1. ინფორმაციის კოდირება-დეკოდირება.

თავად სახელიც გვეუბნება, ინფორმაციის კოდირება არის მოცემული ინფორმაციის ერთი ათვლით სისტემიდან მეორე ათვლით სისტემაშ გადაყვანა. კერძოდ არჩეულ ენაში გამოყენებულ სიმბოლოებს, (სიმბოლოებს რომლის გამოყენებითაც ჩვენ ერთმანეთისათვის გასაგებ ენაზე გადმოვცემთ აზრს.) ვუსაბამებთ რიცხვებს. ეს სიმბოლოები და რიცხვები ერთან ადგენენ ბაზას. ბაზა რაც უფრო არაინტუიტიურია მით უკეთესი კრიპტოგრაფიისათვის.

მას შემგედ რაც ტექსტს შევუსაბამებთ რიცხვების მიმდევრობას. მიღებული რიცხვები გადაგვყავს ერთი ათვლითი სისტემიდან მეორეში. გამოყენება შეიძლება ნებისმიერი ათვლითი ისტემის. ყევლაზე ხშირად ინფორმატიკაში გამოიყენება ორობითი, რვაობითი, თექვსმეტობითი ა.შ.

კრიპტოგრაფიის მხრივ ყველაზე ხშირად ხდება 2-ობითი სისტემის გამოყენება, საიმედოობისათვის. (რაც უკვე დეშიფრაციის საკითხია)

კოდირების იმარტივეს შემთხვევას განვიხილავ პრინციპის აღსაწერად.

ბაზაში დავუშვათ ასო ბ - 1410 სისტემის.

მოვახდინოთ ჩვენი ინფორმაციის კოდირება 2-ობით სისტემაში.

1410  = 11102 (14 ში ყველაზე დიდი 23 მოთავსდა დარჩენილი შევავსე, დანაშტვის გარეშე ბევრად ჩქარა გადამყავს ზეპირად)

დეკოდირება ეწოდება კოდირების შებრუნებულ პროცესს. კერძოდ მიღებული სისტემიდან უკუპროცესით საწყის სისტემაში დაბრუნებას.

11102  = 23 + 22 + 21 = 1410

ხაზი მინდა გავუსვა იმას რომ სისტემა შეიძლება იყოს ნებისმიერი. და იმავე პრინციპით მოხდება კოდირებაც და დეკოდირებაც.

კოდირება-დეკოდირების პროცესი აუცილებელია შემდეგი ეტაპებისათვის წარმატებული

დაშიფვრა-დეშიფრაციისათვის. კოდირება-დეკოდირება ერთგვარი მოსამზადებელი ეტაპია დასაშიფრად და განსაშიფრად.

ინფორმაციაც სწორედ კოდირებული და დაშიფრული გადაიცემა, საიმედოობისათვის.

1. ვიჟინერის მეთოდი

ვიჟინერის მეთოდი არის ერთერთი ინფორმაციის დაშიფვრის მეთოდი. რადგან მასში არ ხდება გასაღების „გამოთვლა“ და წინასწარ შეთანხმებული გასაღებით ხდება დაშიფვრაც და შეშიფრციაც ის არის ერთერთი სიმეტრიული მეთოდი. ის ერთგვარად გაუმჯობესებული ვარიანტია ცეზარის მეთოდის. ვიჟინერმა შემოგვთავაზა, რომ იმის ნაცვლად რომ ბაზაში არსებული ყველა სიმბოლო ერთნაირი ბიჯით წავანაცვლოთ. ყოველი მომდევნო ასო განსხვავებული ბიჯით წანაცვლდება მის ალგორითმში(გასაღების ზომის გათვალისწინებით)

უფრო კონკრეტულად რომ ვისაუბროთ. გვაქვს ტექსტი რისი დაშიფვრაც გვინდა და ასევე ვიგონებთ რაიმე გასაღებ სიტყვას, რისი მეშვეობითაც ვახდენთ პირველადი ტექსტის სახეცვლილებას. ტექსტსაც და შიფრ სიტყვასაც ვუსაბამებთ წინასწარ შედგენილ ბაზას, რომელშიც ყველა სიმბოლოს შეესაბამება ერთი რიცხვი.

მიღებული რიცხვების მიმდევრობას , წევრ წევრად ვუმატებთ შიფრ სიტყვას.

გასათვალისწინებელია რომ ვიჟინერის მეთოდში შფრი უფრო პატარა არის ვიდრე დასაშიფრი ტექსტი. შესაბამისად შიფრს ვიმეორებთ იმდენჯერ სანამ დასაშირი ტექსტია რ ამოგვეწურება.

სადემონსტრაციოდ ვიჟინერის მეთდით დავშიფრავ ჩემს სახელს

ბაზად ავიღებ სიმარტივისათვის 1-33 თანმიმდევრულ შესაბამისობას ქართულ ანბანთან

თუ ჯამი გაცდება ბაზას ვაკლებთ 33 და ვაბრუნებთ სათავეში.

დასაშიფრი სიტყვა : თორნიკე

სიტყვა ბაზის გათვალისწინებით : 8-14-17-13-9-10-5

შიფრი : დათვი

შიფრი ბაზაში : 4-1-8-6-9

შეკრების ოპერაცია :

8-14-17-13-9-10-5

4-1-8-6-9-4-1

შედეგი : 12-15-25-19-18-14-6 = მპშტსოვ

რაღათქმაუნდა ინფორმაცია კოდირებული გადაიცემა თვალსაჩინოებისათვის შესაბამისობა გავაკეთე.

ეს მეთოდი უფრო სანდოა ვიდრე ცეზარის მეთდი მაგრამ ნაკლებად სანდო ვიდრე ვერნამის მეთოდი.

სიმეტრიული ზოგადად ნაკლებად სანდოა. მითუმეტეს თუ გავითვალისწინებთ რომ მესამე პირს გატეხვა რომ მოუნდეს ამის ალბათბა 1/33n  სადაც n არის ჩვენს მიერ შერჩეული შიფრის ზომა. რაც ვერნამმა გამოასწორა შიფრის ზომის გატოლებით დასაშიფრ სიტვასთან.

რაც უფრო იზრდება შიფრი გატეხვა რთულდება.

ხოლო თუ ინფორმაცია გადაიცემა 2 ობით სისტემაში. ეს კიდევ უფრო ართულებს საქმეს რადგან მესამე პირმა ისიც არ იცის წესით რამდენ ერთეულებად უნდა დაყოს მოპოვებული ინფორმაცია.

1. ასიმეტრიული სისტემები

ასიმეტრიული სისტემები არის ისეთი დშიფვრის მეთდები სადაც დაშიფვრისთვის და განშიფვრისთვის გამოიყენება განსხვავებული გასაღებები. გასაღებების გამოთვლისათვის არსებობს სხვადასხვა ნაირი მეთდები, ერთერთს რომელსაც ჩვენ შევეხეთ იყო diffie-hellman ის ასიმეტრიული გასაღებების მიმოცვლის და გენერირების მეთდები. ასიმეტრიული მეთდები ბევერად უფრო სანდოა და რთული გასატეხად. გამოიყენება public და private გასაღებები.

არსებობს ისეთ მიდგომები რომ დამატებითი გამოთვლებით და ოპერაციებით ისე შეიცვალოს ინფორმაცია რომ პირადი გასაღების გაზიარება არ გახდეს საჭირო. დღევანდელ რეალობაში კარგი ასიმეტრიული ალგორითმის მაგალითად როდორიც Diffie hellman ია გატეხვა თითქმის შეუძლებელია.

ასევე შებუნებული მატრიცის მეთოდიც განსხვავებულ გასაღებებს იყენებს საშაშიფრად და განსაშიფრად რომელსაც გავარჩევ შემდგომ საკითხში.

1. შებრუნებული მატრიცის მეთოდი.

ერთ ერთი წარმატებული მეთოდი რომელიც გამოირჩევა სანდოობით. დასაიფრად და განსაშიფრად დაგვჭირდება რამოდენიმე რამ.

მატრიცა და ამ მატრიცის შებრუნებული.

შესაბამისაც ეს მოთხოვნა თავიდანვე გვავალდებულებს რომ ავირჩიოთ კვადრატული გადაუგვარებელი მატრიცა(არანულოვანი დეტერმინანტით)

ამ მეთოდის საიმედოობა გამომდინარეობს იქიდან რომ არ ვართ შეზღუდულები არანაირად მატრიცის ზომასა და გვარობაში ზემოთ ხსენებული პირობების გარდა.

მას შემდეფ რაც ბაზის გამოყენებით მოვახდინეთ ჩვენი ტექსტის სახეცვლილება. მიღებულ რიცხვების მიმდევრობას დავყობთ შერჩეული მატრიცის განზომილების შესაბამის ერთეულებად. ჩავწერთ როგორც სტრიქონ მატრიცას. მარჯვნიდან ვამოქმედებთ(გავამრავლებთ) ჩაფიქრებულ მატრიცაზე. (დაყოფა გვჭირდება სწორედ რომ განზომილება დაემთხვეს და გამრავლება მოხერხდეს მატრიცების).

მიღებული სტრიქონი მატრიცა გადაიგზავნება.

ორივე მხარეს გამოთვლილი აქვს ჩაფიქრებული მატრიცის შებრუნებული მატრიცა.

დაშიფრუნი ინფორმაციის იგივე პრინციპით მოქმედებით შებრუნებულ მატრიცაზე მოხდება.

პირველადი ტექსტის აღდგენა.

A \* A-1 = l მატრიცის შებრუნებულზე გამრავლებით მიიღება ერთეულოვანი მატრიცა რომელიც ინფორმაციას არ ცვლის.

B \* A \* A-1 = B \* I = B

მეთოდი საკმაოდ საიმეეოდა იმის გათვალისინებით რომ შიფრ მატრიცების სიმრავლე უსასრულოა. არსებობს უსასრულო რაოდენობის განზომილებისა და წევრების კომბინაციები რომლებიც აკმაყოფილებენ არაგადაგვარებულობის პირობას.

მესამე პირი შესაბამისად სუსლელი თ არ არის არ დაიწყებს ყველა მატრიცის რიგრიგობით ცდას რაც დიდი ალბათობით არ გაამართლებს.

რაიმე პრინციპის დასაჭერად კი ის სხვა გზას მიმართაბს. ერთერთი რაც გავაკეთე იყო ნებისმიერ პოზიციაზე მდგომი ტექსტის გაშიფვრა. სადაც დავამტკიცე რომ ნებისმიერი წევრი დაიყვანება პირველ წევრზე. შესაბამისად მიიღება რეკურსიული ალგორითმი რითიც გამოითვლება ნებისმიერი წევრი. თუ პირველი წევრები გამოიღვალა და პრინციპი დაიჭირა. ბევრი წვალების გარეშე დანარჩენებსაც გაიგებს ეს არის ცუდი.

ასევე შევეცადე რომ a და a’ შორის დამეჭირა რაიმე პირდაპირი კავშირი და დავამკიცე რომ პირდაპირი კავშირი სწორედ ის მატრიცაა მხოლოდ რომელიც დასაშიფრად გამოიყენებოდა.

რადგან არ არსებობს არანაირი კავშირი a da a’ შორის. გვესაჭიროება განზომილების შესაბამისი რაოდენობა განტოლებელის რომ ამოიხსნას. კოეფიციენტების გამოსახვა ვერ მოხდება სხვა რაიმე მახასიათებლებით რადგან თთეული მათგანი წრფივად დამოუკიდებელია.

რაც ნიშნავს იმას რომ სხვა წევრებით არ გამოისახებოდა. რომ გამოისახებოდეს და წრფივად დამოუკიდებლობა რომ დაიკარგოს დაირღვევა გადაგვარებულობის პირობა.

შესაბამისად ერთადერთი ვარიანტი რომელიც მესამე პირს რჩება არის რამენაირად პირველი წევრები გაშიფროს. და შემდეგ რეკურსიულად გაოთვალოს დანარჩენები. როგორც ავღნიშნე პირველი წევრების გამოთვლაც ძალიან რთულია. შესაბამისად შებრუნებული მატრიცის ალგორითმი ძალზედ საიმედოა.

შებრუნებული მატრიცის გამოთვლა. დაშიფვრა შეშიფრაციის მაგალითები იხილეთ სურათებში.