენ კოდის არც ერთ მუდმივ უბანს. უმეტეს შემთხვევაში ერთი და იგივე ორ ვირუსს არ გააჩნია არც ერთი თანხვედრა.

დღეისათვის არსებულ (ცნობილ) ვირუსებს შეუძლიათ შეასრულონ შემდეგი სპეციალური დამანგრეველი ფუნქციები:

ა)ფაილებში მონაცემების შეცვლა;

ბ)პარალელური და მიმდევრობითი პორტებით გადაცემული მონაცემების შეცვლა;

გ) მონიშნული დისკის შეცვლა (ინფორმაცია იწერება არა მომხმარებლის მიერ მითითებულ დისკზე, არამდ ვირუსის მიერ მითითებულ დისკზე);

დ) ფაილების სახელების შეცვლა (არ ატყობინებს ამის შესახებ მომხარებელს);

ე) დისკის კატალოგების მოსპობა;

ვ) ოპერაციული სისტემის მუშაობის დარღვევა;

ზ) დისპლეის ეკრანზე გამოყვანილი ინფორმაციის წაშლა;

თ) კლავიატურის ბლოკირება;

ი) მყარი დისკის (დისკეტის) ნაწილის ან მთლიანი დისკის ფორმატიზაცია;

კ) კომპიუტერის წარმადობის შემცირება “მცდარი” პროგრამების შესრულების გამო.

3. ბოროტგანმზრახველის (ჰაკერი, ელექტრონული მეკობრე, კომპიუტერული მეკობრე, კრაკერი, ფრაკერი) მიზანმიმართული

მოქმედებები:

ა) არასანქციონირებული შეღწევა ინფორმაციასთან და ქსელის რესურსებთან;

ბ) პროგრამების ან მონაცემების გახსნა და მოდიფიცირება, მათი ასლის გადაღება;

გ) ქსელის ტრაფიკის გახსნა;

დ) კომპიუტერული ვირუსების დამუშავება და გავრცელება, პროგრამულ უზრუნველყოფაში “ლოგიკური ბომბების” შეტანა;

ე) მაგნიტური მატარებლებისა და საანგარიშო დოკუმენტების მოპარვა;

ვ) საარქივო ინფორმაციის დანგრევა ან განადგურება;

ზ) შეტყობინების ფალსიფიცირება, ინფორმაციის მიღების ფაქტის უარყოფა ან ინფორმაციის მიღების თარიღისა და დროის შეცვლა;

თ) კავშირის არხით გადაცემული ინფორმაციის ხელში ჩაგდება;

ქსელში არასანწციონირებული შეღწევის ხელშემწყობი ფაქტორება:

ა)უპაროლო კომპიუტერების გამოყენება;

ბ)ერთობლივი (საერთო) ან ადვილად გასახსნელი პაროლების გამოყენება;

გ) პაროლების პაკეტურ ფაილებში ან კომპიუტერების დისკებზე შენახვა;

დ) რეალურ დროში მომხმარებლის ვინაობის დადგენის შესაძლებლობა;

ე) იდენტიფიკაციის და აუტენტიფიკაციის დაბალი ეფექტურობის მქონე სისტემების გამოყენება ან ასეთი სისტემების გამოუყენებლობა;

ვ) ქსელის მოწყობილობებზე არასაკმარისი ფიზიკური კონტროლის განხორციელება;

ზ) მოდემების დაუცველობა;

თ) დაუშიფრავი მონაცემების გამოყენება.

8.კომპიუტერულ ქსელში ინფორმაციის დაცვის მეთოდები

კომპიუტერულ ქსელში ინფორმაციის დასაცავად გამოიყენება როგორც ორგანიზაციული, ისე ტექნიკური მეთოდები.

ორგანიზაციულ მეთოდებში იგულისხმება იმ აუცილებელი ღონისძიებების გატარება, რომლებიც გარკვეულწილად უზრუნველყოფენ ინფორმაციის დაცვას.

ამ ღონისძიებებს მიეკუთვნება:

ა)ლოკალური ქსელის შექმნისას შენობისა და ამ შენობაში ობიექტების ურთიერთგანლაგების სწორი შერჩევა;

ბ)უცნობი მომხმარებლების ქსელთან დაკავშირების მცდელობის კონტროლი განსაკუთრებით უჩვეულო დროს (ღამის საათებში);

გ) კომპიუტერულ სისტემაში შესავალი პროტოკოლების ფაილების რეგულარული შემოწმება;

დ) კომპიუტერული ჰიგიენის დაცვა, კერძოდ:

- მხოლოდ ლიცენზირებული პროგრამული უზრუნველყოფის გამოყენება;

- პროგრამების ასლის გადაღების აკრძალვა იმ კომპიუტერებიდან, რომლებიც არ აკმაყოფილებენ ჰიგიენურ მოთხოვნებს;

- ისეთი პროგრამების გამოყენების აკრძალვა, რომელთა მოქმედება უცნობია;

- შეძენილი პროგრამების შესწავლათავდაპირველად სისტემური პროგრამისტის მიერ და შემდეგ მათ გამოყენებაზე ნებართვის გაცემა;

- ახალი პროგრამების შემოწმება კარანტინის პერიოდის გათვალისწინებით ისეთ კომპიუტერებზე, რომლებიც არ შეიცავენ საყურადღებო ინფორმაციას;

- ისეთი პროგრამების გამოცდა გაძლიერებული კარანტინის რეჟიმით, რომელთა წარმოქმნის წყაროები უცნობია;

- შემოწმებული ახალი პროგრამული უზრუნველყოფის დუბლიკატის შენახვა სუფთა კომპიუტერში (ორიგინალი უნდა ინახებოდეს ცალკედ ა დაცული უნდა იყოს ჩაწერის რეჟიმისაგან);

- გარეშე პირების კომპიუტერთან დაშვების შეზღუდვა;

- ვირუსის აღმოჩენისას ყველა მომხმარებლის და სისტემური პროგრამისტის გაფრთხილება.

ე) რეზერვირება;

- ოპერაციული სისტემისა და პროგრამული უზრუნველყოფის ყველა ძირითადი კომპონენტის შენახვა არქივში;

- დისკზე ფაილების განაწილების ცხრილის ასლის გადაღება;

- ცვალებადი ფაილების არქივების ყოველდღიური წარმოება.

ვ) პროფილაქტიკა;

- ვინჩესტერის აქტიური ნაწილის შიგთავსის სისტემატიური გადმოტვირთვა დისკეტებზე;

- პროგრამული უზრუნველყოფისა და მომხმარებელთა პროგრამების კომპონენტების ცალ-ცალკე შენახვა;

- გამოუყენებელი პროგრამების არქივში შენახვა;

ზ) რევიზია;

- დისკეტებზე ჩაწერილი ახლად მიღებული პროგრამების გამოკვლევა ვირუსის არსებობაზე;

- ვინჩესტერზე დამახსოვრებული ფაილების სიგრძის სისტემატური კონტროლი;

- პროგრამული უზრუნველყოფის გადაცემისა და შენახვისას საკონტროლო ჯამების მუდმივად შემოწმება;

- ვინჩესტერის ჩასატვირთი სექტორების და სისტემური ფაილების გამოყენებული დისკეტების შიგთავსის შემოწმება;

თ) ფილტრაცია;

- ვინჩესტერის დაყოფა ლოგიკურ დისკებად და მათთან დაკავშირების სხვადასხვა შესაძლებლობების შექმნა;

- ფაილურე სისტემის მოთვალთვალე რეზიდენტული პროგრამული საშუალებების გამოყენება;

ი) სპეციალური პროგრამული საშუალებების გამოყენებით განხორციელებული დაცვა.

ინფორმაციის დაცვის ტექნიკური მეთოდები მოიცავს აპარატულ, პროგრამულ და აპარატულ – პროგრამულ მეთოდებს. ამ მეთოდების გამოყენებით შესაძლებელია განხორციელდეს:

ა) ანტივირუსული დაცვა;

ბ) კომპიუტერული სისტემების და ქსელების დაცვა არასანქცირებული მიერთებისგან;

გ) ელექტრომაგნიტური აკუსტიკური ველების და გამოსხივებების მეშვეობით ინფორმაციის ხელში ჩაგდების თავიდან აცილება;

დ) შეტყობინების გასაიდუმლოების მაღალი სტრუქტურის უზრუნველყოფა კრიპტოგრაფიული მეთოდების გამოყენებით.

ანტივირუსული დაცვა ხორციელდება ისეთი სპეციალური პროგრამების გამოყენებით, როგორიცაა:

1.გამაფრთხილებელი (ფილტრები);

2.გამომჟღავნებული (დეტექტორები);

3.გამომცნობი (დიქტორები).

გამაფრთხილებელი (ამრიდებელი) პროგრამა მუდმივად მოთავსებულია კომპიუტერის მეხსიერებაში. ამ პროგრამით განიცდის ფილტრაციას მიმართვის ნებართვა როგორც ფაილთან (ჩაწერა და წაკითხვა), ისე სხვა პროგრამებთან. ისინი აკონტროლებენ მეხსიერებაში პროგრამების ჩატვირთვას და ამოწმებენ ოპერაციული სისტემის მომსახურე პროგრამების (სისტემური ცხრილები, მმართველი სტრუქტირები და ა.შ.) მუშაობას. როდესაც ვირუსი ცდილობს პროგრამაში შეღწევას, მაშინ გამაფრთხილებელი პროგრამა აჩერებს სისტემას, არ აძლევს ვირუსს შესრულებადი პროგრამის ინფიცირების საშუალებას და ატყობინებს მომხმარებელს ამის შესახებ.

ვირუსით დასენიანების გამომჟღავნებელი პროგრამა აღმოაჩენს ვირუსულ ინფორმაციას ვირუსის მიერ დატოვებული ნაკვალევის მიხედვით. ეს პროგრამები გამოიყენებიან ან დასაცველი პროგრამების ვაქცინაციისათვის (თვითვაქცინაციის ჩათვლით) ან მეხსიერების ფიქსირებული მდგომარეობის კონტროლისთვის.

პროგრამა-ვაქცინა (იმუნიზატორი) ახორციელებს პროგრამისა და დისკების ისეთნაირ მოდიფიცირებას, რომელიც არ აისახება პროგრამის მუშაობაზე. ვირუსი, რომლის საწინააღმდეგოდაც მიმიდნარეობს ვაქცინაცია, თვლის ამ პროგრამებს და დისკებს უკვე დაბინძურებულად. მომხმარებლის მუშაობის დროს პერიოდულად ხდება შედარების ისეთი პროგრამის გაშვება, რომელიც ადარებს სისტემის მიმდინარე მდგომარეობას საწყის მდგომარეობასთან (საკონტროლო ჯამების შემოწმებით) და არეგისტრირებს სისტემის დაბინძურებულ ინფორმაციას.

გამომჟღავნებელი პროგრამების ნაკლოვანებებს წარმოადგენენ:

ა)მათ არ შეუძლიათ ვაქცინაციამდე განხორციელებული დაბინძურების აღმოჩენა;

ბ) იკავებენ მეხსიერების დიდ მოცულობას;

გ) თხოულობენ დროის დანახარჯებს ჩატვირთვისას და ფუნნქციონირებისას;

დ) შესაძლებელია მათი უმოქმედობა იმ შემტხვევაში, თუ ვირუსი გვერდს უვლის მისთვის ცნობილ ვაქცინას.

გამომცნობ პროგრამებს მიეკუთვნებიან: მოთვალთვალე, დაბინძურების განმსაზღვრელი და მონიტორული პროგრამები.

მოთვალთვალე პროგრამა უთვალთვალებს ფაილების მახასიათებელ მონაცემებს (სიგრძე, საკონტროლო ჯამები, შექმნის თარიღი და სხვა.) სპეციალურად ცალკე გამოყოფილ ფაილებში და რეაგირებს ფაილის დაბინძურების შემთხვევაში. ამასთან, დასაცველი ფაილის სიგრძე არ იზრდება და ფაილის
მდგომარეობაზე თვალთვალი ვირუსისათვის შეუმჩნეველი რჩება. ასეთი პროგრამები უნივერსალურია, რადგან ისინი რეაგირებენ ნებისმიერი ვირუსით ინფიცირებისას.

მოთვალთვალე პროგრამების ნაკლოვანებებია:

ა)მათი მოქმედების ეფექტუროობა დამოკიდებულია გაშვებების სიხშირეზე;

ბ)ვერ აღმოაჩენენ მათ გაშვებამდე მომხდარ დაბინძურებას;

გ) საგრძნობლად ზრდიან პროცესორული დროის დანახარჯებს.

დაბინძურების განსაზღვრული პროგრამა კარგად მუშაობს იმ შემთხვევაში, თუ სისტემა უკვე დაბინძურებულია და გაფრთხილებას აზრი არა აქვს. ეს პროგრამები სისტემის ყველა კვანძში ეძებენ იმ სპეციფიკურ სიმბოლოებს, რომლებიც შეიძლება არსებობდნენ ვირუსის პროგრამაში (ნიშნების, წყვეტის ალმების, ფაილების სახელების და სხვა სახის ბრძანებათა თანმიმდევრობა). ასეთი სიმბოლოების აღმოჩენის შემდეგ ხდება ვირუსის სახეობის განსაზღვრა და მისი შემდგომი განადგურება (ე.ი. სისტემა უბრუნდება დაბინძურებამდე არსებულ საწყისს მდგომარეობას).

მონიტორული პროგრამის დანიშნულებაა ვირუსის გავრცელების პროცესის ბლოკირება და ვირუსის ვინჩესტერში ან დისკებზე შეღწევის მცდელობის ბლოკირება. ეს პროგრამები აანალიზებენ დისკეტებთან და ლოგიკურ დისკეტებთან მიმართვის ყველანაირ მოთხოვნებს, გახსნა, პოზიციონირება, ცაწერა და წაკითხვა), ისე სექტორებთან აბსოლუტური და ფიზიკური მისამართებით მიმართვის დონეზე.

კომპიუტერის ვირუსით დაბინძურების ალბათობის შემცირებას და ვირუსის მოქმედებით გამოწვეული შესაძლებელი ზარალის მინიმუმამდე დაყვანას, უზრუნველყოფენ შემდეგი პროფილაქტიკური ღონისძიებები:

ა) კომპიუტერის ჩატვირთვა უნდა განხორციელდეს მხოლოდ ვინჩესტერის გამოყენებით (თუ ვინჩესტერი არაა, მაშინ ჩაწერისაგან დაცული დისკეტებით);

ბ) ვინჩესტერზე ლოგიკური დისკების დაყოფა მიმართვის განსხვავებული ატრიბუტიკის მქონე დისკებად სისტემური პროგრამების, მათემატიკური უზრუნველყოფის საერთო პროგრამებისა და მომხმარებელთა პროგრამების ჩასაწერად;

გ) ცვალებადი ფაილების პერიოდული დაარქივება;

დ) ბრძანებათა ფაილში პროგრამა დეტექტორის გამოძახების ბრძანების ჩართვა და ამ ბრძანების შესრულების მოთხოვნა კომპიუტერის ჩატვირთვისას;

ე) ოპერატიულ მეხსიერებაში ჩაწერილი ინფორმაციის შემმოწმებელი და წყვეტის ვექტორების მდგომარეობის განმსაზღვრელი სადემონსტრაციო პროჰგრამების გამოყენება;

ვ) განგაშის ატეხვა იმ შემთხვევაში, თუ პროგრამის შესრულებისას: ხშირად ჩნდება ოპერაციული სისტემის შეცდომითი შეტყობინებები, დისკებთან მიმართვა რთულდება, კატალოგიდან ქრება პროგრამები და ფაილები, საგრძნობლად მცირდება ოპერაციული მეხსიერების თავისუფალი სივრცე და გაჩნდა ვირუსის არსებობის დამადასტურებელი ვიზუალური ეფექტები.

კომპიუტერული სისტემის ვირუსით დაბინძურების შემთხვევაში მომხმარებელმა უნდა შეასრულოს შემდეგი მოქმედებები:

ა) განსაზღვროს ვირუსის სახეობა დამ ის მიერ გამოწვეული დაზიანება;

ბ) გამორთოს დაბინძურებული კომპიუტერი;

გ) ჩართოს კომპიუტერი და ჩატვირთოს იგი ჩაწერისაგან დაცული დისკეტით. დარწმუნდეს, რომ ჩატვირთვა განხორციელდა ნორმალურად;

დ) დაბინძურებულ კომპიუტერში არ დაუშვას არც ერთი პროგრამის გაშვება შესრულებაზე;

ე) წინასწარ მომზადებულ სუფთა დისკეტებზე მოახდინოს ყველა შეუსრულებელი ფაილის ასლის გადაღება, ჩამტვირთავი

დისკეტის უტილიტიეს გამოყენებით;

ვ) გადახედოს დაბინძურებული დისკის ყველა ფაილს, შეადგინოს გადმოსატვირთავი ფაილების სია და განახორციელოს მათი

გადმოტვირთვა იმ შემთხვევაში, თუ შესაბამისი ფაილების ასლი არ არის არქივში შენახული დისკეტების სახით;

ზ) გამორიცხოს გადმოსატვირთავი ფაილების სიიდან ის ფაილები, რომლებიც იწვევენ გაუგებრობას;

თ) განახორციელოს დარჩენილი ფაილების დამუშავება ანტივირუსული პროგრამებით;

ი) მოახდინოს დაბინძურებული დისკის ფორმატირება და შეამოწმოს მისი სისუფთავე;

კ) აღადგინოს ოპერაციული სისტემა და დირექტორია;

ლ) შეცვალოს ყველა შესასრულებელი ფაილი არქივიდან აღებული ეტალონური დისკეტიდან გადაწერით;

მ) განსაზღვროს ყველა ის დისკეტა, რომელსაც კავშირი ჰქონდა დაბინძურებულ კომპიუტერთან და განახორციელოს მათი

ანტივირუსული დამუშავება;

ნ) შეამოწმოს პროგრამული უზრუნველყოფის მუშაობის უნარიანობა, მიაქციოს ყურადღება აღმოჩენილი ვირუსის შესაძლებელ

გამოჩენას და საჭიროების შემთხვევაში გამოიყენოს მის ხელთ არსებული ანტივირუსული პროგრამები.

კომპიუტერული სისტემებისა და ქსელების დაცვა არასანქცირებული მიერტებისაგან შეიძლება განხორციელდეს:

ა) პაროლური სისტემის გამოყენებით;

ბ) ინტელექტუალური (მიკროპროცესორული) ბარათების გამოყენებით;
გ) ელექტრონული გასაღებების გამოყენებით;
დ) ქსელთაშორისი ეკრანების გამოყენებით;
ე) ელექტრომაგნიტური ველების და გამოსხივებების მეშვეობით ინფორმაციის ხელში ჩაგდების თავიდან აცილების მეთოდების გამოყენებით.

პაროლური სისტემა დღევანდლამდე ითვლებოდა კომპიუტერული ქსელების არასანქციონირებული მიერთებისაგან დაცვის ერთადერთ მეთოდად. დაცვისათვის გამოყენებული პაროლები შეიძლება დაიყოს შვიდ ჯგუფად:
ა) მომხმარებლის მიერ დაყენებული პაროლე;
ბ) სისტემის მიერ გენერირებული პაროლე;
გ) სისტემის მიერ გენერირებული შემთხვევითი კოდები;
დ) ნახევარსიტყვა;
ე) ფრაზა-გასაღები;
ვ) ინერაქტიული მიმდევრობა "კითხვა-პასუხი";
ზ)მკაცრი პაროლები.

პაროლი რომ იყოს საიმედო, ამისთვის ის უნდა აკმაყოფილებდეს შემდეგ მოთხოვნებს:
ა) უნდა იყოს განსაზღვრული სიგრძის;
ბ) უნდა შეიცავდეს როგორც მთავრულ, ისე ნუსხურ ასოებს;
გ) უნდა შეიცავდეს ერთ ან რამდენიმე ციფრს;
დ) უნდა შეიცავდეს ერთ არაციფრულ და ერთ არააალფაბეტურ სიმბოლოს.

პაროლური სისტემის ნაკლოვანებას წარმოადგენს ის, რომ დაინტერესებულ პირს სხვადასხვა ხერხების (მომსახურე პერსონალის მოსყიდვა, სატელეფონო ხაზებით გადაცემული ინფორმაციის მოძებნა დას ხვ) გამოყენებით სეუძლია გაიგოს საიდუმლო პაროლის მნიშვნელობა და მომხმარებლის სახელი.

მომხმარებლის მიერ პაროლის აუცილებელი დამახსოვრებისგან განთავისუფლება შესაძლებელია ე.წ. გასაღები-იდენტიფიკატორის გამოყენებით. ასეთი იდენტიფიკატორის როლს ასრულებს ინტელექტუალური (მიკროპროცესორული) ბარათი, რომელშიც ჩაწერილია მომხმარებლის სახელი და პაროლე. გაშვების ან მუშაობის პროცესში ქსელიდან მიღებული როგორც პაროლის, ისე სახელის მნიშვნელობები ედარება ბარათში ჩაწერილ მნიშვნელობებს და მხოლოდ თანხვედრის შემტხვევაში შესასრულებელ პროგრამას ეძლევა ოპერაციების სესრულების ნებართვა.

ელექტრონული გასაღები წარმოადგენს თანამედროვე და მოხერხებულ მოწყობილობას. მისი მეშვეობით შესაძლებელია ნებისმიერ აპარატულ – პროგრამულ დონეზე განხორციელდეს ინფორმაციული უშიშროების უზრუნველყოფის ამოცანების გადაწყვეტა. ელექტრონული გასაღების ნაირსახეობას წარმოადგენს გასაღები HASP (Hardware Adainst Software Piracy). ამ გასაღების ინტელექტუალური და ფიზიკური შესაძლებლობების განმსაზღვრელია სპეციალური მიკროსქემა Asic (Application Specific Integrated), რომლის ფუნქციონირების ლოგიკის რეალიზება სტანდარტული მიკროსქემების გამოყენებით პრაქტიკულად შეუძლებელია.

HASP გასაღები y=F(x) ფუნქციის გამოყენების საშუალებას იძლევა. x არისგასაღებში გასაგზავნი მთელი რიცხვი 0-დან 65535-მდე დიაპაზონში, ხოლო y გასაღების მიერ დაბრუნებული ოთხი მთელი რიცხვია იგივე დიაპაზონიდან.

რიცხვების გენერაციის მექანიზმის გამოყენება საგრძნობლად ართულებს კრიპტოანალიზის ამოცანას, რადგან ღია ან დაშიფრული ინფორმაცია გასაღების შესახებ არ ინახება არც პროგრამაში და არც გასაღების მეხსიერებაში.

ელექტრომაგნიტური ველების და გამოსხივებების მეშვეობით ინფორმაციის ხელში ჩაგდების თავიდან აცილების მეთოდებია:
ა) პასიური მეთოდი, რომლის დროსაც ხდება არასასურველი ელექტრომაგნიტური გამოსხივებისა და ველების ინტენსივობის შემცირება;
ბ) აქტიური მეთოდი, რომლის დროსაც ხდება ხმაურიანი ველების შექმნა;

გ) ფიზიკურად დაცული ელემენტებისა და ტექნოლოგიების გამოყენება (მაგალითად ოპტიკურ-ბოჭკოვანი კაბელები).

პასიური დაცვის მეთოდებს მიეკუთვნება: დაეკრანება, ფილტრაცია, დამიწება და გარეშე ელექტრომაგნიტური ველების შესუსტება.

დაეკრანება არასასურველი ელექტრომაგნიტური ველების ინტენსივობის შემცირების ერთ-ერთი ძირითადი მეთოდია. ამ დრო ხდება როგორც ინფორმაციული საშუალებების, მათი ელემენტების და შემაერთებელი ხაზების დაეკრანება, ისე იმ შენობების ნაწილობრივი ან სრული დაეკრანება, სადაც განლაგებულია ეს საშუალებები (დაეკრანებული შენობა, კონტეინერი და სხვ). ნაწილობრივი დაეკრანების საშუალებებია: მაეკრანებელი დაფის, მავთულბადის, მოლითონებული მინის, დენგამტარი ემალის, ფისის, საპოხი მასალების და სხვ. გამოყენება. უკანასკნელ წლებში ნაწილობრივი ან ლოკალური დაეკრანებისათვის გამოიყენება გამტარი პლასტმასისაგან დამზადებული ეკრანები, დიელექტრიკული ეკრანები, არმატურიანი მეტალის ბადეები ან ლითონური დაფრქვევით მიღებული ეკრანები.

ფილტრაციისას გამოიყენება დამცველი ფილტრები, რომელთა დანიშნულებაა სიხშირის ზოლში მოთავსებული სიხშირეების გატარება მნიშვნელოვანი შესუსტების გარეშე და სიხშირის ზოლის გარეთ მოთავსებული სიხშირეების ჩახშობა.

გარეშე ელექტრომაგნიტური ველების შესამცირებლად გამოიყენება: დამიწება, შთამთქმელი და არააამრეკლი საფარები, კაბელის ბოლოებში შეთანხმებული დატვირთვებისა და შთამნთქმელი მაღალსიხშირული ფერიტის რგოლების ჩართვა.

აქტიური დაცვის მეთოდებში იგულისხმება შეფერხებების ხელოვნურად შექმნა გარეშე ხმაურის შემოტანის გზით. გარეშე ელექტრომაგნიტური ხმაურის მისაღებად გამოიყენება სპეციალური გენერატორები და ანტენები. გენერატორი აფორმირებს მოცემული ენერგეტიკული და სპექტრული მახასიათებლების მქონე ხმაურიან ძაბვას და ამ ძაბვით ხდება ინფორმაციული სიგნალის დამახინჯება იმ ადგილებში, სადაც არსებობს ინფორმაციის გაჟონვის საშიშროება (კაბელი, სადენი და დენგამტარი კონსტრუქცია). სპეციალური ანტენის საშუალებით ხდება შენიღბული შეფერხებების გამოსხივება გარემომცველ სივრცეში.

აქტიური დაცვის მეთოდებში მეთოდის გამოყენებისას აუცილებლად უნდა იქნეს გამოკვლეული გარეშე ელექტრომაგნიტური ხმაურის ზემოქმედების შედეგები, როგორც დასაცველი მოწყობილობის, ისე ხმაურის ზონაში მოთავსებული სხვა ინფორმაციული მოწყობილობების მუშაობაზე. უარყოფითი ზემოქმედების შემთხვევაში ამ მეთოდის ნაცვლად გამოიყენება კოდური ხმაურის შემოტანის მეთოდი.

დაცვის საუკეთესო შედეგის მისაღწევად საჭიროა აქტიური და პასიური მეთოდების კომპლექსური გამოყენება. თუმცა უნდა აღინიშნოს, რომ მონაცემებისა და შეტყობინებების საიდუმლოების დაცვის ძირითად ხერხად ითვლება ინფორმაციის დაშიფვრა სხვადასხვა სახის კრიპტოგრაფიული მეთოდების გამოყენებით.

- **იდენტიფიკაცია და აუტენტიფიკაცია**

ობიექტის (მომხმარებლის) იდენტიფიკაცია ეს არის დაცვის ქვესისტემის ერთ-ერთი ფუნქცია. კომპიუტერულ ქსელთან დაკავშირებულ თითოეულ მომხმარებელს გააჩნია იდენტიფიკატორი. იდენტიფიკატორი შეიძლება იყოს რიცხვი, სიმბოლოების ერთობლიობა, ალგორითმი ან რაიმე სხვა სახის ისეთი ინფორმაცია, რომელიც ცალსახად იდენტიფიცირებს მომხმარებელს.

თუ მომხმარებელს გააჩნია ქსელში დარეგისტრირებული იდენტიფიკატორი, მაშინ იგი ითვლება კანონიერ (ლეგალურ) მომხმარებლად. წინააღმდეგ შემთხვევაში მომხმარებელი არაკანონიერია (არალეგალურია).

მომხმარებელი კომპიუტერულ ქსელში შესვლისას წინასწარ წარადგენს თავის იდენტიფიკატორს. ქსელში ხდება ამ იდენტიფიკატორის შედარება წინასწარ დამტკიცებულ ჩამონათვალთან და თუ იდენტიფიკაციის პროცედურა წარმატებით დამთავრდა, მაშინ მომხმარებელი ჩაითვლება კანონიერ მომხმარებლად. უნდა აღინიშნოს, რომ მარტო წარდგენილი იდენტიფიკატორით შეუძლებელია ქსელის დაცვა არაკანონიერი

მომხმარებლის მიერთებისგან. ამიტომ იდენტიფიკაციის შესრულების შემდეგ ხდება მომხმარებლის აუდენტიფიკაცია.

აუდენტიფიკაცია წარმოადგენს მომხმარებლის ნამდვილობის შემოწმებას. ამ პროცედურის დროს მოწმდება წარმოადგენს თუ არა მოხმარებელი ზუსტად იმას ვისი სახელითაც წარსდგა იგი. აუდენტიფიკაციისას გამოიყენება მომხმარებლის აუტენტიფიკატორი. ეს უკანასკნელი შეიძლება იყოს:

ა) მომხმარებლის განკარგულებაში არსებული წინასწარ განსაზღვრული ინფორმაცია (პაროლი, შეთანხმებული სპეციალური

კოდირებული ფრაზები);

ბ) მომხმარებლის განკარგულებაში არსებული აპარატული უზრუნველყოფილი ელემენტები (გასაღები, მაგნიტური ბარათი,

მიკროსქემა);

გ) მომხმარებლისათვის დამახასიათებელი განსაკუთრებული პირადი ნიშნები (თითების ანაბეჭდები, თვალის ბადურის

სურათი, ხმის ტემბრი);

დ) მომხმარებლისთვის დამახასიათებელი ქცევა (მუშაობისათვის საჭირო ხერხების გამოყენება რეალურ დროში, მუშაობის

სტილი კლავიატურაზე);

ე) მომხმარებლის ჩვევები და ცოდნა განპირობებული მისი აღზრდით, განათლებით, კულტურით, წეს-ჩვეულებებით და ა.შ.

იდენტიფიკაციისა და აუტენტიფიკაციის ჩატარების შემდეგ თუ დადგინდება მომხმარებლის კანონიერება, მაშინ მას მიეცემა ქსელის რესურსებთან დაკავშირების ნებართვა.

მონაცემების გადასაცემი არხების დაცვისას მომხმარებლის აუტენტიფიკაცია ნიშნავს კავშირის ხაზით ერთმანეთთან დაკავშირებული მომხმარებლის ნამდვილობის ურთიერთ დადგენას. როგორც წესი, აქუტენტიფიკაციის პროცედურა სრულდება მომხმარებლების ერთმანეთთან დაკავშირების პროცესის დასაწყისში. ამ პროცედურის მიზანია დარწმუნება იმაში, რომ შეერთება განხორციელებულია კანონიერ მომხმარებელთან და ინფორმაცია მიაღწევს დანიშნულ ადგილს.

აუტენტიფიკაციის შედეგად ხდება ელექტრონული დოკუმენტების დაცვა ისეთი არაკეთილსინდისიერი მოქმედებებისაგან, როგორიცაა: გადაცემული დოკუმენტის ხელში ჩაგდება ბოროტგანმზრახველის მიერ და მისი შინაარსის შეცვლა, სხვისი სახელით დაკავშირება ქსელის მომხმარებელთან, მიღებული დოკუმენტის შინაარსის შეცვლა ან დოკუმენტის მიღების უარყოფა, გაგზავნილი დოკუმენტის უარყოფა და სხვ.

აუტენტიფიკაციის პროცესები შეიძლება დაიყოს შემდეგ სახეობებად:

ა) მარტივი აუტენტიფიკაცია (პაროლების გამოყენება);

ბ) მკაცრი აუტენტიფიკაცია (კრიპტოგრაფიული მეთოდების და საშუალებების გამოყენება);

გ) აუტენტიფიკაციის პროცესი (პროტოკოლი) მომხმარებლის ნამდვილობის დამტკიცების შესახებ ნულოვანი ცოდნის შემთხვევაში.

9.1 აუტენტიფიკაციის მეთოდები

ტრადიციულად კომპიუტერული ქსელის ყველა კანონიერ მომხმარებელს ენიჭება საიდენტიფიკაციო ნომერი და პაროლი.

მუშაობის სეანსის დაწყების წინ მომხმარებელი მიუთითებს კომპიუტერულ სისტემას თავის საიდენტიფიკაციო ნომერს. მომხმარებლისაგან იდენტიფიკატორის მიღების შემდეგ სისტემა თხოვს მომხმარებელს პაროლის დასახელებას.

გამოყენებული პაროლის ჭეშმარიტებაში დასარწმუნებლად შეიძლება გამოყენებულ იქნეს მარტივი მეთოდი. კერძოდ, მომხმარებლის მიერ წარმოდგენილი Pa პაროლი შედარდება კომპიუტერულ ცენტრში შენახულ საწყისს P’a მნიშვნელობას. რადგან პაროლი ინახება საიდუმლოდ, ამიტომ დაუცველი არხით

გადაცემისას აუცილებელია მისი დაშიფვრა. თუ Pa და P'a მნიშვნელობები დაემთხვევა, მაშინ Pa პაროლი ითვლება ნამდვილ პაროლად, ხოლო მომხმარებელი კანონიერ მომხმარებლად

ნახ.9.1

ამ მეთოდის ნაკლი იმაში მდგომარეობს, რომ არაკანონიერ მომხმარებელს შეუძლია ქსელში ჩართვის უფლების მოპოვება, თუ იგი რაიმე ხერხით გაიგებს საიდენტიფიკაციო ნომერს და პაროლს.

ზოგჯერ საჭიროა, რომ მიმღებმა არ გახსნას პაროლის საწყისი ღია ფორმა. ამ შემტხვევაში გამგზავნმა პაროლის ღია ფორმის ნაცვლად უნდა გააგზავნოს ერთმიმართული ფუნქციით გარდაქმნილი პაროლი. ასეთმა გარდაქმნამ ხელი უნდა შეუშალოს არაკანონიერი მომხმარებლის ყველანაირ მცდელობას, რომელიც პაროლის გასახსნელად იქნება მიმართული.

ერთმიმართული ფუნქცია შეიძლება განისაზღვროს, როგორც

$$a(P)=E_P(ID),$$

სადაც P არის გამგზავნის პაროლი; ID - გამგზავნის საიდენტიფიკაციო ნომერი; Ep-P პაროლის გასაღებად გამოყენებისას განხორციელებული დაშიფვრის პროცედურა.

ასეთი ფუნქცია ძალიან მოსახერხებელია, თუ პაროლისა და გასაღების სიგრძეები ერთი და იგივეა. ამ შემტხვევაში პაროლის ჭეშმარიტებაში დასარწმუნებლად მიმღები ადარებს a(P)-ს წინასწარ გამოთვლილ და დამახსოვრებულ a'(P) ეკვივალენტთან.

პრაქტიკულად, ადვილად დამახსოვრების გამო, პაროლი შედგება რამდენიმე სიმბოლოსგან. მოკლე პაროლის ნაკლს წარმოადგენს მისი გაშიფვრის შესაძლებლობა კრიპტოანალიზური შეტევის განხორციელებისას. ამ ნაკლის უგულებელსაყოფად a(P) ფუნქცია განისაზღვრება, როგორც

$$a(P)=E_{P??Z}(ID)$$

სადაც z და ID, შესაბამისად, გამგზავნის გასაღები და საიდენტიფიკაციო ნომერია.

ცხადია, a(P)-ს მნიშვნელობა გამოითვლება წინასწარ და ინახება a'(P) სახით მიღების საიდენტიფიკაციო ცხრილში. მიმღები ახდენს a(P) და a'(P)-ს ერთმანეთთან შედარების

ნახ. 9.2

ქსელში ჩართულ ორ მომხმარებელს შორის კავშირის დამყარებისას საჭიროა ორივეს დარწმუნება პარტნიორის ნამდვილობაში. ურთიერთშემოწმებისას ძირითადად გამოიყენება პროცედურა, რომელიც ცნობილია სახელწოდებით "ხელის ჩამორთმევა".

ვთქვათ, ამ პროცედურის შესასრულებლად გამოყენებულია სიმეტრიული კრიპტოსისტემა და როგორც A, ისე B მომხმარებელი ფლობს ერთი და იგივე Z_{AB} საიდუმლო გასაღებს. პროცედურის მსვლელობა ნაჩვენებია 9.3 ნახ-ზე.

ნახ.9.3

ვთქვათ, პროცედურას იწვევს A მომხმარებელი. იგი გააგზავნის B მომხმარებელთან თავის იდენტიფიკატორს (ID_A) ღია ფორმით. B მომხმარებელი ID_A იდენტიფიკატორის მიღებისას იწყებს მონაცემთა ბაზაში Z_{AB} საიდუმლო გასაღების მოძებნას. მოძებნილ Z_{AB} გასაღებს B მომხმარებელი იყენებს თავის კრიპტოსისტემაში.

ამავე დროს, a მომხმარებელი PG ფსევდოშემთხვევითი გენერატორით აფორმირებს S შემთხვევით მიმდევრობას და გააგზავნის B მომხმარებელთან ამ მიმდევრობას კრიპტოგრამის სახით

$$E_{ZAB}(S)$$

B მომხმარებელი გაშიფრავს ამ მიმდევრობას და აღადგენს საწყისს S მიმდევრობას. შემდეგ ორივე მომხმარებელი გარდაქმნის S მიმდევრობას ღია ერთმიმართული a(·) ფუნქციის გამოყენებით, B მომხმარებელი შიფრავს a(s) სეტყობინებას და გააგზავნის კრიპტოგრამას a მომხმარებელთან.

ბოლოს, a მომხმარებელი ადარებს მიღებულ a'(S) სეტყობინებას საწყისს a(S) მნიშვნელობასთან. თუ a'(S) და a(S) ერთნაირია, მაშინ A მომხმარებელი თვლის B მომხმარებელს ნამდვილ პარტნიორად.

ზუსტად იგივე ალგორითმით რწმუნდება B მომხმარებელი A-ს ნამდვილ პარტნიორობაში (ე.ი. პროცედურას იწყებს B მომხმარებელი).

თუ მიმღებ მომხმარებლებს სურთ მოახდინონ გამგზავნის შემოწმება სეანსის მთელი ხანგრძლივობის განმავლობაში, მაშინ შემოწმების ალგორითმს ექნება 9.4 ნახ-ზე ნაჩვენები სახე.

ნახ.9.4

A მომხმარებელი გააგზავნის B მომხმარებელთან კრიპტოგრამას

$$Y=E_Z(ID_A'X),$$

სადაც ID_A არის გამგზავნის იდენტიფიკატორი, X - შეტყობინება.

B მომხმარებელი გაშიფრავს ამ კრიპტოგრამას და პოულობს ყოველი (ID_AX) წყვილიდან ID_A-ს. თუ მიღებული იდენტიფიკატორი ID_A დაემთხვევა დამახსოვრებულ ID'_A-ს, მაშინ B მომხმარებელი აღიარებს მიღებულ კრიპტოგრამას.

თუ იდენტიფიკატორის ნაცვლად გამოყენებული იქნება ორივე მომხმარებლისათვის ცნობილი საიდუმლო გასაღები, მაშინ განუწყვეტელი შემოწმების ალგორითმით ერთმანეთს შედარდება P_A და P_B პაროლების მნიშვნელობები. ამ შემთხვევაში A მომხმარებელი ადგენს კრიპტოგრამას.

$$Y=E_Z(P_A'X)$$

B მომხმარებელი მიღებული კრიპტოგრამის გაშიფვრით აღადგენს P_A-ს მნიშვნელობას და შეადარებს მას საწყისს P'_A-თან. ამ მნიშვნელობების თანხვედრისას მიმღები აღიარებს კრიპტოგრამას.

უნდა აღინიშნოს, რომ დაინტერესებულ არაკანონიერ მიმღებს შეუძლია პაროლის ხელში ჩაგდება შემჩნევით, გამოცნობით ან, უბრალოდ, მოპარვით. ამ გარემოების თავიდან ასაცილებლად გამოიყენება აუტენტიფიკაციის პროცედურა ერთჯერადი პაროლის (დინამიკური პაროლის) გამოყენებით. ასეთ შემთხვევაში ქსელში დაშვების ყოველი ახალი მოთხოვნის გაგზავნისას მომხმარებელი აგზავნის ახალ პაროლს.

დინამიკური პაროლის რეალიზაცია შესაძლებელია ისეთი მეთოდების გამოყენებით როგორიცაა: დროითი ჭდეების მექანიზმი ერთიანი დროის სისტემაში, მომხმარებლისთვის და შემმოწმებლისთვის სემტხვევითი პაროლების საერთო სიის შექმნა და მათი სინქრონიზაციის უზრუნველყოფა, ერთიანი საწყისი მნიშვნელობის მქონე შემთხვევითი რიცხვების გენერატორების მიერ. გასაღებების მნიშვნელობების გენერირება და სხვ.

თუ შემოვიტანთ შემდეგ აღნიშვნებს:

za- A მონაწილის მიერ გენერირებული შემთხვევითი რიცხვი;

zb – B მონაწილის მიერ გენერირებული შემთხვევითი რიცხვი;

ta-A მონაწილის მიერ გენერირებული დროის წდე;

Ek-k გასაღებით განხორციელებული სიმეტრიული გაშიფვრა (k გასაღები წინასწარ განაწილებულია A და B მონაწილეებს შორის),

მაშინ ცალმხრივი აუტენტიფიკაცია, რომელიც ემყარება დროითი ჭდეების მეთოდს იქნება:

$$A \quad B{:}E_k(t,B).$$

ამ შეტყობინების მიღებისა და გაშიფვრის შემდეგ, B მონაწილე რწმუნდება, რომ დროის t ჭდე ნამდვილია და შეტყობინებაში მითითებული იდენტიფიკატორის მნიშვნელობა B ემთხვევა მის საკუთარ მნიშვნელობას. ამ შეტყობინების ხელმეორედ გადაცემა გამოირიცხება, რადგან გასაღების მნიშვნელობის ცოდნის გარეშე შეუძლებელია t და B მნიშვნელობების შეცვლა.

ცალმხრივი აუტენტიფიკაცია, რომელიც ემყარება შემთხვევითი რიცხვების გამოყენებას, შემდეგია:

$$A \quad B: z_B;$$
$$A \quad B: E_K(z_B, B).$$

B მონაწილე აგზავნის A მონაწილესთან შემთხვევით z_b რიცხვს, A მონაწილე მიღებული z_B რიცხვისა და B იდენტიფიკატორისაგან შედგენილ შეტყობინებას შიფრავს და დაშიფრულ ტექსტს აგზავნის B მონაწილესთან. B გაშიფრავს მიღებულ შეტყობინებას და შეადარებს მასში არსებულ შემთხვევით რიცხვს მის მიერ გაგზავნილ რიცხვთან. დამატებით ხდება შეტყობინებაში მითითებული სახელის შემოწმება.

შემთხვევითი z_A და z_B რიცხვებით შესაძლებელია ორმხრივი აუტენტიფიკაციის ჩატარება. ამ შემთხვევაში:

$$A \quad B: z_B;$$
$$A \quad B: E_K(z_A, z_B, B),$$
$$A \quad B: E(z_A, z_B).$$

წინა შემთხვევისგან განსხვავებით, B მონაწილე დამატებით გაშიფრავს z_A რიცხვს და ჩართავს ამ რიცხვს A მონაწილესთან გასაგზავნ ბოლო შეტყობინებაში. z_A და z_B მნიშვნელობების შემოწმებით A მონაწილე რწმუნდება, რომ მას საქმე აქვს პირადად B მონაწილესთან.

აუტენტიფიკაციის პროტოკოლების განხორციელება შესაძლებელია აგრეთვე ერთმიმართული ჰეშ-ფუნქციების გამოყენებით (ნახ. 9.5).

ნახ. 9.5

K გასაღები წარმოადგენს ჰეშ-ფუნქციის პარამეტრს. $m=h_k(M)$ ჰეშ-ფუნქციის მნიშვნელობა ეგზავნება მიმღებს M შეტყობინებასთან ერთად. მიმღებმა იცის გადამცემის მიერ გამოყენებული ჰეშ-ფუნქციის მიღების ალგორითმი და თვითონ მიიღებს M სეტყობინებებიდან $m'=h_k(M)$ ჰეშ-ფუნქციას. შემდეგ ხდება m და m' მნიშვნელობების ერთმანეთთან შედარება და m=m' პირობის შესრულებისას ჩაითვლება, რომ აუტენტიფიკაცია წარმატებით შესრულდა.

9.6 ნახ-ზე ნაჩვენებია ერთმიმართული ჰეშ-ფუნქციის გამოყენების მოერე ვარიანტი.

ნახ.9.6

ამ შემთხვევაში K გასაღები არ წარმოადგენს ჰეშ-ფუნქციის პარამეტრს და ჰეშ-ფუნქციის მიღება ხდება M და K გაერთიანებული შეტყობინების ჰეშირებით, ე.ი. $m=h(M,K)$. მიმღები იგივე K გასაღების M სეტყობინებაზე დამატებით ახდენს $m'=h(M,k)$ ჰეშ-ფუნქციის მიღებას და m=m' პირობის შემოწმებას.

როცა ქსელის მომხმარებელთა რაოდენობა იზომება მილიონობით, მაშინ მომხმარებელთა რეგისტრაცია იდენტიფიკატორისა და აუტენტიფიკატორის გამოყენებით პრაქტიკულად არარეალიზებადია. ასეთ სემტხვევაში გამოიყენება ციფრული ელექტრონული სერტიფიკატი, რომელიც წარმოადგენს მომხმარებლის პირადობის მოწმობას. სერტიფიკატი გაიცემა მომხმარებლის მოთხოვნაზე სპეციალური რწმუნებით აღჭურვილი ორგანიზაციების, ე.წ. სერტიფიცირების ცენტრების მიერ. მომხმარებლისთვის სერტიფიკატის გაცემის პროცედურა მოიცავს მისი ნამდვილობის სემოწმებას სერტიფიცირების ცენტრის მიერ.

ციფრული სერტიფიკატის გამოყენებისას კომპიუტერული ქსელი, რომელიც იძლევა მის რესურსებზე დაშვების ნებართვას, მისი მომხმარებლის შესახებ არავითარ ინფორმაციას არ ინახავს. მომხმარებელი მის შესახებ ინფორმაციას წარადგენს თვითონ სერტიფიკატის მეშვეობით.

სერტიფიკატზე მოცემულია შემდეგი სახის ინფორმაცია:

- სერტიფიკატის მფლობელის ღია გასაღები;
- სერტიფიკატის მფლობელის მონაცემები (სახელი, ელექტრონული მისამართი, იმ ორგანიზაციის დასახელება, რომელშიც იგი მუშაობს და ა.შ.);
- სერტიფიკატის გამცემი ორგანიზაციის დასახელება;
- სერტიფიკატის გამცემი ორგანიზაციის ელექტრონული ხელმოწერა.

ეს ინფორმაცია დაშიფრულია სერტიფიკატის გამცემი ორგანიზაციის საიდუმლო გასაღებით. ხელმოწერის გაშიფვრა ხდება სერტიფიკატის მფლობელის ღია გასაღებით.

კავშირის დამყარების შემდეგ აუცილებელია უზრუნველყოფილ იქნეს გადასაცემი ინფორმაციის დაცვის მოთხოვნების შესრულება. მიმღები დარწმუნებული უნდა იყოს მონაცემების წყაროს ნამდვილობაში და მიღებული მონაცემების სისწორეში, ხოლო გამგზავნი დარწმუნებული უნდა იყოს, რომ მის მიერ გაგზავნილი მონაცემები შეუცვლელად მიღებული აქვს სასურველ მიმღებს.

მიმღების დარწმუნება ხდება გამგზავნის ხელმოწერის მიღებით, ხოლო გამგზავნის დარწმუნება კი მიმღებიდან ჩაბარების დამადასტურებელი შეტყობინების მიღებით. ამ შემთხვევაში გამგზავნი ვერ უარყოფს ვერც შეტყობინების გაგზავნის ფაქტს და ვერც მის შინაარსს, ხოლო მიმღები ვერ უარყოფს ვერც შეტყობინების მიღების ფაქტს და ვერც მისი შინაარსის სისწორეს.

• ციფრული (ელექტრონული) ხელის მოწერა

ციფრული (ელექტრონული) ხელის მოწერის დადასტურების მეთოდი გამოიყენება მომხმარებლებს შორის სანქციონირებული და საიდუმლო დაკავშირების უზრუნველსაყოფად. თითოეული მომხმარებელი ახდენს საკუთარი როგორც საიდუმლო, ისე ღია გასაღების გენერაციას და შემდეგ ღია გასაღების მნიშვნელობას აგზავნის ყველა პარტნიორთან.

განვიხილოთ ორი მომხმარებლის (A-გამგზავნი, B-მიმღები) დაკავშირებისას ციფრული ხელმოწერის დადასტურების პროცესის შემსრულებელი სქემა.

A მომხმარებელი:

- შეირჩევს ორ დიდ მარტივ P და Q რიცხვებს. გამოთვლის $N=P\cdot Q$ და $\varphi(N)=(P-1)(Q-1)$;
- შეირჩევს საიდუმლო D და ღია E გასაღებებს შემდეგი პირობების გათვალისწინებით:
  E $\varphi(N)$, უსგ(E, $\Phi(N)$)=1, $D<N, E\cdot D=1(\text{mod } \Phi(N))$;
- შიფრავს S შეტყობინებას D გასაღებით: $C=S^D(\text{mod } N)$;
- მომხმარებელთან გააგზავნის შრიფტექსტს (S,C) წყვილის სახით (ე.ი. ხელმოწერილ S შეტყობინებას).
  B მომხმარებელი შიფრავს C-ს E გასაღებით: $S'=C^E(\text{mod}N)$.
  თუ აღმოჩნდა S'=S, მაშინ ჩაითვლება, რომ S შეტყობინება მიღებულია A მომხმარებლიდან.
  განვიხილოთ მაგალითი.
  ვთქვათ,

$$P=11,\ Q=13,\ E=7 \text{ და } S=5.$$
$$N=P\cdot Q=143,\ \varphi(N)=(P-1)(Q-1)=120,$$
$$E=7(7<120, \text{უსგ}(7,120)=1),$$
$$7\cdot D=1(\text{mod}120), D=103,$$
$$C=S^D(\text{mod}N)=S^{103}(\text{mod}143)=125,$$
$$S'=C^E(\text{mod}N)=125^7(\text{mod}143)=5, S=S'.$$

ხელის მოწერის ციფრული ალგორითმებია, აგრეთვე:

- ალგორითმი RSA;
- ელ-გამალის ალგორითმი;
- ალგორითმი DSA;
- ბრმად ხელის მოწერის პროტოკოლი;

- ედავო ხელის მოწერის ალგორითმი;
- აუტენტიფიკაციის პროტოკოლი ნულოვანი ცოდნის გადაცემით.

9.2.1 ალგორითმი RSA

ციფრული დოკუმენტის გამგზავნი (A) შეირჩევს ორ დიდ P და Q მარტივ რიცხვს, გამოთვლის $N=P\cdot Q$ და $\varphi(N)=(P-1)(Q-1)$ ნამრავლს, შეირჩევს E და D რიცხვებს შემდეგი პირობების გათვალისწინებით: $E<\varphi(N)$, უსგ $(E, \varphi(N))=1$, $D<N$, $E\cdot D=1(\text{mod } \varphi(N))$.

E წარმოადგენს ღია გასაღებს და რიცხვების (E,N) წყვილი ეგზავნება ყველას, ვისაც ესაჭიროება A-ს ხელმოწერის შემოწმება.

D წარმოადგენს A მხარის საიდუმლო გასაღებს და იგი ინახება მასთან. ალგორითმის განზოგადებული სქემა ნაჩვენებია 9.7 ნახ-ზე.

ნახ.9.7

გამგზავნი M შეტყობინების შეკუმშვით ახდენა m=h(M) ჰეშ-ფუნქციის მიღებას და ამ უკანასკნელის დაშიფვრას D გასაღებით ($S=m^D(\text{mod}N)$). B მიმღებს ეგზავნება S,E,N და M. მიმღები E და N რიცხვების მეშვეობით აღადგენს ჰეშ-ფუნქციის m' მნიშვნელობას და შეადარებს მას M შეტყობინების შეკუმშვით (შეკუმშვა ხდება იგივე მეთოდით) მიღებულ m ჰეშ-ფუნქციის მნიშვნელობას. m=m' პირობის შესრულებისას B მიმღები ადასტურებს A გამგზავნის ხელმოწერას.

9.2.2 ელ-გამალის ალგორითმი

გამგზავნი (A) შეირჩევს დიდ მარტივ P და G რიცხვებს, მთელ x რიცხვს $(1<x<(p-1))$, გამოთვლის ღია გასაღებს $y=G^x(\text{mod } P)$ და აგზავნის y-ს დოკუმენტების პოტენციურ მიმღებთან. x წარმოადგენს საიდუმლო გასაღებს და იგი ინახება A=სთან.

გამგზავნი M შეტყოვბინების ჰეშირებით ახდენს m=h() $(1<m<(P-1))$ ჰეშ-ფუნქციის მიღებას, შეირჩევს მთელ რიცხვს შემდეგი პირობების გათვალისწინებით: $(1<k<(P-1)$, უსგ$[k,(P-1)]=1$, გამოთვლის $a=G^k(\text{mod}P)$ მთელ რიცხვს და საიდუმლო გასაღებით გამოთვლის b მთელ რიცხვს $m=x\cdot a+k\cdot b(\text{mod}(P-1))$ განტოლებიდან. a და b რიცხვების წყვილი არის ციფრული ხელმოწერა, ე.ი. S=(a,b)./ მიმღებს ეგზავნება (M,a,b), ხოლო (x,k) წყვილი ინახება საიდუმლოდ შეტყობინების გამგზავნთან.

მიმღები მიღებული M შეტყობინებით ახდენს m=h(M) ჰეშფუნქციის მიღებას, გამოთვლის A=($y^a a^b$)mod P და აღიარებს M შეტყობინების უტყუარობას, თუ A=G^m(modP). ე.ი. მიმღები ამოწმებს ($y^a a^b$) modP=G^m(modP) ტოლობას.

უნდა აღინიშნოს, რომ ხელის მოწერის ეს ალგორითმი საფრთხოა მხოლოდ იმ შემთხვევაში, თუ ყოველი ახალი შეტყობინების გაგზავნისას ხელის მოწერა სრულდება k რიცხვის ახალი მნიშვნელობით და თანაც მისი შერჩევა ხდება შემთხვევითი სახით.

9.2.3 ალგორითმი DSA

გამგზავნი და მისი მიმღები გამოიყენებენ L რაოდენობის ბიტის შემცველ ორ დიდ მარტივ G და P რიცხვს (512<L<1024) და 160 ბიტის შემცველ q მარტივ რიცხვს, რომელიც P-1 სხვაობის გამყოფია და, ამასთან, აკმაყოფილებს პირობას G=$h^{(p-1)/q}$(modP>1, სადაც h მთელი რიცხვია (1, P-1) შუალედიდან.

გამგზავნი საიდუმლო გასაღებად შეირჩევს 160 ბიტის შემცველ მთელ x რიცხვს (1<x<q) და გამოთვლის y=G^x(modP). y რიცხვი, რომელიც წარმოადგენს ღია გასაღებს, ეგზავნება ყველა მომხმარებელს და გამოიყენება გამგზავნის ხელმოწერის შესამოწმებლად.

გამგზავნი ანიჭებს M შეტყობინებას საიდუმლო K ნომერს (0<K<q) და ასრულებს ხელის მოწერიას (r,s) წყვილის გამოთვლის გზით, სადაც r=(G^kmodP)modq და ?????????????????? s=????????????? modq (H(M)-M შეტყობინების ჰეშ-კოდია და იგი მიღებულია SHA-1 მეთოდით).

მიმღებს ეგზავნება M შეტყობინება და ხელმოწერა (r,s). მიმღები M შეტყობინების შეკუმშვცით ახდენს H(m) ჰეშ-კოდის მიღებას და შემდეგი გამოთვლების შესრულებას:

W=???????modq, U_1=[H(M)W]modq, U_2=(r·W)modq, v=[(G^{U_1}·Y^{U_2})modP]modq.

v=r პირობის შესრულებისას მიმღები რწმუნდება გამგზავნის ხელმოწერის უტყუარობაში.

DSA ალგორითმის ნაკლს წარმოადგენს გაყოფის რთული ოპერაციების შესრულება

9.2.4 ბრმად ხელის მოწერის პროტოკოლი

ეს ალგორითმი წარმოადგენს შეტყობინების გამგზავნ A მხარესა და ამ შეტყობინებაზე ხელის მომწერ B მხარეს შორის ორმხრივ პროტოკოლს. ამ ალგორითმის დანიშნულება იმაში მდგომარეობს, რომ ხელის მომწერმა მხარემ ვერ შეძლოს მიღებული შეტყობინების (რომელსაც თვითონ აწერს ხელს) შინაარსის გაგება და ამ შეტყობინებაზე ხელმოწერის გარკვევა.

ალგორითმის ძირითადი იდეა შემდეგში მდგომარეობს: A აგზავნის B მხარესთან ინფორმაციის პორციას და ეს ინფორმაცია უნბრუნდება უკან B მხარის ხელმოწერით. A მხარეს შეუძლია გამოთვალოს B მხარის ხელმოწერა მისთვის მნიშვნელოვან M შეტყობინებაზე. ამ პროტოკოლის დამთვარებისას B მხარემ არაფერი იცის როგორც შეტყობინების, ისე ხელმოწერის შესახებ.

ამ ალგორითმის გამოყენება შესაძლებელია ანონიმურ უნაღდო ანგარიშსწორების ჩასატარებლად. მაგალითად, B ბანკის A კლიენტს სურს ფულის დახარჯვა ისე, რომ დარჩეს ანონიმურ მეანაბრედ.

პროტოკოლის შესადგენად საჭიროა შემდეგი დოკუმენტები:

ა) ჩვეულებრივი ხელის მოწერის ალგორითმი (მაგალითად, RSA);

ბ) f(·) და g(·) ფუნქციები, რომლებიც ცნობილია მხოლოდ შეტყობინების გამგზავნი A მხარესათვის. ეს ფუნქციები აკმაყოფილებენ შემდეგ პირობას: g(S_b(f(m)))=S(m) და, ამასთან, f(·) არის შესანიღბავი ფუნქცია, g(·) - შენიღბვის მომხსნელი ფუნქცია, f(m) - შენიღბული და m შეტყობინება, ხოლო S - შეტყობინებაზე B მხარის მიერ შესრულებული ხელმოწერა.

უნდა აღინიშნოს, რომ S, f და g-ს შერჩევა ხდება მთელი რიგი შეზღუდვებით.

დავუშვათ, B მხარეს ხელის მოწერის ალგორითმად გამოყენებული აქვს RSA ალგორითმი ღია (N,E) და საიდუმლო D გასაღებებით. ე.ი. $N=P\cdot Q$ (P და Q მთელი მარტივი რიცხვებია), $\varphi(N)=(P-1)(Q-1)$, $1<E<\Phi(N)$, $E\cdot D=1(\mathrm{mod}\ \Phi(N))$.

A მხარე შეირჩევს შემთხვევით K მთელ რიცხვს ($0<k<N$, უსგ $(N,K)=1$), გამოთვლის შრენიღბულ $m'=(m\cdot k^E)\mathrm{mod}N$ შეტყობინებას და აგზავნის ამ შეტყობინებას B მხარესთან.

B მხარე გამოთვლის ხელმოწერას $S'=(m')^D\mathrm{mod}N$ და აგზავნის მას A მხარესთან.

A მხარე გამოთვლის $S=(K^{-1}\cdot S)\mathrm{mod}N$ ხელმოწერას, რომელიც წარმოადგენს m შეტყობინებაზე B მხარის ხელმოწერას საიდუმლო D გასაღებით. მართლაც,

$S=K^{-1}\cdot S=K^{-1}\cdot(m)^D=K^{-1}\cdot(m\cdot K^E)^D=K^{-1}\cdot m^D\cdot K^{ED}=K^{-1}\cdot K\cdot m^D=m^D(\mathrm{mod}N)$,

სადაც $K\cdot K^{-1}=1(\mathrm{mod}N)$.

განვიხილოთ მაგალითი.

$P=3,Q=11,E=7,m=9,K=5$,
$N=P\cdot Q=33$, $\Phi(N)=(P-1)(Q-1)=20,7\cdot D=1(\mathrm{mod}20)$ და $=3$,
$m'=(m\cdot K^E)\mathrm{mod}N=(9\cdot 5^7)\mathrm{mod}33=27$,
$S'=(m)^D\mathrm{mod}N=27^3(\mathrm{mod}33)=15$,
$5\cdot K^{-1}=1(\mathrm{mod}33)$, $K^{-1}=20$,
$S=(K^{-1}\cdot S')\mathrm{mod}N=(20\cdot 15)\mathrm{mod}33=3$,
$S=m^D(\mathrm{mod}N)=9^3(\mathrm{mod}33)=3$.

9.2.5 უდავო ხელის მოწერის ალგორითმი

უდავო ხელის მოწერის ალგორითმი ჩვეულებრივი ალგორითმისაგან იმით განსხვავდება, რომ ხელის მოწერის დადასტურება მომწერის გარეშე შეუძლებელია.

უდავო ხელის მოწერის შესრულების საჭიროება შეიძლება აიხსნას შემდეგ მაგალითზე. დავუშვათ, A არის პროგრამული უზრუნველყოფის პაკეტის შემქმნელი ცნობილი კორპორაცია და ან პაკეტის მყიდველია B, რომლის დასარწმუნებლად იმაში, რომ პაკეტი ორიგინალია და არ შეიცავს ვირუსებს, A ხელს აწერს პაკეტს უდავო ხელის მოწერის ალგორითმის შესაბამისად. ასეთი ხელმოწერის შესრულებით გამორიცხულია B მყიდველის მიერ პაკეტის ასლის გადაღება და მისი მიყიდვა სხვა C კლიენტისათვის, რადგან B მყიდველს არ შეუძლია A გამყიდველის გარეშე დაარწმუნოს C მყიდველი, რომ პაკეტი ორიგინალია და არ შეიცავს ვირუსებს.

უდავო ხელის მოწერის ალგორითმი შემდეგში მდგომარეობს:

- ხელის მომწერი A მხარე ასრულებს შემდეგ ოპერაციებს:

ა)შეირჩევს შემთხვევით მარტივ მთელ $P=2q+1$ რიცხვს,სადაც q მარტივი მთელი რიცხვია;

ბ) $z=\{2,\ldots,P-1\}$ სიმრავლიდან შეირჩევს შემთხვევით β რიცხვს და გამოთვლის $\alpha=\beta^{(p-1)/p}\mathrm{mod}P$:· $\alpha>1$ პირობის შესრულებით (თუ $\alpha=1$, მაშინ შეირჩევა β-ას ახალი მნიშვნელობა);

გ) $\{1,2,\ldots,q-1\}$ სიმრავლიდან შეირჩევას შემთხვევით x რიცხვს (საიდუმლო გასაღებს) და გამოთვლის $y=\alpha^x(\mathrm{mod}P)$;

დ) გამოთვლის $S=mx(\mathrm{mod}P)$, სადაც m წარმოადგენს შეტყობინებას.

ამ ოპერაციების შესრულების შემდეგ A მხარე აგზავნის B მხარესთან $\{(P,\alpha,y),(S,m)\}$ სიმრავლეს, სადაც $\{(P,\alpha,y)$ არის ღია გასაღები, ხოლო S-ხელმოწერა გადაცემულ შეტყობინებაზე.

B მხარე საიდუმლოდ შეირჩევს $\{1,2,\ldots,q-1\}$ სიმრავლიდან ორ a და b რიცხვს, გამოთვლის $z=(S^a\cdot y^b)\mathrm{mod}P$ რიცხვს და აგზავნის ამ უკანასკნელს A მხარესთან.

A მხარე გამოთვლის $w=(z)^{1/x}\mathrm{mod}P$, სადაც $x\cdot x^{-1}=1(\mathrm{mod}q)$ და აგზავნის w-ს B მხარესთან.

B მხარე გამოთვლის $w'=(m^a a^b)\mathrm{mod}P$ და $w=w'(\mathrm{mod}q)$ პირობის შესრულებისას ცნობს A მხარის ხელმოწერას S-ს, როგორც ორიგინალს. მართლაც: $w=z^{1/x}=(S^a y^b)^{1/x}=(m^{ax}a^{bx})^{1/x}=(m^a a^b)\mathrm{mod}P=w'(\mathrm{mod}q)$.

განვიხილოთ მაგალითი.
ვთქვათ, q=11, β=17, x=8, m=5, a=3 და b=5. ალგორითმის მიხედვით გამოთვლების შესრულებისას მივიღებთ:

$$P=2q+1=2\cdot 11+1=23,$$
$$\alpha=\beta^{(p-1)/q}\ (\mathrm{mod}P)=17^{2}(\mathrm{mod}23)=13>1,$$
$$y=a^{x}(\mathrm{mod}P)=13^{8}(\mathrm{mod}23)=2,$$
$$(P,\alpha,y)\qquad(23,13,2),$$
$$S=m^{x}(\mathrm{mod}P)=5^{8}(\mathrm{mod}23)=16,$$
$$(S,m)\qquad(16,5),$$
$$z=(S^{a}y^{b})\mathrm{mod}P=(16^{3}\cdot 2^{5})\mathrm{mod}23=18,$$
$$x\cdot x^{-1}=1(\mathrm{mod}q)\qquad 8\cdot x^{-1}=1(\mathrm{mod}11)\qquad x^{-1}=7,$$
$$w=(z)^{x^{-1}}\mathrm{mod}P=18^{7}(\mathrm{mod}23)=6,$$
$$w'=(m^{a}\cdot a^{b})\mathrm{mod}P=(5^{3}\cdot 13^{5})\mathrm{mod}23=17,$$
$$w=w'(\mathrm{mod}q)\qquad 6=17(\mathrm{mod}11).$$

ე.ი. B მხარე ცნობს A მხარის ხელმოწერას.

9.3. აუტენტიფიკაციის პროტოკოლი ნულოვანი ცოდნის გადაცემით

ინტელექტუალური ბარათების უსაფრთხო გამოყენებას უზრუნველყოფს აუტენტიფიკაციის პროტოკოლი ნულოვანი ცოდნის გადაცემით.

თუ ინტელექტუალური ბარათი წარმოადგენს A მხარეს, ხოლო შემმოწმებელია B მხარე, მაშინ A მხარემ უნდა დაუმტკიცოს B მხარეს თავისი ნამდვილობა. ორივე მხარისათვის ცნობილია N მოდულისა და v ხარისხის მაჩვენებლის მნიშვნელობები (N წარმოადგენს საიდუმლოდ შერჩეული ორი მარტივი P და Q რიცხვის ნამრავლს). A მხარის საიდენტიფიკაციო ინფორმაცია წარმოადგენს ბიტებოის შემცვალ Y სტრიქონს. Y შეიცავს ბარათის მფლობელის სახელს, ბარათის მოქმედების ვადას, საბანკო ანგარიშის ნომერს და სხვ. A მხარის საიდუმლო გასაღებს წარმოადგენს ისეთი G სიდიდე, რომელიც აკმაყოფილებს თანაფარდობას

$$Y\cdot G^{v}=1(\mathrm{mod}N)$$

A მხარე გააგზავნის B მხარესთან Y მონაცემებს და შემდეგ იწყებს B მხარისათვის იმის დამტკიცებას, რომ საიდენტიფიკაციო მონაცემები ეკუთვნის სწორედ მას. თუ A დაარწმუნებს B-ს, რომ მისი საიდუმლო გასაღებია G(G-ს მნიშვნელობის გაგზავნის გარეშე), მაშინ B დარწმუნდება A-ს ნამდვილობაში.

A-ს ნამდვილობის დამამტკიცებელ პროტოკოლს, B მხარისათვის G-ს მნიშვნელობის გადაუცემელ, აქვს შემდეგი სახე:

- A მხარე შეირჩევს შემთხვევით r მთელ რიცხვს ($0<r\le N-1$), გამოთვლის $T=r^{v}\mathrm{mod}N$ და გააგზავნის T მნიშვნელობას B მხარესთან;
- B მხარე შეირჩევს შემთხვევით d მთელ რიცხვს ($0<d\le N-1$) და გააგზავნის ამ მნიშვნელობას A-სთან;
- A მხარე გამოთვლის $D=(r\cdot G^{d})\mathrm{mod}N$ და გააგზავნის D მნიშვნელობას B-სთან;
- B მხარე გამოთვლის $T'=(D^{v}Y^{d})\mathrm{mod}N$.

რადგან $T'=D^{v}Y^{d}=(rG^{d})^{v}Y^{d}=r^{v}G^{dv}Y^{d}=r^{v}(YG^{v})^{d}=r^{v}=T(\mathrm{mod}N)$, ამიტომ A მხარის ნამდვილობის შემოწმება მთავრდება წარმატებით.

განვიხილოთ მაგალითი. ვთქვათ, y=23, P=5, Q=7 და v=5.

$y\cdot G^{v}=1(\mathrm{mod}N)\qquad(23\cdot G^{5})\mathrm{mod}35=1\qquad G^{5}=32\qquad G=2.$

A მხარე შეირჩევს r=9 და გამოთვლის $T=rv\mathrm{mod}N=95\mathrm{mod}35=4$

B მხარე შეირჩევს d=11.

A მხარე გამოთვლის $D=(r\cdot G^{d})\mathrm{mod}N=(9\cdot 2^{11})\mathrm{mod}35=22.$

B მხარე გამოთვლის $T'=(D^v \cdot Y^d) \text{mod} N=(22^5 \cdot 23^{11}) \text{mod} 35=4$.

T=T' და B მხარე რწმუნდება A მხარის ნამდვილობაში G-ს გაგზავნის გარეშე.

აუტენტიფიკაციის განხორციელება ნულოვანი ცოდნის გადაცემით შეიძლება, აგრეთვე ე.წ. გამარტივებული სქემით და პარალელური სქემით. ორივე სქემაში ერთი მხარე (A) უმტკიცებს მეორე მხარეს (B) თავის ნამდვილობას, ხოლო მეორე მხარე (B) ამოწმებს A მხარის მტკიცებულებას.

აუტენტიფიკაციის გამარტივებული სქემით განხორციელებისას სანდო არბიტრის (ცენტრის) მიერ A და B მომხმარებლებისათვის შეირჩევა N მოდულის მნიშვნელობა, რომელიც წარმოადგენს ორი დიდი მარტივი რიცხვის ნამრავლს. მოდულის მნიშვნელობის მიხედვით არბიტრი A მხარის ღია გასაღებად შეირჩევს a რიცხვს, რომელიც წარმოადგენს კვადრატულ გამონაქვითს N მოდულით (მოკლე ცნობების ნახვა კვადრატული გამონაქვითის შესახებ შესაძლებელია დანართში). ე.ი. $x^2=a(\text{mod}N)$. შემდეგ ხდება A მხარის საიდუმლო S გასაღების უმცირესი მნიშვნელობის განსაზღვრა შემდეგი თანაფარდობის მიხედვით:

$S=\text{sqrt}(a^{-1})(\text{mod}N)$, სადაც a^{-1} არის a-ს შებრუნებული მულტიპლიკატიური N მოდულით, ხოლო sqrt აღნიშნავს კვადრატულ ფესვს.

N,a და S მნიშვნელობის საშუალებით მიმდინარეობს აუტენტიფიკაციის პროტოკოლი შემდეგი თანმიმდევრობით:

- A მხარე შეირჩევს შემთხვევით r(r<N) რიცხვს, გამოთვლის $x=r^2(\text{mod}N)$ და აგზავნის x-ს B მხარეშსთან;
- B მხარე აგზავნის A-სთან შემთხვევით b ბიტს (b=0 ან b=1);
- თუ b=0, მაშინ A აგზავნის B -სთან r-ს, ხოლო თუ b=1, მაშინ A ააგზავნის $y=(r \cdot S)\text{mod}N$;
- თუ b=0, მაშინ B მხარე ამოწმებს $x=r^2(\text{mod}N)$ ტოლობას, რათა დარწმუნდეს ,რომ A მხარემ იცის sqrt(x);
  თუ b=1, მაშინ B მხარე ამოწმებს $x=(y^2 \cdot a)\text{mod}N$, რათა დარწმუნდეს, რომ A მხარემ იცის $\text{sqrt}(a^{-1})$.

განვიხილოთ ოთხი ბიჯი წარმოადგენს პროტოკოლის ერთ ციკლს და მას აკრედიტაცია ეწოდება. A და B მხარეები ასეთ ციკლებს იმეორებენ რამდენჯერმე r და b სხვადასხვა მნიშვნელობებისათვის მანამ, სანამ B არ დარწმუნდება იმაში, რომ A მხარემ იცის S-ის მნიშვნელობა.

r-ის მნიშვნელობის გამეორება A მხარის მიერ დაუშვებელია, რადგან, ასეთ შემთხვევაში, თუ B მხარე მეორე ბიჯზე გააგზავნის საპირისპირო მნიშვნელობის მქონე მქონე b-ს, მაშინ B-ს ექნება A მხარის ორივე პასუხი და იგი ადვილად გამოთვლის S -ის მნიშვნელობას.

აუტენტიფიკაციის პარალელური სქემით განხორციელებისას N შეირჩევა ისე, როგორც გამარტივებულ სქემაში. A მხარის ღია გასაღებად აიღება $a_1,a_2\ldots..a_k$ რიცხვებისაგან შედგენილი სტრიქონი, სადაც თითოეული a_i წარმოადგენს კვადრატულ გამონაქვითს N მოდულით. შემდეგ გამოითვლება A მხარის საიდუმლო გასაღები $S_1,S_2\ldots.,S_k$, სადაც S_i წარმოადგენს $S_i=\text{sqrt}(a_i^{-1})\text{mod}N$ გამოსახულების უმცირეს მნიშვნელობას.

აუტენტიფიკაციის პროტოკოლს აქვს შემდეგი სახე:

- A მხარე შეირჩევს შემთხვევით r(r<N) რიცხვს, გამოთვლის $x=r^2(\text{mod}N)$ და აგზავნის x-ს B მხარესთან.
- B მხარე აგზავნის A-სთან k რაოდენობის ბიტისგან შედგენილ შემთხვევით ოროობით სტრიქონს $b_1,b_2\ldots.,b_k$.
- A მხარე გამოთვლის $y=[r \cdot (S_1^{b1} \cdot S_2^{b2},\ldots S_k^{bk})]\text{mod}N$ (ამრავლებს მხოლოდ იმ Si მნიშვნელობებს, რომლებისთვისაც bi=1) და აგზავნის y-ს B მხარესთან.
- B მხარე ამოწმებს, რომ $x=[y^2 \cdot (a_1^{b1} \cdot a_2^{b2},\ldots a_k^{bk})]\text{mod}N$.
  A და B მხარეები ამ პროტოკოლს იმეორებენ მანამ, სანამ B არ დარწმუნდება იმაში, რომ A მხარემ იცის $S_1,S_2\ldots.,S_k$.

განვიხილოთ მაგალითი. ვთქვათ, N=35=5·7. კვადრატული გამონაქვითები იქნება 1, 4,9,11,16,29. თუ შევადგენთ ცხრილს a,a^{-1} და S მნიშვნელობებით მიიღება (ცხრილი 9.1)

ცხრილი 9.1.

a	a-1	S=Sqrt(a-1)
1	1	1
4	9	3
9	4	2
11	16	4
16	11	9
29	29	8

მაშასადამე A მხარის ღია გასაღები, თუ K=4, იქნება a=[4,11,16,29], ხოლო შესაბამისი საიდუმლო გასაღები - კი S=[3,4,9,8].

პროტოკოლის ერთი ციკლი სრულდება შემდეგნაირად:

- A მხარე შეირჩევს r=16, გამოთვლის x=162(mod35)=11 და აგზავნის x=11 B-სთან;
- B მხარე აგზავნის A-სთან შემთხვევით ორობით სტრიქონს [1,1,0,1];
- A მხარე გამოთვლის $y=[r\cdot(S_1^{b1}\cdot S_2^{b2},\ldots..S_k^{bk})]modN=[16\cdot(3^1\cdot4^1\cdot9^0\cdot8^1)]mod35=31$ და აგზავნის B-სთან;
- B მხარე ამოწმებს

$x=[y^2\cdot(a_1^{b1}\cdot a_2^{b2},\ldots..a_k^{bk}]modN=[31^2\cdot(4^1\cdot11^1\cdot16^0\cdot29^1)]mod35=11.$

10. ელექტრონული ფოსტის დაცვა

ელექტრონული ფოსტის ფუნქციონირებისათვის აუცილებელია აუტენტიფიკაციის და კონფიდენციალურობის უზრუნველყოფა. თანამედროვე ეტაპზე ელექტრონული ფოსტის დაცვისათვის გამოიყენება (PGP(Pretty Good Privacy) ან S/MIME(Secure/Multipuprose Internet Mail Extension) სისტემა. განვიხილოთ PGP სისტემა.

PGP სისტემა დამუშავებულია ფილიპე ციმერმანის მიერ. ამ სისტემაში გამოყენებულია: თანამედროვე კრიპტოგრაფიული ალგორითმები (RSA/SHA, IDEA ან სამგასაღებიანი DES ალგორითმი, დიფი-ჰელმანის ან ელ-გამალის ალგორითმი და სხვ), მონაცემთა შეკუმშვის ალგორითმი (ZIP), დაშიფრული შეტყობინების ASCII კოდში გარდამქმნელი (Radix 64), სხვადასხვა სახის გასაღებეი (სეანსური, ღია, საიდუმლო) და სხვ.

10.1 ნახ-ზე ნაჩვენებია PGP სისტემის სტრუქტურული სქემა.

ნახაზზე გამოყენებულია შემდეგი აღნიშვნები:

M-შეტყობინება; H-ჰეშირების ფუნქცია; Z-შეკუმშვა ZIP ალგორითმით (კომპრესია); EC-დაშიფვრა სეანსური გასაღებით (დაშიფვრის ტრადიციული სქემა); Ks-სეანსური გასაღები; KU_a და KU_b -ღია გასაღებები; KRb-მიმღების

პირადი გასაღები; DP - ღია გასაღების დაშიფვრის სქემა; DC-გაშიფვრა ტრადიციული გაშიფვრის სქემით; Z^{-1} - დეკომპრესია.

ამ სისტემით ხდება აუტენტიფიკაციის და კონფიდენციალურობის უზრუნველყოფა. გადამცემი და მიმღები მხარეები ასრულებენ შემდეგ პროცედურებს: გადამცემი მხარე აფორმირებს M შეტყობინებას და 128 ბიტის შემცველ ერთჯერად სეანსურ გასაღებს (Ks); SHA ალგორითმის გამოყენებით ახდენს 512 ბიტის შემცველი M შეტყობინების ბლოკის ჰეშირებას და 160 ბიტის შემცველი ჰეშ-კოდის მიღებას; ჰეშ-კოდს შიფრავს RSA კრიპტოსისტემისა და KRa პირადი გასაღების გამოყენებით; გაერთიანებულ M შეტყობინებას და ჰეშ-კოდს კუმშავს ZIP ალგორითმით (აკეთებს კომპრესიას); შეკუმშნსური ულ ინფორმაციას შიფრავს IDEA ან 3DES ალგორითმისა და სეანსური Ks გასაღების გამოყენებით; Ks გასაღებს შიფრავს RSA კრიპტოსისტემისა და პირადი გასაღების გამოყენებით ახდენს სეანსური გასაღების გაშიფვრას; სეანსური გასაღებით გაშიფრავს მიღებულ ინფორმაციას; გაშიფრული შეტყობინების დეკომპრესიის შედეგად აღადგენს M შეტყობინებას და დაშიფრულ ჰეშ-კოდს; გადამცემის ღია გასაღებით გაშიფრავს ჰეშ-კოდს და ამ უკანასკნელს შეადარებს აღდგენილი M შეტყობინების ჰეშირებით მიღებულ ჰეშ-კოდს.

ამ სისტემით შესაძლებელია, აგრეთვე, მხოლოდ აუტენტიფიკაციის (ნახ.10.2) ან მხოლოდ კონფიდენციალურობის უზრუნველყოფა (ნახ. 10.3).

ღია გასაღებების გაცვლა (KUa და KUb) ხორციელდება დიფი-ჰელმანის ალგორითმით.

PGP სისტემაში გადასაცემი ინფორმაციის მთლიანი ბლოკი ნაწილობრივ (მხოლოდ აუტენტიფიკაცია) ან სრულად (მხოლოდ კონფიდენციალურობა) წარმოადგენს რვაბიტიანი ნებისმიერი ბიტების ნაკადს. ეს კი ელექტრონული ფოსტის მრავალი სისტემისათვის დაუშვებელია, რადგან ისინი იყენებენ მხოლოდ ASCII კოდის შესაბამისი სიმბოლოებისაგან შედგენილ ბლოკებს. ასეთი შეზღუდვის მოსახსნელად PGP სისტემა მოიცავს სერვისს (Radix-64), რომლითაც ხდება რვაბიტიანი ორობითი ნაკადის კონვერტაცია ASCII კოდის სიმბოლოებად.

Radix-64 -ით ორობითი სიმბოლოებისაგან შედგენილი სამბაიტიანი ჯგუფი გარდაიქმნება ASCII კოდის ოთხ სიმბოლოდ და თანაც თითოეულ სიმბოლოს ემატება ერთი საკონტროლო სიმბოლო მონაცემების გადაცემისას შეცდომების აღმოსაჩენად (კოდი ლუწობის ან კენტობის შემოწმებით). ე.ი. ამ სერვისის გამოყენებისას გადაცემული შეტყობინების სიგრძე იზრდება 33%-ით.

Radix-64-ით ორობითი სიმბოლოებისაგან შედგენილი სამბაიტიანი ჯგუფი (24 ბიტი) იყოფა ექვსბიტიან ჯგუფებად, თითოეული ჯგუფის ორობითი კომბინაციის შესაბამისი ათობითი რიცხვით განისაზღვრება შესატყვისი სიმბოლო Radix-64-ის კოდირების ცხრილის მიხედვით (ცხრილი 10.1) და ეს სიმბოლო შეიცვლება იგივე სიმბოლოთი, ოღონდ ASCII კოდით.

11. Internet ქსელიდანა განხორციელებული შემოტევების აცილების მეთოდები და საშუალებები

გლობალური ქსელი Internet -ი წარმოადგენს ღია სისტემის და მისი დანიშნულებაა ინფორმაციის თავისუფალი გაცვლა. ღია სისტემის იდეოლოგია კი ბოროტგანმზრახველს საშუალებას აძლევს შეაღწიოს ქსელში და განახორციელოს:

- კონფიდენციალურ ინფორმაციასთან არასანქცირებული მიერთება;
- მნიშვნელოვანი ინფორმაციის პირის გადაღება;
- პაროლების, სერვერების მისამართებისა და სერვერების შიგთავსის გაგება;
- ლოკალური ქსელის ინფორმაციულ სისტემაში დარეგისტრირებული მომხმარებლის სახელით შეღწევა და ა.შ.

მიღებული ინფორმაციით ბოროტგანმზრახველს შეუძლია მნიშვნელოვანი ზიანი მიაყენოს ლოკალური ქსელის მფლობელის (ფირმა, საწარმო, ბანკი და სხვ) კონკურენტუნარიანობას და გამოიწვიოს მისი კლიენტების ნდობის დაკარგვა.

ლოკალური კომპიუტერურლი ქსელის ბოროტგანმზრახველისაგან დასაცავად გამოიყენება ქსელთაშორისი ეკრანი (ნახ.11.1).

ნახ.11.1.

ქსელთაშორისი ეკრანი წარმოადგენს დაცვის სისტემას, რომელიც აცალკევებს ლოკალურ ქსელს Internet ქსელიდან ან კორპორაციული Intranet ქსელიდან და გარკვეული წესების მიხედვით განსაზღვრავს მონაცემების პაკეტების გატარების პირობებს ლოკალურ ქსელსა და გარე ქსელს შორის.

მიუხედავად იმისა, რომ არც ერთი ქსელთაშორისი ეკრანი არ იძლევა ლოკალური ქსელის დაცვის სრულ გარანტიას, მისი დაყენება აუცილებელია, რადგან მის გარეშე შიგა ქსელის სისტემები განიცდიან შემოტევის საშიშროებას გარე ქსელიდან. Internet ქსელიდან შემოტევის განხორციელებას ხელს უწყობს იმ "თანდაყოლილი" ნაკოვანებების (სუსტი ადგილების) არსებობა დაცვის მიმართ, რომლითაც ხასიათდებიან გლობალურ ქსელში კომუნიკაციების განმახორციელებელი პროტოკოლები და სამსახურები. ასეთ პროტოკოლებს და სამსახურებს მიეკუთვნებს:

1. TCP/IP(Transmission Control Protocol/Internet Protocol) - წარმოადგენს პროტოკოლების პაკეტს და გამოიყენება არაერთგვაროვან ქსელურ გარემოში კომუნიკაციების ორგანიზმებისათვის. იგი უზრუნველყოფს სხვადასხვა ტიპის კომპიუტერების შეთავსებადობას და გლობალური ქსელის რესურსებთან დაშვების შესაძლებლობას. ამ პაკეტის სათაურში მიეთითება ისეთი ინფორმაცია, რომელმაც შეიძლება განიცადოს ჰაკერის თავდასხმა. კერძოდ, ჰაკერს შეუძლია შეცვალოს გამგზავნის მისამართი თავის "მავნე" პაკეტებში და წარმოადგინოს ისინი, როგორც პაკეტები გადაცემული კანონიერი კლიენტის მიერ.
2. SMTP(Simple Mail Transfer Protocol) - ელექტრონული ფოსტის გადაცემის მარტივი პროტოკოლია და ასრულებს Internet ქსელის საფოსტო ტრანსპორტის სამსახურს. პროტოკოლის ნაკლს წარმოადგენს ის გარემოება, რომ მომხმარებელს არ შეუძლია დაადგინოს გამომგზავნის მისამართი შეტყობინების სათაურიდან. ამ ნაკლის გამოყენებით ჰაკერს შეუძლია ლოკალურ ქსელში საფოსტო შეტყობინებების დიდი რაოდენობის გაგზავნით გამოიწვიოს საფოსტო სერვერის გადატვირთვა და მისი მუშაობის ბლოკირება.
3. Sendmail - ელექტრონული ფოსტის პროგრამაა და იგი მუშაობს პროცესში იყენებს ქსელური ინფორმაციის ნაწილს (გამგზავნის IP მისამართს). ამ პროგრამით გადაცემული შეტყობინების ხელში ჩაგდებით ჰაკერს შეუძლია გამოიყენოს ეს ინფორმაცია თავდასხმისთვის (მაგალითად, მისამართების შესაცვლელად).
4. FTP(File Transfer Protocol) - ფაილების გადაცემის პროტოკოლია. იგი უზრუნველყოფს ტექსტური და ორობითი ფაილების გადაცემას და ამიტომ Internet-ში გამოიყენება ინფორმაციასთან ერთობლივი დაკავშირების ორგანიზებისათვის. FTP სერვერში ინახება დოკუმენტები, პროგრამები, გრაფიკა და ინფორმაციის სხვა სახეობები. FTP სერვერის ფაილებთან უშუალო დაკავშირება შეუძლებელია. ფაილებთან დაკავშირება შეიძლება მხოლოდ იმ შემთხვევაში, თუ ისინი მთლიანად გადაიწერება ლოკალურ სერვერში. ზოგიერთი FTP სერვერი ზღუდავს მომხმარებლის დაშვებას არქივთან პაროლის საშუალებით, ხოლო ზოგიერთი - ხასიათდება თავისუფალი დაშვებით (ე.წ. ანონიმური FTP სერვერი). ანონიმური FTP სერვერის არქივის გამოყენებისას მომხმარებელი დარწმუნებული უნდა იყოს იმაში, რომ სერვერში შწნახული ფაილები განკუთვნილია მხოლოდ თავისუფალი გავრცელებისათვის.
5. DNS (Domain Name System) - ქსელური სახელების სამსახურია და წარმოადგენს განაწილებული მონაცემების ბაზას. იგი უზრუნველყოფს პაკეტების სათაურებში მითითებულ მომხმარებლების და მმართველი კომპიუტერების სახელების გარდაქმნას IP მისამართებში და პირიქით. DNS შეიცავს ინფორმაციას ქსელის სტრუქტურის შესახებ. მის სუსტ ადგილს წარმოადგენს მონაცემების ბაზსი დაუცველობა არაკანონიერი მომხმარებლებისაგან.
6. WWW (World Wide Web) - მსოფლიო აბლაბუდა. ეს არის სიტემა, რომელიც მომხმარებელს სხვადასხვა სერვერზე განლაგებული ინფორმაციის დათვალიერების საშუალებას აძლევს. მასში გამოყენებულია

ჰიპერტექსტური დოკუმენტები, რომლებშიც მოცემულია მითითებები სხვა დოკუმენტებისა და Web კვანძების შესახებ. ეს მითითებები მომხმარებელს ერთი კვანძიდან მეორეზე ადვილად გადასვლის საშუალებას აძლევს. ამავე დროს, ასეთი გადასვლების არსებობა წარმოადგენს WWW სისტემის სუსტ ადგილს, რადგან Web კვანძებზე მითითებები შეიცავენ ინფორმაციას იმის შესახებ, თუ როგორ ხდება მიმართვა თითოეულ კვანძთან. ამ ინფორმაციის გამოყენებით ჰაკერს შეუძლია Web კვანძის განადგურება ან მასში მოთავსებულ კონფიდენციალურ ინფორმაციასთან დაკავშირება.

7. TELNET - დაშორებული ტერმინალის ემულაციის სამსახურია და გამოიყენება ლოკალური ქსელისა და დაშორებული სისტემების დასაკავშირებლად. ამ სერვისის გამოყენებისას Internet-ის მომხმარებლები რეგისტრირდებიან TELNET სერვერზე თავიანთი სახელისა და პაროლის შეტანით. მომხმარებლის აუტენტიფიკაციის შემდეგ მისი მუშა სადგური დაკავშირებულია გარეშე მმართველ კომპიუტერთან და ფუნქციონირებს "ბლაგვი" ტერმინალის რეჟიმში. ამ ტერმინალიდან მომხმარებელს შეუძლია შეყვანოს ისეთი ბრძანებები, რომლებიც უზრუნველყოფენ მის დაშვებას ფაილებთან და პროგრამის გაშვებას. TELNET სერვერთან დაკავშირებით ჰაკერს შეუძლია ამ პროგრამის ისეთი კომფიგურაციით წარმოადგენა, რომ მან ჩაწეროს მომხმარებლის სახელები და პაროლები.

სუსტი ადგილის მქონე პროტოკოლებია, აგრეთვე: UUCP - ასლების გადაღების პროტოკოლი; RIP - მარშრუტიზაციის პროტოკოლი; X Windows - გრაფიკული ფაანჯრების სისტემა და სხვ.

ქსელთაშორისი ეკრანის განსახორციელებლად გამოიყენება შემდეგი ძირითადი სქემები:

- ქსელთაშორისი ეკრანი - გამფილტრავი მარშრუტიზატორი;
- ქსელთაშორისი ეკრანი ორპორტიანი რაბით;
- ქსელთაშორისი ეკრანი ეკრანირებული რაბით;
- ქსელთაშორისი ეკრანი - ეკრანირებული ქვექსელი.

ქსელთაშორისი ეკრანი, რომელიც ემყარება პაკეტების გაფილტვრას, არის ყველაზე უფრო გავრცელებული და მარტივი სქემა. იგი წარმოადგენს ლოკალურ ქსელსა და Internet -ს შორის მოთავსებულ გამფილტრავ მარშრუტიზატორს (ნახ.11.2).

გამფილტრავი მარშრუტი

ნახ.11.2.

გამფილტრავი მარშრუტიზატორით ხდება როგორც შესავალი, ისე გამოსავალი პაკეტების ფილტრაცია ან ბლოკირება YCP/IP პაკეტების სათაურში მითითებული მისამართების და პორტების ანალიზის შედეგად.

პორტი - ეს არის პროგრამული ცნება, რომელიც გამოიყენება კლიენტის ან სერვერის მიერ შეტყობინების გასაგზავნად ან მისაღებად. პორტი იდენტიფიცირდება თექვსმეტბიტიანი რიცხვით.

გამფილტრავი მარშრუტიზატორის დადებითი თვისებებია:

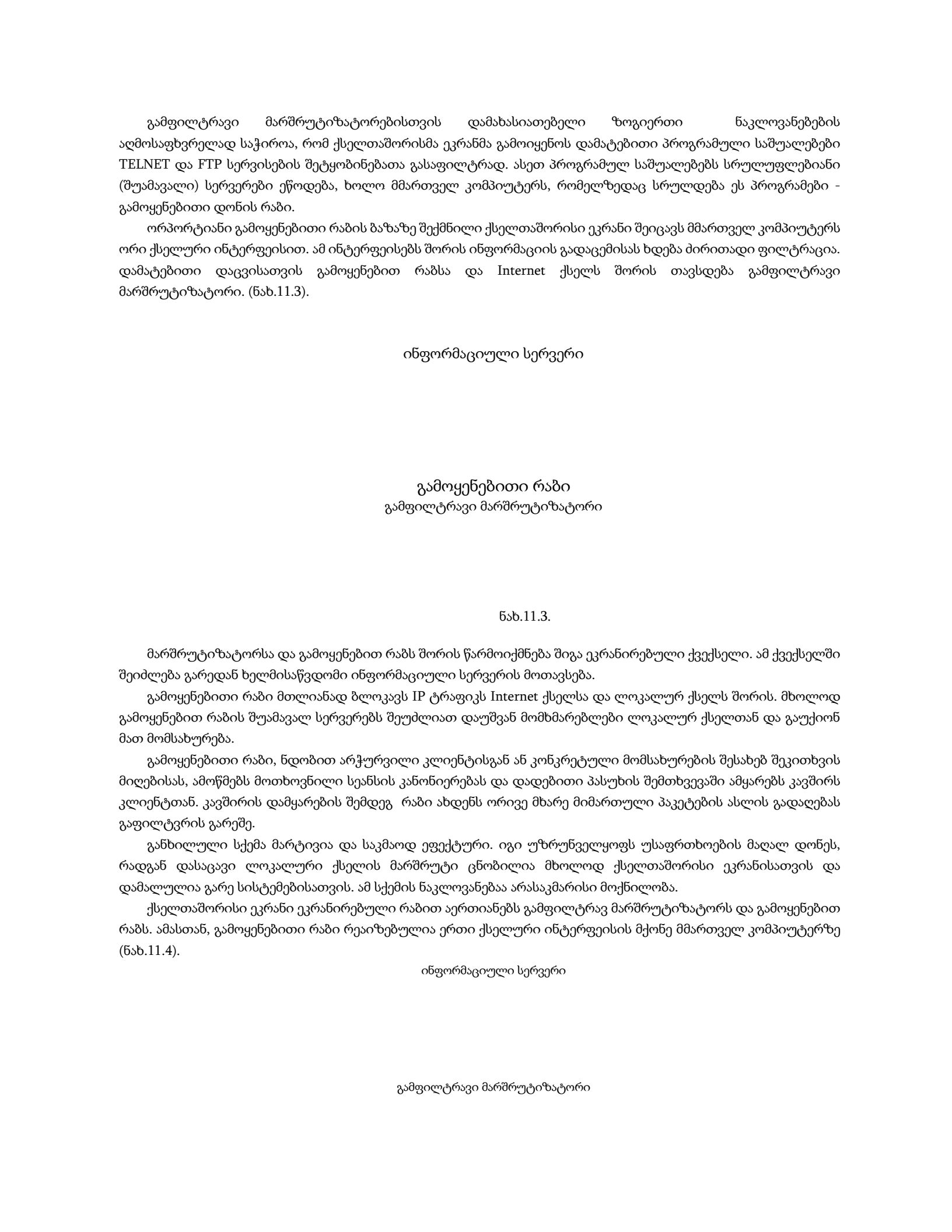
- მოითხოვს შედარებით მცირე დანახარჯებს;
- მოქნილია ფილტრაციის წესების განსაზღვრისას;
- პაკეტების გაცვლა მიმდინარეობს მცირეოდენი დაყოვნებით.

გამფილტრავი მარშრუტიზატორის ნაკლოვანებებია:

- Internet-ის მხრიდან ადვილია ლოკალური ქსელის კონფიგურაციის დადგენა;
- პაკეტების ფილტრაციის წესები ძნელად აღსაწერია და ზოგჯერ ფილტრაციის წესების ერთობლიობა შეიძლება გახდეს არამართვადი;
- ქსელთაშორისი ეკრანის დაზიანებისას ყველა კომპიუტერი დაუცველი ან ხელმიუწვდომელი ხდება;
- მომხმარებლის დონეზე აუტენტიფიკაცია არ ხორციელდება.

გამფილტრავი მარშრუტიზატორებისთვის დამახასიათებელი ზოგიერთი ნაკლოვანებების აღმოსაფხვრელად საჭიროა, რომ ქსელთაშორისმა ეკრანმა გამოიყენოს დამატებითი პროგრამული საშუალებები TELNET და FTP სერვისების შეტყობინებათა გასაფილტრად. ასეთ პროგრამულ საშუალებებს სრულუფლებიანი (შუამავალი) სერვერები ეწოდება, ხოლო მმართველ კომპიუტერს, რომელზედაც სრულდება ეს პროგრამები - გამოყენებითი დონის რაბი.

ორპორტიანი გამოყენებითი რაბის ბაზაზე შექმნილი ქსელთაშორისი ეკრანი შეიცავს მმართველ კომპიუტერს ორი ქსელური ინტერფეისით. ამ ინტერფეისებს შორის ინფორმაციის გადაცემისას ხდება ძირითადი ფილტრაცია. დამატებითი დაცვისათვის გამოყენებით რაბსა და Internet ქსელს შორის თავსდება გამფილტრავი მარშრუტიზატორი. (ნახ.11.3).



ნახ.11.3.

მარშრუტიზატორსა და გამოყენებით რაბს შორის წარმოიქმნება შიგა ეკრანირებული ქვექსელი. ამ ქვექსელში შეიძლება გარედან ხელმისაწვდომი ინფორმაციული სერვერის მოთავსება.

გამოყენებითი რაბი მთლიანად ბლოკავს IP ტრაფიკს Internet ქსელსა და ლოკალურ ქსელს შორის. მხოლოდ გამოყენებით რაბის შუამავალ სერვერებს შეუძლიათ დაუშვან მომხმარებლები ლოკალურ ქსელთან და გაუქიონ მათ მომსახურება.

გამოყენებითი რაბი, ნდობით არჭურვილი კლიენტისგან ან კონკრეტული მომსახურების შესახებ შეკითხვის მიღებისას, ამოწმებს მოთხოვნილი სეანსის კანონიერებას და დადებითი პასუხის შემთხვევაში ამყარებს კავშირს კლიენტთან. კავშირის დამყარების შემდეგ რაბი ახდენს ორივე მხარე მიმართული პაკეტების ასლის გადაღებას გაფილტვრის გარეშე.

განხილული სქემა მარტივია და საკმაოდ ეფექტური. იგი უზრუნველყოფს უსაფრთხოების მაღალ დონეს, რადგან დასაცავი ლოკალური ქსელის მარშრუტი ცნობილია მხოლოდ ქსელთაშორისი ეკრანისათვის და დამალულია გარე სისტემებისათვის. ამ სქემის ნაკლოვანებაა არასაკმარისი მოქნილობა.

ქსელთაშორისი ეკრანი ეკრანირებული რაბით აერთიანებს გამფილტრავ მარშრუტიზატორს და გამოყენებით რაბს. ამასთან, გამოყენებითი რაბი რეაიზებულია ერთი ქსელური ინტერფეისის მქონე მმართველ კომპიუტერზე (ნახ.11.4).

გამოყენებითი რაბი

ნახ.11.4.

ამ სქემით პირველადი დაცვის შემსრულებულია გამფილტრავი მარშრუტიზატორი. გამფილტრავ მარშრუტიზატორში ფილტრაციის პაკეტი შეიძლება რეალიზებულ იქნეს შემდეგი ორი ხერხიდან ერთ-ერთით:

- ნება დართოს შიგა ქსელის მმართველ კომპიუტერებს დაამყარონ კავშირი Internet ქსელის მმართველ კომპიუტერებთან გარკვეული სერვისების განსახორციელებლად;

- აუკრძალოს კავშირის დამყარება შიგა ქსელის ყველა მმართველ კომპიუტერს და აიძულოს ისინი გამოიყენონ გამოყენებით რაბში მოთავსებული შუამავალი სერვერები.

ასეთი მიდგომა სხვადასხვა სერვისების კომბინირების საშუალებას იძლევა. კერძოდ, ზოგიერთ სერვისს ეძლევა საშუალება პირდაპირი დაკავშირებისათვის პაკეტური ფილტრაციის გავლით, ხოლო ზოგიერთს დაკავშირება შეუძლია გამოყენებითი რაბის საშუალებით. სერვერების ასეთი შერჩევა დამოკიდებულია შიგა ქსელში მიღებული უსაფრთხოების დაცვის კონკრეტულ პოლიტიკაზე.

ამ სქემით შესრულებული ქსელთაშორისი ეკრანი უფრო მეტად მოქნილია, ვიდრე ქსელთაშორისი ეკრანის სქემა ორპორტიანი რაბით, მაგრამ უსაფრთხოების თვალსაზრისით ნაკლებად დაცულია. მისი ნაკლოვანი მხარეებია:

- თუ ბოროტგანმზრახველი შეაღწევს მმართველ კომპიუტერში, მაშინ მის წინ აღმოჩნდება შიგა ქსელის დაუცველი სისტემები;

- მარშრუტიზატორის კომპრომენტაციის შემთხვევაში შიგა ქსელი გახდება ხელმისაწვდომი ბოროტგანმზრახველისათვის.

ამ სქემის განვითარებას წარმოადგენს ქსელთაშორისი ეკრანი ეკრანირებული ქვექსელით.

ეკრანირებული ქვექსელის შესაქმნელად გამოიყენება ორი ეკრანირებული მარშრუტიზატორი. გარე მარშრუტიზატორი მოთავსებულია Internet-ის ქსელსა და ეკრანირებულ ქვექსელს შორის, ხოლო შიგა = ეკრაირებულ ქვექსელსა და დასაცავ შიდა ქსელს შორის. ეკრანირებული ქვექსელი შეიცავს გამოყენებით რაბს, ინფორმაციულ სერვერებს და სხვა სისტემას (ნახ. 11.5).

ინფორმაციული სერვერი

შიგა მარშრუტიზატორი

გარე მარშრუტიზატორი

გამოყენებითი რაბი
ელექტრონული ფოსტის სერვერი

ნახ.11.5.

ასეთი სქემის დროს ლოკალურ ქსელში შესაღწევად ბოროტგანზრახველმა უნდა გაიაროს ორი გამფილტრავი მარშრუტიზატორი. თუ ბოროტგანმზრახველი შეაღწევს გამოყენებითი რაბის მმართველ კომპიუტერში, მას მოუწევს კიდევ შიგა მარშრუტიზატორის გავლა. მაშასადამე, ლოკალური ქსელის არც ერთ სისტემასთან არ შეიძლება Internet-იდან უშუალო დაკავშირება.

ქსელთაშორისი ეკრანები გამოიყენება ვირტუალური კორპორაციული ქსელების დასაცავად (ნახ. 11.6) ტერმინი “ვირტუალური” მიუთითებს იმაზე, რომ კორპორაციულ ქსელში შემავალი რამდენიმე ლოკალური ქსელიდან ნებისმიერი ორი ერთმანეთთან დაკავშირებულია არა მუდმივად, არამედ მხოლოდ მაშინ, როცა მათ შორის ხდება ინფორმაციის მიმოცვლა (ე.ი. დაკავშირება სრულდება Internet ქსელის საშუალებით).

ქსელთაშორისი ეკრანი
ქსელთაშორისი ეკრანი

ქსელთაშორისი ეკრანი

ქსელთაშორისი ეკრანი

ნახ. 11.6.

რადგან ვირტუალურ კორპორაციულ ქსელში მონაცემების გადაცემა მიმდინარეობს გამჭვირვალედ, ამიტომ გადასაცემი ინფორმაციის კონფიდენციალურობისა და მთლიანობის უზრუნველსაყოფად საჭიროა დაშიფვრის სხვადასხვა საშუალებებისა და ციფრული ხელის მოწერის მეთოდების გამოყენება.

• ტრადიციული სიმეტრიული კრიპტოსისტემის პროგრამული უზრუნველყოფა

ამ თავში წარმოდგენილია მესამე თავში განხილული ტრადიციული სიმეტრიული კრიპტოსისტემების შესაქმნელი ზოგიერთი ალგორითმის პროგრამული უზრუნველყოფა, რომელიც შესრულებულია პასკალის ენაზე (პროგრამები შემუშავებულია სახელმძღვანლოს ავტორების მიერ).

ეს ალგორითმებია:

- ცეზარის დაშიფვრის სისტემები (ალფაბეტის სიმბოლოს K ოზიციით გადაადგილება, ჩასმების აფინური სისტემა, ერთალფაბეტიანი ჩასმის სისტემა);
- დაშიფვრის გრონსფელდის მეთოდი;
- ჩარლზ-უინსტონის დაშივრის მეთოდი;
- ვიჟინერის დაშიფვრის სისტემა (ერთი და იგივე გასაღების მრავალჯერ გამოყენების რეჟიმი, ავტოგასაღების რეჟიმი შრიფტექსტის გამოყენებით, ავტოგასაღების რეჟიმი ღია ტექსტის გამოყენებით);
- მრავალალფაბეტიანი დაშიფვრის მეთოდი;
- დაშიფვრის ცხრილური მეთოდები (მაგაირუი კვადრატი, მბრუნავი გისოსი, ჭადრაკის დაფა);

ყველა პროგრამაში ალფაბეტად აღებულია ASCII კოდის ოთხმოცდათხუთმეტი სიმბოლოსგან შედგენილი ალფაბეტი (ნახ.12.1).

ნახ.12.1.

ამ საწყისს ალფაბეტში შემავალი სიმბოლოების გადამაცვლების შედეგად შესაძლებელია 95!-ის ტოლი რაოდენობის ალფაბეტის მიღება. პროგრამებში გამოყენებულია ათი ალფაბეტისაგან შედგენილი ალფაბეტების მასივი (1,2,….,10). ცხადია, დამშიფრავი და გამშიფრავი მხარეებისათვის ალფაბეტების მასივი ცნობილია. ალფაბეტეის მასივისა და დაშიფვრის ერთ-ერთი მეთოდის გამოყენებით შესაძლებელია ერთი და იგივე ღია ტექსტის წარმოდგენა განსხვავებული შრიფტექსტით.

თითოეული პროგრამის გამოძახებისას დისპლეის ეკრანზე ჩნდება ფანჯარა, რომლის მარცხენა მხარე მოიცავს პანელს, ხოლო მარჯვენა ორ ტექსტურ ფანჯარას (ნახ.12.2).

ნახ. 12.2.
პანელზე განლაგებული პროგრამის სამართავი ღილაკები და დიალოგური ფანჯარები (ნახ.12.3.)

ნახ.12.3.

პანელის ზედა ნაწილში მოთავსებული ღილაკის “შესრულება” (ნახ. 12.3 ა) გააქტიურება იწვევს პროგრამის შესრულებას ?? - ღილაკის (ნახ. 12.3 ბ) გააქტიურებისას ზედა ტექსტურ ფანჯარაში მოთავსებული ტექსტი გადადის ქვედა ფანჯარაში, ხოლო ქვედა ფანჯარაში მოთავსებული კი ზედაში გადამრთველით “მოქმედება” (ნახ.12.3 გ) ხდება პროგრამის მუშაობის რეჟიმის (დაშიფვრის ან გაშიფვრის) არჩევა. ღილაკი “ტექსტის გაწმენდა “(ნახ.12.3 დ) გააქტიურებით ზედა ტექსტურ ფანჯარაში მოთავსებული ტექსტი იწმინდება ისეთი სიმბოლოებისაგან, რომლებიც არ შედის ალფაბეტში. ენის ასარჩევი ფანჯრის (ნახ. 12.3 ე) საშუალებით შესაძლებელია სასურველი ენის (ინგლისური, რუსული ან ქართული) არჩევა, ხოლო ალფაბეტის ნომრის ასარჩევი ფანჯრით (ნახ. 12.3 ვ) კი ალფაბეტის ვარიანტის არჩევა. ეს ღილაკები და დიალოგური ფანჯრები ყველა პროგრამისათვის საერთოა.

ზედა ტექსტურ ფანჯარაში თავსდება დასაშიფრი ან გასაშიფრი ტექსტი (აიკრიფება კლავიატურაზე ან აიღება ფაილიდან), ხოლო ქვედა ფანჯარაში პროგრამის შესრულების შემდეგ გაჩნდება დაშიფრული ან გაშიფრული ტექსტი. თითოეულ ფანჯარაზე თაგვის ღილაკის ორჯერ დაწკაპუნებით, ეკრანზე ჩნდება დიალოგური ფანჯარა (ნახ.12.4). ამ დიალოგური ფანჯრით შესაძლებელია ტექსტური ფაილის (TXT გაფართოების)გახსნა ზედა ფანჯარაში და ქვედა ფანჯრის შიგთავსის შენახვა ფაილში.

ნახ.12.4.

გარდა ჩამოთვლილი საერთო ღილაკებისა და დიალოგური ფანჯრებისა პანელზე განლაგებულია, აგრეთვე, ის დამატებითი მართვის ორგანოები, რომლებიც აუცილებელია ამა თუ იმ ალგორითმის განსახორციელებლად.

განვიხილოთ დაშიფვრის პროგრამები.

12.1 პროგრამა "ცეზარი"

ამ პროგრამით შესაძლებელია დაშიფვრის სამი სახეობის განხორციელება: I სახეობა - ალფაბეტის სიმბოლოს K პოზიციით გადაადგილება, II - ჩასმების აფინური სისტემა, III - ერთალფაბეტიანი ჩასმის სისტემა. სახეობის არჩევა ხორციელდება დიალოგური ფანჯრის "სახეობა" საშუალებით (ნახ. 12.5).

I სახეობის დროს რედაქტორის ფანჯარაში "დაძვრა" ჩაიწერება K-ს მნიშვნელობა (ნახ. 12.5 ა), II სახეობის დროს (ნახაზები 12.5 ბ და გ) რედაქტორის ფანჯარაში "AT+B" იწერება A და B-ს მნიშვნელობები (უსგ(A,n)=1, სადაც n=95),ხოლო III სახეობის დროს- რედაქტორის ფანჯარაში "სიტყვა გასაღებით" იწერება K-ს მნიშვნელობა და სიტყვა-გასაღები (ნახ. 12.5 დ).

ნახ.12.5.

პროგრამას აქვს შემდეგი სახე:

```
s1:=memol. Text;
s2:=s1;
if saxeoba. ItemIndex=0 then begin
                              cheing:=copy(symbol[SN], k+1,n-k);
                              cheing:=cheing+copy(symbol[SN], 1, k);
                              end;
if saxeoba. ItemIndex=1 then begin
            if usg(a,n) then
            for i:=1 to n do cheing (i):=symbol [SN] ?? ((a'(i-1)+b) mod n)+1]
                          else
                              begin
                                form2. Caption:='n='+intostr(n);
                                form2. Visible:=true;
                                form1. Enabled:=false;
                                s2:='';
                              end;
                                end;
if saxeoba. ItemIndex=2 then begin
                              kk1:=symbol[SN];
                              key:=edit3. Text+symbol[SN];
                              for i:= 1 to length(key)-n do
                              for j:=i+1 to length(key) do
                                if key [i]=key[j]  then key [j]:=31;
j:=1;
```

12.2 პროგრამა “გრონსფელდი”

რედაქტორის ფანჯარაში “რიცხვი” იწერება გასაღების მნიშვნელობა, წარმოდგენილი რიცხვის სახით (ნახ.12.6).

ნახ.12.6.

პროგრამას აქვს შემდეგი სახე:

```
s1:=memol.Text;
s2:=s1;
if edit 1.Text=’’ then key:=’0’  else key:=edit1.Text;
k:=length (key);
h:=0;


if rbl. Checked then
          for i:= 1 to length (s1) do
            begin
              nom:=pos (s1[i], symbol [SN]);
              if I mod k= 0 then h:=k  else  h:=I   mod k;
              nom:=nom+strtoint  (key [h]);
              if nom  > n  then  nom:=nom-n;
              s2[i]:=symbol [SN] [nom];
          end
   else
        for i:= 1  to   length  (s1)   do
         begin
              nom:=  pos (s1[i], symbol [SN]);
              if i mod  k=  0 then  h:=k   else   h:=I  modk;
              nom:=npm-strtoint  (key[h]);
              if nom  <  1  then  nom:=  npm+n;
              s2 [i]:=  symbol  [SN] [nom];
         end;
memo2. Text:=s2;
```

12.3 პროგრამა "ჩარლზ-უიტსტონი"

ამ პროგრამაში ხდება ორი ალფაბეტის ნომრების შერჩევა (AK და Bm, k ≠ m, K და m იცვლებიან ერთიდან ათის ჩათვლით). თითოეული ალფაბეტი დალაგებულია 19x5 ცხრილის სახით. 12.7 ნახ-ზე ნაჩვენებია ალფაბეტების არჩევის ერთ-ერთი ვარიანტი.

ნახ.12.7.

პროგრამაში გამოყენებულია ჩარლზ-უიტსტონის მეთოდის განსახორციელებელი ალგორითმი ნაწილობრივი ცვლილებით. ეს ცვლილება იმაში მდგომარეობს, რომ შრიფტექსტის თითოეული ბიგრამის პირველი სიმბოლო ყოველთვის მარჯვენა ალფაბეტის სიმბოლოა, ხოლო მეორე სიმბოლო - მარცხენა ალფაბეტის.

დაშიფვრის ალგორითმი წარმოდგენილია მაგალითის სახით (სიმბოლოს ინდექსის პირველი ციფრი წარმოადგენს სტრიქონის ნომერს, ხოლო მეორე ციფრი - სვეტის ნომერს).

$a_{21}b_{34}$ $b_{24}a_{31}$ $a_{71}b_{73}$ $b_{71}a_{73}$ $a_{71}b_{71}$ $b_{71}a_{71}$

პროგრამას აქვს შემდეგი სახე:

```
s1:=memol.Text;
if length (sl) mod 2 = 1 then sl : = sl + ' ' :
i : = l;
if rbl. Checked then
    begin
   while i<=length (sl) do
       begin
        ai : =CharmasA[sl [i] ] div 5;
        aj : = CharmasA[sl [i] ] mod 5
       bj : = CharmasB[sl [i+1] ] div 5
       bj : = CharmasB[sl [i+1] ] mod 5
       if  (ai=bi)  and  (aj=bj) then s2 :=s2+s] [i+1] +sl [i]
                                  else
                                    begin

                if ai=bi   then s2 : =s2+symbol B [SN] [ai *5+aj=1]+symbol A [bi *5+bj+1]
                           else  s2 : = s2+symbol B [SN] [ai *5+bj=1]+symbol A [bi *5+aj+1]
                                       end;

         i : =i=2;
          end;
      end
  else
    begin
   while i<=length (sl) do
       begin
ai : = Charmas A [sl [i+1] ] div 5;
aj : = Charmas A [sl [i+1] ] mod 5;
bi : = Charmas B [sl [i] ] div 5;
bj : = Charmas B [sl [i] ] mod 5;

if (ai = bi) and (aj = bj) then s2 : = s2=sl (i+1)+sl (i+1)+sl (i)
                           else
                             begin
   if ai+bi then s2 : =s2+symbol A[bi *5+bj=1]+symbol B [SN] [ai *5+aj+1]
           else  s2 : =s2+symbol A[bi *5+aj=1]+symbol B [SN] [ai *5+bj+1]
```

```
                    end

      i : = i+2;
       end;
    end;
memo2. Text : = s2;
```

12.4 პროგრამა "ვიჟინერი"

ეს პროგრამა მოიცავს სამ სახეობას: I - პირდაპირი (ერთი და იგივე გასაღების მრავალჯერ გამოყენება); II - ავტოგასაღების რეჟიმი შრიფტექსტის გამოყენებით; III - ავტოგასაღების რეჟიმი ღია ტექსტის გამოყენებით. სახეობის არჩევა ხდება ფანჯრის "სახეობა" (ნახ. 12.8 ა) საშუალებით, ხოლო სიტყვა გასაღები იწერება რედაქტორის ფანჯარაში "სიტყვა გასაღები" (ნახ. 12.8 ბ).

ნახ.12.8.

პროგრამას აქვს შემდეგი სახე:

```
s := ml.Text;
sl : =s;
key :=edit 1. Text;
  if saxeoba . ItemIndex=0  then begin
                                  ki : =key;
                                  for i : =1  to (length  (s) div  leng
```

12.5 პროგრამა “მრავალალფაბეტიანი შიფრი”

ამ პროგრამაში ალფაბეტის თითოეულ სიმბოლოს შეესაბამება სამელემენტიანი სიმრავლე. ამ სიმრავლეებით შედგენილი მატრიცა გამოიყენება დაშიფვრისა და გაშიფვრისათვის. პროგრამა მოიცავს ათ განსხვავებულ მატრიცას. მატრიცის ნომერი შეიძლება შევარჩიოთ პანელზე მოთავსებულ ფანჯარაში “მატრიცის ნომერი” შესაბამისი რიცხვის ჩაწერით (ნახ.12.9).

პროგრამას აქვს შემდეგი სახე:

```
s1:=memol.Text;
   if rbl. Checked then
                        begin
                  s2:=’ ‘;
                  for  i:= 1  to  length  (s1)   do
                  begin
                     w:=pos (s1[i], symbol)-1;
                      s2:=s2+  base[w, random(3)+1];
                  end;
                           end
                       else
                           begin
                        kk1:=’ ‘;  nom:=1;
                        s2:= ‘ ‘;
                        j:=1;
                        for  i:=1 to  length (s1)  div  2 do
                        begin
                            kk1:=copy (s1,j,2);
                            j:=j+2;
                            for w:=0  to  n-1   do
                               for h:=1   to 3 do
                                  if kk1=base [w,h]  then
                                                  begin
                                                   nom:=w;
                                                   end;
                            s2:=s2+ symbol [nom+1];
                        end;
                               end;
memo2.Text:=s2;
```

12.6 პროგრამა “მაგიური კვადრატი”

პროგრამაში რეალიზებულია 4x4 მაგიური კვადრატის სამოცდაოთხი ვარიანტი. თითოეული კვადრატით იშიფრება ღია ტექსტის 16 სიმბოლო. საწყისი კვადრატის ნომერი შეირჩევა კვადრატის ნომრის ასარჩევ ფანჯარაში(ნახ.12.10 ა). არჩეული კვადრატის გამოსახულების ჩვენება ხდება პანელის ქვედა ნაწილში (ნახ. 12.10 ბ) და ამ საწყისი კვადრატით იშიფრება პირველი თექვსმეტი სიმბოლო. შემდეგი 16 სიმბოლო იშიფრება იმ კვადრატაის გამოყენებით, რომლის ნომერიც ერთით მეტი ან ნაკლებია საწყის ნომერზე. ნომრის მატების ან კლების არჩევა შესაძლებელია დიალოგური ფანჯრის საშუალებით(ნახ. 12.10 გ).

ნახ.12.10

თუ დასაშიფრი ტექსტის სიმბოლოების რაოდენობა არ არის 16-ის ჯერადი, მაშინ ადგილი აქვს სიმბოლოების დამატებას ხელით ან ავტომატურად (ნახ. 12.11).

ნახ.12.11

პროგრამას აქვს შემდეგი სახე:

```
 s1:=memol.Text;
s2:=' ';    gg : =`
1 : = length (sl);
RN: = strtoint (spindet 1. text);

 if rbl. Checked then
 if 1 mod  16 + 0 then
begin
   while  1>15  do
            begin
              for  i :=1  to 16 do
                   gg (i) : =sl (rect [i,RN]);
 s2: =s2+gg;
 delete (sl,1,16);
 i: = length (sl);
 if up. Cheked them begin RN:=RN+1; if RN>64  then  RN:=RN-64  end else begin RN:=RN-1; if RN<1 then RN: = Rn+64
end;

                          end;
```

```
        end
        else
       begin
          k1:= 16-(1 mod 16);
         form2. visible:=true;
         form2. Enabled:=false;
        form2. Labell.Caption:=daamate +inttostr (kl) +  simbolo;
         form2. Checkbox1. Cheked:=false;
 end
else
 begin
     while  1.15 do
 begin
   for  i:=1  to 16 do
      gg (rect (i, RN]) : =sl (i);
s2:=s2+gg;
delete (sl,1,16);
1:=length (sl);
if up. Checked then begin RN:-RN+1; if RN.64  then RN: = RN-64 end else begin RN: = RN-1; if RN,1  then RN: =RN+64 end;
   end;
end;

memo2. Text : =s2;
```

12.7 პროგრამა “მბრუნავი გისოსი”

პროგრამაში გამოყენებულია მბრუნავი გისოსი 4x4-ზე გისოსის საწყის კომბინაციად აღებულია 1,2,3, 4 ციფრები. სხვადასხვა კომბინაციების არჩევა ხორციელდება ფანჯარაში “ელემენტების ჯგუფში” სასურველი კომბინაციების ჩწერით (ნახ. 12.12)

ნახ. 12.12

მბრუნავუ გისოსით ხდება 16 სიმბოლოს დაშიფვრა. თუ სიმბოლოების რაოდენობა არ არის 16-ის ჯერადი, მაშინ სიმბოლოების დამატება ხორციელდება ხელით ან ავტომატურად.

პროგრამას აქვს შემდეგი სახე:

12.8. პროგრამა “ჭადრაკის დაფა”

ეს პროგრამა უზრუნველყოფს ისეთი ტექსტების დაშიფვრას, რომლებიც შეიცავენ 64-ის ჯერად სიმბოლოების რაოდენობას. თუ სიმბოლოების რაოდენობა არ არის საკმარისი, მაშინ ეკრანზე ჩნდება დიალოგური ფანჯარა, რომელშიც ნაჩვენებია დასამატებელი სიმბოლოების რაოდენობა. სიმბოლოების დამატება შეიძლება განხორციელდეს ოპერატორის მიერ ან ავტომატურად (ნახ.12.13). ავტომატურად შევსებისათვის საჭიროა ოფციის “ავტომატური შევსება” გააქტიურება.

ნახ.12.13.

პროგრამის დასაწყებად საჭიროა: დაფის საწყისი უჯრის K ნომრის არჩევა (ნახ. 12.14), საწყისი ნომრის მომდევნო ნომრის არჩევა (ერთით მატება ან კლება) და დაფიდან დაშიფრული ტექსტის წაკითხვის მეთოდის შერჩევა (ნახ. 12.15).

ნახ.12.14. ნახ.12.15.

თუ ოფციები: “სვეტებით წაკითხვა” და “ნომრის კლება” არაა გააქტიურებული, მაშინ ნომრის არჩევა ხდება მატებით და წაკითხვა მიმდინარეობს სტრიქონების მიხედვით.

K-ს მნიშვნელობის შერჩევის შემდეგ, დაფაზე სიმბოლოების განლაგება მიმდინარეობს (K ± i)mod64 გამოსახულების მიხედვით, სადაც i=1,2,….,64 (+ აიღება მატებისას, ხოლო მინუსი - კლებისას).

პროგრამას აქვს შემდეგი სახე:

12.9. კომბინირებული პროგრამა "კრიპტოგრაფია"

განხილული პროგრამების ერთობლივი გამოყენებით (მაგალითად, თავდაპირველად ცეზარის აფინური სისტემა, შემდეგ ვიჟინერის მეთოდი და, ბოლოს, ერთ-ერთი ცხრილური მეთოდი) საგრძნობლად გაიზრდება შიფრის სკრიპტომედეგობა. ამასთან, ამ შემთხვევაში გამოიყენება ერთი გასაღები, რომელიც გამოსახულია არაბული ციფრებით და წარმოადგენს სხვადასხვა მონაცემების გაერთიანებას. ეს მონაცემები შეიძლება იყოს:

- ალფაბეტის ვარიანტის ნომერი;
- მეთოდების ვარიანტის ნომერი;
- ცეზარის, გრონსფელდის და ვიჟინერის მეთოდებისათვის საჭირო მონაცემები;
- მაგიური კვადრატის ან მბრუნავი გისოსის ვარიანტის ნომერი;
- ჭადრაკის დაფაზე პირველი სიმბოლოს გასანთავსებელი უჯრის ნომერი;
- შევსებული მაგიური კვადრატიდან (გისოსიდან) ან ჭადრაკის დაფიდან სისმბოლოების წაკიტხვის მეთოდი;

- მაგიური კვადრატის (გისოსის) გამოყენებისას ყოველი 16 სიმბოლოს განლაგების შემდეგ ახალი ცხრილის არჩევის მეთოდი;
- ჭადრაკის დაფის გამოყენებისას მოძრაობის მიმართულების (ნომრის მატება ან კლება) არჩევის მეთოდი.

12.16 ნახ-ზე ნაჩვენებია კომბინირებული პროგრამის "კრიპტოგრაფია" პანელი.

პროგრამა უზრუნველყოფს გაერთიანებული მეთოდების რვა ვარიანტიდან ერთ-ერთის არჩევას. ღილაკის "პარამეტრები" გააქტიურებისას ეკრანზე გამოდის დიალოგური ფანჯარა და მისი მეშვეობით ხდება არჩეული ვარიანტისათვის საჭირო მონაცემების შეტანა. რედაქტორის ფანჯარაში "კოდი", დაშიფვრის პროცესის შესრულებისას, ავტომატურად იწერება არაბული ციფრებით წარმოდგენილი გასაღების მნიშვნელობა.

ნახ. 12.16

მაგალითად, თუ არჩეულია პირველი სახეობა (ცეზარი 2, ვიჟინერი1, ჭადრაკი) და ამ სახეობის პარამეტრებია: ალფაბეტის ნომერი (0-ფან 9-ის ჩათვლით), A და B-ს მნიშვნელობები ცეზარის მე-2 მეთოდისათვის, სიტყვა-გასაღების მნიშვნელობა ვიჟინერის მეთოდისათვის, ჭადრაკის დაფაზე პირველი სიმბოლოს გასანთავსებელი უჯრის ნომერი, შემდეგი უჯრის არჩევის მეთოდი (მატება ან კლება), შევსებული ჭადრაკის დაფიდან დაშიფრული ინფორმაციის წაკითხვის მეთოდი (სტრიქონების ან სვეტების მიხედვით), მაშინ კოდს ექნება შემდეგი სახე:

პირველ პოზიციას შეესაბამება არჩეული ალფაბეტის ნომერი (2), მეორე პოზიციას - კომბინირებული მეთოდის ნომერი (0), მესამე პოზიციას - A da B -ს მნიშვნელობები, მეოთხე პოზიციას - სიტყვა-გასაღების მნიშვნელობა, მეხუთეს - ჭადრაკის დაფაზე საწყისი უჯრის ნომერი (54), მეექვსე პოზიციას პირველი ციფრის ლუწობა ან კენტობა განსაზღვრავს, შესაბამისად, სტრიქონებით ან სვეტებით წაკითხვას, ხოლო მეორე ციფრის ლუწობა ან კენტობა კი, შესაბამისად, ნომრის მატებას ან კლებას (მოყვანილ მაგალითში წაკითხვა მიმდინარეობს სვეტებით და შემდეგი უჯრის ნომრის შერჩევა ხდება მატებით).

გასაღების მნიშვნელობა იგზავნება დაშიფრულ ტექსტთან ერთად და მიმღები ახდენს გაშიფვრის პროცესის შესრულებას.

დ ა ნ ა რ თ ი

რიცხვთა თეორიის ელემენტები

- **მოდულური არითმეტიკა**

თუ a მთელი რიცხვია, ხოლო ნ-დადებითი მთელი, მაშინ ჩანაწერი a(modn) განისაზღვრება როგორც ნაშთი, რომელიც მიიღება a-ს გაყოფით n-ზე.

მაგალითად: 42(mod13)=3,
27(mod11)=5.

ამბობენ, რომ ორი მთელი a და b რიცხვი სადარია n მოდულით, თუ (amodn)=(bmodn). ეს თანაფარდობა ჩაიწერება a=b(modn) სახით, იკითხება "a სადარია b-თან და n მოდულით" და იგი სამართლიანია მხოლოდ მაშინ, თუ a,b და n($n \neq 0$) მთელი რიცხვებისათვის a=b+k·n, სადაც k მთელი რიცხვია.

მაგალითად, 45=6(მოდ13),
45=13·3+6, (k=3).

ამ შემთხვევაში b-ს ეწოდება a რიცხვის გამონაქვითი n მოდულით და იგი წარმოადგენს მთელ რიცხვს, რომელიც მოთავსებულია [0,n-1] შუალედში.
მოდულურ არითმეტიკაში არითმეტიკული ოპერაციების შესრულებისას შეიძლება გამოსახულება დაყვანილ იქნეს n მოდულით, ხოლო შემდეგ შესრულდეს ოპერაციები ან პირიქით, ჯერ შესრულდეს ოპერაციები და შემდეგ დაყვანილ იქნეს n მოდულით, ე.ი.:

(a+b)modn=[a(modn)+b(modn)]modn,
(a-b)modn=[a(modn)-b(modn)]modn,
(a·b)modn=[a(modn)·b(modn)]modn.

მოდულური არითმეტიკა ხასიათდება კომუტატიურობის, ასოციაციურობის და დისტრიბუციულობის თვისებებით:

(w+x)modn = (x+w)modn,
(w·x)modn + (x·w)modn, კომუტატიურობა;

[(w+x)+y]modn=[w+(x+y)]modn,
[(w·x)·y]modn=[w·(x·y)]modn ასოციაციურობა;

[(w+x)·y]modn=[(w·y)+(x·y)]modn - დისტრიბუციულობა

მოდულურ არითმეტიკაში სამართლიანია შემდეგი თანაფარდობები:
1. a=a(modn) ნებისმიერი მთელი a რიცხვისათვის;
2. თუ a=b(modn) და b = a(modn) a და b მთელი რიცხვებისათვის;
3. თუ a= b (modn) და b = c (modn), მაშინ a = c (modn);
4. თუ a =b(modn) და c = d(modn), მაშინ a+c =(b+d)modn და ac=(bd)modn;
5. თუ a=b(modmn), მაშინ a=b(modm) და a=b(modn);
6. თუ ac-(bc)modn da უსგ(c,n) = 1, მაშინ a=b(modn);
7. თუ a=b(modn), მაშინ $a^m=b^m$(modn), სადაც m მთელი დადებითი რიცხვია;
8. თუ a=b(modn), a=b(modn) და უსგ(m,n) -1, მაშინ a=b(modmn)
9. თუ a+b=(a+c)modn, მაშინ b=c(modn).

მოდულურ არითმეტიკაში შესაძლებელია შემდეგი მანიპულაციების ჩატარება:
-12(mod7)=-5(mod7)=2(mod7)=9(mod7)=16(mod7)=23(mod7) და ა.შ.

- მოდულური ექსპონენტი

კრიპტოგრაფიაში დაშიფვრის ალგორითმების უმეტესობა ემყარება მოდულური ექსპონენტის გამოთვლას (ხარისხში ახარისხებს n მოდულით).

$$a^x \text{mod} n.$$

თუ X ორის ჯერადია (მაგალითად x=8 ან x=16), მაშინ:

$$a^8 \text{mod} n = ((a^2 \text{mod} n)^2 \text{mod} n)^2 \text{mod} n$$
$$a^{16} \text{mod} n = (((a^2 \text{mod} n)^2 \text{mod} n)^2 \text{mod} n)^2 \text{mod} n$$

თუ x არ არის ორის ჯერადი, მაშინ მას წარმოადგენენ, თვლის ორობით სისტემაში და შემდეგ ორის ფუძიანი ხარისხების ჯამით. მაგალითად:

$$x=25_{(10)} \quad 11001B,\ 25=2^4+2^3+2^0 \text{ და}$$

ამ მეთოდს ადიტიური ჯაჭვის მეთოდი ეწოდება და მისი პროგრამული უზრუნველყოფა C ალგორითმულ ენაზე შემდეგია:

```
unsigned lond qe2 (unsigned long x, unsigned long y, unsigned long n)

{
unsigned long s,t,u;
int i;
s=1; t=x; u=y;
whil (u)

                {
                if (u&1)  s=(s*t) %n;
                u>>+l;
                t=(t*t)%n;
return s;
}
```

$a^x(\text{mod}n)$ გამოსახულების მნიშვნელობის გამოსათვლელად გამოიყენება სხვადასხვა სახის ალგორითმები. უ x წარმოდგენილია თვლის ორობით სისტემაში: $x=x_0\cdot 2^z+x_1\cdot 2^{z-1}+\ldots x_{z-1}\cdot 2+x_z$, სადაც $x_0=1$, ხოლო დანარჩენი $x_1,x_2,\ldots x_z$ უდრის 0 ან 1-ს, მაშინ მოდულური ექსპონენტების გამოთვლის ერთ-ერთი ალგორითმი შემდეგია:

$$A_1=A_{i-1}^2\cdot A^{x1}(\text{mod}n)$$

სადაც

$$i=1,2,\ldots.z, \quad z<\log_2 n \text{ და } A_0=A$$

განვიხილოთ მაგალითი. ვთქვათ გამოსათვლელია $5^{19}(\text{მოდ}17)$. რადგან $19=1\cdot 2^4+0\cdot 2^3+0\cdot 2^2+1\cdot 2^1+1$, ამიტომ $x_0=1$, $x_1=0$, $x_2=0$, $x_3=1$, $x_4=1$ და $A_0=A=5$.

$$A_1 = A_0^2\cdot A^{X1}(\text{mod}n) = (5^2\cdot 5^0)\text{mod}17 = 8$$
$$A_2 = A_1^2\cdot A^{X2}(\text{mod}n) = (8^2\cdot 5^0)\text{mod}17 = 13$$
$$A_3 = A_2^2\cdot A^{X3}(\text{mod}n) = (13^2\cdot 5^1)\text{mod}17 = 12$$
$$A_4 = A_3^2\cdot A^{X4}(\text{mod}n) = (12^2\cdot 5^1)\text{mod}17 = 6$$

ე.ი. $5^{19}(\mathrm{mod}17) = 8$

3. შებრუნებული სიდიდეების გამოთვლა

ნამდვილ რიცხვთა არითმეტიკაში არანულოვანი a რიცხვის შებრუნებულ ადიტიურ რიცხვს წარმოადგენს -a, ხოლო შებრუნებულ მულტიპლიკატიურ რიცხვს a^{-1} ე.ი. $a+(-a)=0$ და $a\cdot a^{-1}=1$.

მოდულურ არითმეტიკაში a რიცხვის ($a \in z_n$) ადიტიური ისეთი b რიცხვია, რომელიც აკმაყოფილებს $a+b0(\mathrm{mod}n)$ შედარებას, a რიცხვის ადიტიური აღინიშნება - a-თი.

მაგალითად, როცა a=4 და n=7, მაშინ -a=3, რადგან $(4+3)\mathrm{mod}7=0$.

მოდულურ არითმეტიკაში შებრუნებული მულტიპლიკატიური რიცხვის გამოთვლა წარმოადგენს რთულ ამოცანას. მაგალითად, $a\cdot x=n\cdot k+1$. განტოლების ამოხსნაზე, სადაც x და k მთელი რიცხვებია.

თეორემა 1. თუ a და n ურთიერთმარტივი მთელი რიცხვებია (ე.ი. უსგ(a,n)=1), მაშინ არსებობს a რიცხვის შებრუნებული ისეთი a^{-1} რიცხვი, რომელიც აკმაყოფილებს შემდეგ პირობებს:

$$0<a^{-1}<n,$$
$$a\cdot a^{-1}=1(\mathrm{mod}n).$$

როცა უსგ $(a,n) \neq 1$, მაშინ a^{-1} არ არსებობს.

a^{-1} მოძებნა შესაძლებელია $a\cdot x=n\cdot k+1$ გამოსახულებით ან ეილერის მიერ განზოგადებული ფერმის მცირე თეორემის გამოყენებით.

თეორემა 2. თუ n დადებითი მთელი რიცხვია და უსგ (a,n)=1, აშინ

$$a^{\Phi(n)}=1(\mathrm{mod}n),$$

სადაც Φ(n) ეილერის ფუნქციაა, რომლის მნიშვნელობაც დამოკიდებულია n-ზე, კერძოდ:

- როცა n მარტივი რიცხვია, მაშინ $\Phi(n)=n-1$ და $\Phi(n^k)=n^{k-1}(n-1)$, სადაც $k>1$;
- როცა $n=a^k$, სადაც a მარტივი რიცხვია, მაშინ $\Phi(n)=a^{k-1}(a-1)$. ადვილად მისახვედრია, რომ როცა a=2, მაშინ $\Phi(n)=2^{k-1}$.
- როცა n=p,q…w მარტივი რიცხვებია, მაშინ
$$\Phi(n)=(P-1)\cdot(q-1)..(w-1);$$

პირველ ცხრილში მოცემულია ეილერის Φ(n) ფუნქციის მნიშვნელობები n-ის სხვადასხვა მნიშვნელობებისათვის ($n \in [1,30]$).

დავასაბუთოთ ცხრილში მოყვანილი მონაცემები n-ის რამდენიმე მნიშვნელობისათვის:

თუ n იშლება ურთიერთმარტივი რიცხვების ნამრავლის სახით, მაშინ φ(n)-ის მნიშვნელობა შეიძლება გამოითვალოს შემდეგნაირად: φn)= φ(p·q)= φ(p)· φ(q).

მაგალითად

φ(15)= φ(5·3)= φ(5)· φ(3)=4·2=8;
φ(100)= φ(25·4)= φ(25)· φ(4)=20·2=40
ადვილად მისახვედრია, რომ როცა $n=2^k \cdot m$, სადაც m მთელი კენტი რიცხვია და k>1, მაშინ $\varphi(n)=2^{k-1}\cdot \varphi(m)$.
მაგალითად, $n=24=2^3 \cdot 3$, $\varphi(24)=2^{3-1}\varphi(3)=4\cdot 2=8$.

თუ დავუკვირდებით პირველ ცხრილში მოყვანილ მნიშვნელობებს შევამჩნევთ, რომ როცა n>2, მაშინ φ(n) ლუწი რიცხვია.

ეილერის თეორემის ალტერნატიულ ფორმულირებას წარმოადგენს $a^{\Phi(n)}=a(\mathrm{mod} n)$.

ეილერის ფუნქციის საშუალებით $a^{-1}(\mathrm{mod} n)=a^{\Phi(n)-1}=(\mathrm{mod} n)$.

განვიხილოთ შებრუნებული მულტიპლიკატიური გამოსახულების მოძებნის მაგალითები ax=nk+1 განტოლების ან ეილერის ფუნქციის გამოყენებით:

- a=3 და n=7, რადგან უსგ(3,7)=1, ამიტომ

$$3\cdot a-1=1(\mathrm{mod}7),$$
$$3\cdot a-1=7k+1.$$

(0,1,…..6) შუალედში k-ს შერჩევით მიიღება, რომ როცა K=2, მაშინ $a^{-1}=5$. მართლაც,

$$(3\cdot 5)\mathrm{mod}7=1$$

- a=9 და n=14. რადგან უსგ(9,14)=1, ამიტომ

$$9\cdot a-1=1(\mathrm{mod}14),$$
$$9\cdot a-1=14k+1.$$

(0,…13) შუალედში k -ს შერჩევით მიიღება, რომ როცა k=7. მაშინ a-1=11. მართლაც,

$$(9\cdot 11)\mathrm{mod}14=1.$$

ე.ი. $a \cdot a^{-1}(\text{mod}1011)=1$.

a^{-1} -ის გამოთვლის მეთოდი გამოიყენება ისეთი რთული შედარებების ამოსახსნელად, როგორიცაა $a \cdot x=b(\text{mod}n)$, სადაც $b \neq 1$.

თავდაპირველად ამოიხსნება შედარება $a \cdot y=1(\text{mod}n)$, ე.ი. განისაზღვრება $y=a^{-1}(\text{mod}n)$, ხოლო შემდეგ $x=a^{-1}b(\text{mod}n)=y \cdot b(\text{mod}n)$.

მაგალითად, ვთქვათ, საჭიროა x -ის განსაზღვრა $5 \cdot x=9(\text{mod}23)$ შედარებიდან.

თავდაპირველად ამოიხსნება შედარება $5 \cdot y=1(\text{mod}23)$. რადგან $n=23$, ამიტომ $\Phi(n)=23-1=22$.

$y=5^{-1}(\text{mod}23)=5^{22-1}(\text{mod}23)=5^{21}(\text{mod}23)=(5 \cdot 5^{20})\text{mod}23=(5(5^2)^{10})\text{mod}23=(5(25)^{10})\text{mod}23=(5 \cdot 2^{10})\text{mod}23=5120\text{mod}23=14$,

$x=5^{-1} \cdot 9(\text{mod}23)=9 \cdot 5^{-1}(\text{mod}23)=(9 \cdot 14)\text{mod}23=126(\text{mod}23)=11(\text{mod}23)$.

ე.ი. $x=11$.

უნდა აღინიშნოს, რომ როცა b ყოფს უსგ(a,n)-ს (უსგ(a,n)b), მაშინ $ax=b(\text{mod}n)$ შედარებას აქვს მთელი ამონახსნების სასრული რაოდენობა და ეს ამონახსნებია $x_0 + t \cdot n/$უსგ (a,n), სადაც $t=1,2,3\ldots$, უსგ (a,n), ხოლო x_0 - სათვის არსებობს ისეთი y_0, რომ (x_0,y_0) წყვილი წარმოადგენს $ax+ny=b$ განტოლების ამონახსნს.

მაგალითად, ვთქვათ, შედარებას აქვს შემდეგი სახე: $35x=14(\text{mod}84)$. რადგან უსგ(35,84)=7 და 7/14, ამიტომ ამ შედარებასს ექნება შვიდი სხვადასხვა ამონახსნი.

- მოდულის პირვანდელი ფესვი

მოდულურ არითმეტიკაში ერთ-ერთი მნიშვნელოვანი ცნებაა n მოდულის პირვანდელი (პრიმიტიული) ფესვი.
თუ a არის n-ის პირვანდელი ფესვი (n მარტივი რიცხვია), მაშინ $a^1,a^2,a^3,\ldots a^{\Phi(n)}$ რიცხვების მოდულები n-ით სხვადასხვაა და ისინი მიეკუთვნებიან [1, Φ(n) ანუ [1,n-1] შუალედს. ე.ი. a რიცხვის ხარისხები ხარისხის მაჩვენებლით 1-დან Φ(n)-მდე წარმოქმნიან ყველა მთელ რიცხვს [0,n-1] შუალედში მხოლოდ ერთხელ.

მე-2 ცხრილში მოცემულია მთელი რიცხვების ხარისხები მოდულით 19. ცხრილიდან ჩანს, რომ 19-ის პირვანდელი ფესვებია: 2,3,10,13,14 და 15.

იმის გასარკვევად, წარმოადგენს თუ არა a რიცხვი პირვანდელ ფესვს n მოდულით. საჭიროა n-1 სხვაობის დაშლა მარტივ მამრავლებად ($q_1,q_2,\ldots q_k$) და $a^{(n-1)/q}(\mathrm{mod} n)$ გამოსახულების მნიშვნელობის გამოთვლა თითოეული q-ს შემთხვევაში. თუ ყველა q-სათვის აღმოჩნდება $a^{(n-1)/q}(\mathrm{mod} n) \neq 1$, მაშინ a წარმოადგენს პირვანდელ ფესვს. q-ს რომელიმე მნიშვნელობის დროს ერთიანის მიღება ნიშნავს, რომ a რიცხვი არ არის პირვანდელი ფესვი. განვიხილოთ მაგალითები:

ე.ი. 3 არ არის პირვანდელი ფესვი 11-ის მოდულით.

თუ n მარტივი რიცხვია და a დადებითი მთელი რიცხვია (0<a<n-1), მაშინ: მოდულიანი გამოსახულებების გაანგარიშებისას უნდა გავითვალისწინოთ შემდეგი თანაფარდობები:

$a^n(modn)=a, a^{n-1}(modn)=1$, $a^{(n-1)/2}(modn)=1$ ან $a^{(n-1)/2}(modn)=n^{-1}$, $a^{(n-1)/2}(modn)=1$ (როცა $a-k^2$).
ამ თანაარდობების სისწორეში შეიძლება დარწმუნება მე-2 ცხრილის მონაცემებით (a^{18} და $a^{(19-1)/2}=a^9$.

- რიცხვის რიგი n მოდულით

თუ n მთელი დადებითი რიცხვია და a ისეთი მთელი რიცხვია, რომ უსგ (a,n)=1, მაშინ a რიცხვის რიგი n მოდულით ეწოდება ისეთ უმცირეს მთელ დადებით k რიცხვს, რომლის დროსაც $a^k-1(modn)$. a რიცხვის რიგი აღინიშნება $Ord_n a$-თი. (ე.ი. $Ord_n a=k$).

მე-2 ცხრილის მიხედვით შეგვიძლია ვთქვათ, რომ $Ord_{19}2=18$, $Ord_{19}4=9$, $Ord_{19}7=3$, $Ord_{19}12=6$.

a რიცხვის რიგი ხასიათდება შემდეგი თვისებებით:

ა) თუ $a^m=1(modn)$, სადაც m მთელი რიცხვია, მაშინ k ყოფას m-ს (ცხრილი 2-ის მიხედვით $Ord_{19}11=3$, $11^3(mod19)=11^5(mod19)=11^9(mod19)=11^{12}(mod19)=11^{15}(mod19)=11^{18}(mod19)=1$ ე.ი. m=3;6;9;12;15;18 და 3/m);
ბ) K ყოფს Φ(n) (როცა n=19, მაშინ Φ(n)=18 (მე-2 ცხრილის მიხედვით K=3;6;9;18 და ყველა შემთხვევაში K/ Φ(n);
გ) r და S მთელი რიცხვებისათვის $a'=a^s(modn)$ მხოლოდ მაშინ, როცა r=S(modK) (მე-2 ცხრილის მიხედვით, როცა a=8, მაშინ K=6, $8^5=8^{11}(mod19)=12$ და 5=11(mod6)).

ცხადია, რომ როცა a პირვანდელი ფესვია n მოდულით, მაშინ K= Φ(n).

- კვადრატული გამონაქვითი

მოდულურ არითმეტიკაში სარგებლობენ ე.წ. კვადრატული გამონაქვითებით. თუ განვიხილავთ მარტივ n>2 და a<n რიცხვებს, მაშინ a -ს ეწოდება კვადრატული გამონაქვითი n მოდულით, თუ a შესადარია რიცხვის კვადრატისა მოდულით n, ე.ი. $x^2=a(mind)$.

თუ a კვადრატული გამონაქვითია, მაშინ $x^2=a(mind)$ შედარებას აქვს ორი ამონახსნი: +x და -x ე.ი. a-ს გააჩნია ორი კვადრატული ფესვი n მოდულით.

ყველა კვადრატულ გამონაქვითებს განსაზღვრავენ 1,2,3,…(n-1)/2 ელემენტების კვადრატში აყვანით. a-ს ყველა მნიშვნელობა არ წარმოადგენს კვადრატულ გამონაქვითს. მაგალითად, როცა n=7, მისთვის კვადრატული გამონაქვითებია:1,2,4.

კვადრატული გამონაქვითების რაოდენობა (n-1)/2--ს ტოლია, თუ a კვადრატული გამონაქვითებია n მოდულით, მაშინ a-ს გააჩნია ზუსტად ორი კვადრატული ფესვი: ერთი ფესვი მოთავსებილია 0-სა და (n-1)/2-ს შორის, ხოლო მეორე (n-1)/2 -სა და (n-1)-ს შორის.

ამ ორი კვადრატული ფესვიდან ერთი არის კვადრატული გამონაქვითი n მოდულით და მას მთავარი კვადრატული ფესვი ეწოდება. კვადრატული ფესვების გამოთვლა, როდესაც n=7 ნაჩვენებია მე-3 ცხრილში.

იმის გასარკვევად, წარმოადგენს თუ არა ნებისმიერი a მთელი რიცხვი კვადრატულ გამონაქვითს n მოგულით, სადაც n მარტივი რიცხვია (n>2), საჭიროა $a^{(n-1)/2}(\mathrm{mod} n)$ გამოსახულების მნიშვნელობის გამოთვლა. თუ ეს გამოსახულება აღმოჩნდება I-ის ტოლი, მაშინ შეგვიძლია ვთქვათ, რომ a კვადრატული გამონაქვითია. მე-2 ცხრილის მიხედვით შეგვიძლია ვთქვათ, რომ 1,4,5,6,7,9,11,16 და 17 კვადრატული გამნაქვითებია მოდულით 19.

თუ n წარმოადგენს ორი მარტივი მთელი რიცხვის ნამრავლს, ე.ი. $n=p\cdot q$, მაშინ არსებობს ზუსტად $(p-1)(q-1)/4$ რაოდენობის კვადრატული გამონაქვითი n მოდულით, რომლებიც n რიცხვის მიმართ მარტივია.

მაგალითად, თუ $n=35=5\cdot 7$, მაშინ კვადრატული გამონაქვითების რაოდენობა იქნება.

$$(5-1)(7-1)/4=6$$

$x^2=a(\mathrm{mod}35)$ შედარების ამოხსნით მიიღება ცხრილი 4.

შევნიშნოთ, რომ 14,15,21,25 და 30 არიან 35-ის მიმართებაში შედგენილი რიცხვები, ამიტომ კვადრატული გამონაქვითები იქნება: 1,4,9,11,16,29.

- უდიდესი საერთო გამყოფის გამოთვლა

უდიდესი საერთო გამყოფის მოსაძებნად გამოიყენება ევკლიდეს ალგორითმი, რომელიც შემდეგში მდგომარეობს: თუ a არაუარყოფითი მთელი რიცხვია, მაშინ ნებისმიერი მთელი b რიცხვისათვის სამართლიანია შედეგი:

- მარტივი რიცხვების შემმოწმებელი ალგორითმები

რადგან თანამედროვე კრიპტოგრაფიული ალგორითმები ემყარებიან მარტივი რიცხვების გამოყენებას, ამიტომ საჭირო ხდება მარტივი რიცხვების შემმოწმებელი სწრაფი ალგორითმების დამუშავება.

არითმეტიკიდან ცნობილია შემდეგი განსაზღვრებები და თეორემები:

განსაზღვრება 1. მარტივი ეწოდება ერთზე მეტ ისეთ მთელს რიცხვს, რომელსაც არ გააჩნია დადებითი გამყოფები გარდა ერთისა და თვით ამ რიცხვისა (მაგალითად 2,3,5,7,13,97);

განსაზღვრება 2. ერთზე მეტი დადებითი რიცხვი წარმოადგენს შედგენილ რიცხვს, თუ იგი მარტივი არაა(მაგალითად, 4,26,,39,65);

თეორემა 4. მარტივ რიცხვთა სიმრავლე უსასრულოა;

თეორემა 5. ნებისმიერი დადებითი ერთზე მეტი n რიცხვი წარმოადგენს ან მარტივ რიცხვს, ან იგი შეიძლება გამოისახოს მარტივი რიცხვების ნამრავლისს სახით. მაგალითად:

n=13;

n=210=2·3·5·7;

n=39616304=2· 2· 2· 2· 7· 7· 13· 13· 23=2^4· 7^2· 13^2· 23

თეორემა 6. თუ დადებითი მთელი n რიცხვი წარმოადგენს შედგენილ რიცხვს, მაშინ n-ს გააჩნია ისეთი მარტივი გამყოფი p, რომ $p^2 \le n$.

ამ თეორემიდან გამომდინარე, შეგვიძლია ვთქვათ, რომ, უ n რიცხვი არ იყოფა [2p] შუალედში მოთავსებული არც ერთ მარტივ რიცხვზე, მაშინ n მარტივია.

მაგალითად,

ა)n=521.

რადგან 22^2=484 da 23^2=529, ამიტომ p=22 და[2,22] შუალედში მოთავსებული მარტივი რიცხვებია : 2,3,5,7,11,13,17, და 19. 521 არ იყოფა ამ რიცხვებიდან არც ერთზე და ამიტომ n=521 წარმოადგენს მარტივ რიცხვს.

ბ) n-177.

რადგან 13^2=169 და 14^2=196, ამიტომ p=13 და [2,13] შუალედში მოთავსებული მარტივი რიცხვებია:2,3,5,7,11,13,177. იყოფა 3-ზე და ამიტომ n=177 წარმოადგენს შედგენილ რიცხვს.

ამ თეორემის შესაბამისი ალგორითმის პროგრამული უზრუნველყოფა პასკალის (Delphi) ენაზე შემდეგია:

- კვადრატული გამონაქვითი

მოდულურ არითმეტიკაში სარგებლობენ ე.წ. კვადრატული გამონაქვითებით. თუ განვიხილავთ მარტივ