**კრიპტოგრაფია. ლექცია N1. განსაზღვრებები**

კრიპტოგრაფიაში ძირითად სუბიექტებს წარმოადგენენ - **გამგზავნი** და **მიმღები**. ვთქვათ გამგზავნს სურს მიაწოდოს მიმღებს რაიმე შეტყობინე­ბა, ისეთნაირად, რომ თუ კი ვინმეს ეს შეტყობინება ჩაუვარდა ხელში, მან ვერ წაიკითხოს ის. “ წაკითხვა“ ამ შემთხვევაში ნიშნავს იმას, რომ მე­სამე პირი - **შეტყობინების მიმტაცებელი**, ვერ ჩაწვდება ამ შეტყობინ­ების არსს. ამდენად შეტყობინების, ინფორმაციის გადაცემას გამგზავნი­დან მიმღებამდე, თუ კი მისს არსს ვერ ჩაწვდა შეტყობინების მიმტაცებე­ლი ეწოდება *ინფორმაციის უსაფრთხო გადაცემა*.

საწყის შეტყობინებას, რომლის გადაცემაც სურთ, ეწოდება **ღია ტექსტი** (კლერი). შეტყობინების ფორმის, მისი სახის ცვლილებას, იმისთვის, რომ შეტყობინების არსი იქნეს დაფარული ეწოდება დაშიფრვა. დაშიფრულ შეტყობინებას ვუწოდოთ **შიფროტექსტი**. შიფროტექსტის გარდაქმნა ღია ტექსტად არის ***დეშიფრირება***.



ნახატი 1. დაშიფრვა და დეშიფრირება

ISO 7498-2 სტანდარტით ინგლისურ ლიტერატურაში მიღებულია გამო­ყე­ნებულ იქნას ტერმინი encipher - encrypt-ის (დაშიფრვა) მაგიერ და decipher - decrypt-ს (დეშიფრება) მაგიერ.

უსაფრთხო შეტყობინებების ხელოვნებასა და მეცნიერებას ეწოდება **კრიპ­ტოგრაფია**. კრიპტოგრაფიაში მოღვაწეებს **კრიპტოგრაფებს** უძახიან. შიფროტექსტების „გატეხვის“ ხელოვნებასა და მეცნიერებას **კრიპტოანა­ლიზი** ეწოდება. ვინც კრიპტოანალიზს ეწევა, მას **კრიპტოანალიტიკოსი** ეწოდება. კრიპტოგრაფია და კრიპტოანა­ლიზი ერთობლიობაში ქმნის მათემატიკურ მიმართულებას, რომელსაც **კრიპტოლოგია** ეწოდება. კრიპ­ტოლოგიის სპეციალისტებს **კრიპტოლოგები** ეწოდება.

ავღნიშნით ღია ტექსტი **M**-ით (ინგ. Message, შეტყობინება), ან **P** (ინგ. Plaintext, ღია ტექსტი). როგოც წესი **M** შეიძლება იყოს ორობითი ინფორ­მაცია, ტექსტური ფაილი,ციფრული აუდიო, ციფრული ვიდეო, ბიტების ნაკადი და მრავალი სხვა.

ავღნიშნით შიფროტექსტი **C**-ით (ინგ ciphertext). **C** –ც ასევე ზოგადად კომპიუტერისთვის ორობითი მონაცემია, **C** -ს და **M**-ის ზომები შეიძლება განსხვავებულებინ იყვნენ. დაშიფრვის ფუნქცია **E** მოქმედებს **M**-ზე და შედეგად ვიღებთ **C** -ს, რაც შეიძლება ჩაიწეროს მათემატიკური თანა­ფარდობებით:

**E(M)=C**

უკუ პროცესი, ანუ დეშიფრირება ნიშნავს იმას, რომ დეშიფრირების **D** ფუნქცია მოქმედებს **C** -ზე და აღადგენს **M**-ს:

**D(C)=M**

ცხადია, რომ **E** -ს და **C** -ს სუპერპოზიციით ვღებულობთ საწყის ღია ტექსტს:

**D(E(M))=M**

შეტყობინებათა კონფიდენციალობის გარდა კრიპტოგრაფია გამოიყენება სხვა დანიშნულებებისათვისაც:

1. **ორიგინალობის შესამოწმება**. მიმღებს შეუძლია შეტყობინების წყაროს შემოწმება, თაღლითი ვერ მოახერხებს თავის გასაღებად ვინმეს სახელით.

2. **მთლიანობა**. შეტყობინების მიმღებს შეუძლია შეამოწმოს, ხომ არ იყო შეტყობინება შეცვლილი გადმოგზავნის პროცესში, თაღლითი ვერ მოახერხებს სწორი შეტყობინების ყალბით შეცვლას.

3. **ავტორობის არაუარყოფა**. გამგზავნი ვერ შეძლებს გაგზავნილი შეტყობინების არგადზავნის ტყუილით მტკიცებას.

**კრიპტოგრაფიული ალგორითმი** ან **შიფრი**, არის მათემატიკური ფუნქ­ცია, რომელიც გამოიყენება დაშიფრვისა და დეშიფრირებისთვის. საერთოდ საქმე გვაქვს ორ ურთიერთდაკავშირებულ ფუნქციასთან - ერთი გამოიყენება დაშიფრვისთვის, მეორე დეშიფრირებისთვის.

*შეზღუდული* კრიპტოგრაფიული ალგორითმი, ეს არის ისეთი ალგო­რით­მი, რომლის უსაფრთხოება დაფუძნებულია თავად ალგორითმის საიდუმლოდ შენახვაზე. ასეთი ტიპის კრიპტოგრაფიული უნიკალური ალგორითმი, დღეს უკვე ნაკლებ საიმედონი არიან. მაგალითად თუ კი ჯგუფი, რომე­ლიც ამ კრიპტოგრაფიულ ალგორითმს იყენებს, ვინმემ დატოვა, ეს ალგორითმი შესაცვლელია. მაგრამ ამ ალგორითმს მაინც იყენებენ იქ სადაც უსაფრთხოების მაღალი დონე არ მოითხოვება.

თანამედროვე კრიპტოგრაფიაში უნივერსალური ალგორითმის პრობ­ლემის მოგვარება ხდება K გასაღების საშუალებით. K-ს მნიშვნელობა შეიძლება შერჩეულ იქნეს გასაღებთა სივრციდან. დაშიფრვა და დეშიფ­რირება ამ გასაღების საშუალებით ასე ჩაიწერება:

 **EK(M)=C**

**DK(C)=M**

**DK(EK(M))=M**

ზოგიერთი ალგორითმისთვის გამოიყენება სხვადასხვა გასაღები დაშიფრვა და დეშიფრირებისას - ანუ დაშიფრვის გასაღები **K1**განსხვავდება დეშიფრირების **K2** გასაღებისგან, ამ შემთხვევაში:

**EK1(M)=C**

**DK2(C)=M**

**DK2(EK1(M))=M**

ამ ალგორითმების უსაფრთხოება სრულად არის დამოკიდებული გასა­ღებზე და არა ალგორითმის დეტალებსა თუ ნიუანსებზე. ანუ ეს ნიშნავს, რომ შესაძლებელია ალგორითმის გამოქვეყნება, გაანალიზება. ასეთ ალ­გორითმებზე დაფუძნებული პროდუქტების ტირაჟირება უკვე შესაძლე­ბელია, რადგანაც აღარ აქვს მნიშვნელობა იმას, იცის თუ არა შენმა მოწი­ნაათმდეგენ ალგორითმი, რადგანაც თუ კი მან არ იცის კონკრეტული გასაღები, ის ვერ წაიკითხავს შეტყობინებას.

კრიპტოსისტემა ეს არის ალგორითმი და მას დამატებული ნებისმიერი ღია ტექსტი, შიფროტექსტი და გასაღებები.



ნახატი 2. დაშიფრვა და დეშიფრირება გასაღებით



ნახატი 3. დაშიფრვა და დეშიფრირება ორი სხვადასხა გასაღებით

გასაღებთან მიმართებაში არსებობს ორი ტიპის ალგორითმები: *სიმეტრი­ული* და *ღია გასაღებით*.

**სიმეტრიული ალგორითმები**, ან ზოგჯერ როგორც მათ უწოდებენ- პირობითი ალგორითმები, ისეთი თვისების მატარებლები არიან, რომ შესაძლებელია დაშიფრვის გასაღები გამოთვლილი იქნეს დეშიფრირების გასაღებით და პირიქით. უმეტეს სიმეტრიულ ალგირითმში დაშიფრვის და დეშიფრირების გასაღები ერთი და იგივეა. ამ ალგორითმებს ხანდახან უწოდებენ - ***ალგორითმებს საიდუმლო ან ერთი გასაღებით***. მათი გამო­ყენებისთვის აუცილებელია, რომ გამგზავნმა და მიმღებმა შეტყობინების უსაფრთხო გადაცემის სეანსის წინ შეათანხმონ გამოსაყენებელი გასაღე­ბი. სიმეტრიული ალგორითმის უსაფრთხოება განისაზღვრება მისი გა­საღებით, სეანსების პროცესში გასაღები უნდა იყოს გასაიდუმლოებუ­ლი. თუ კი ვინმემ მოახდინა ამ გასაღების გაგება, მაშინ შეტყობინება უკვე აღარ იქნება კონფიდენციალური. სიმეტრიული ალგორითმით დაშიფ­რვის და დეშიფრირების პროცესი ასე აღიწერება:

**EK(M)=C**

**DK(C)=M**

სიმეტრიული ალგორითმები იყოფიან ორ კატეგორიად - ერთნი ღია გასაღებს ამუშავებენ ბაიტური ( ან ბიტური) მიმდევრობით და მათ ეწოდება *ნაკადური ალგორითმები* ან *ნაკადური შიფრები*, მეორენი ღია ტექსტის ბიტების ან ბაიტების რაღაც ჯგუფს - ბლოკს ამუშავებენ, მათ კი *ბლოკური ალგორითმები* ან *ბლოკური შიფრები* ეწოდება. კომპიუტე­რებში ბლოკის ზომა 64 ბიტია, რაც საკმაოდ დიდი მოცულობაა, რომ ხე­ლი შეუშალოს კრიპტოანალიზს და საკმაოდ მცირეა და მოსახერხებელი მუშაობისას.

***ასიმეტრიული ალგორითმები*** - ან რაც იგივეა - **ალგორითმები ღია გასა­ღებით** - შემუშავებულია იმ პრინციპით, რომ გასაღები, რომელიც გამო­იყენება დაშიფვრისთვის განსხვავდება იმ გასაღებისგან, რომლითაც სარ­გებლობენ დეშიფრირებისთვის, ამასთან დეშიფრირების გასაღები არ შე­იძლება გამოთვლილ იყოს დაშიფვრის გასაღებით, ყოველ შემთხვევაში დროის ზომიერ, გონიერ ინტერვალში. ტერმინი ”ალგორითმები ღია გასაღებით” გამოიყენება იმოტომ, რომ დაშიფვრის გასაღები შეიძლება იყოს ღია, მისი ცოდნა შეუძლია ნებისმიერ ადამიანს, მაგრამ მხოლოდ კონკრეტულ პიროვნებას, რომელსაც აქვს დეშიფრირების გასაღები. ამი­ტომაც ასეთ კრიპტოგრაფიულ სისტემაში დაშიფრვის გასაღებს უწოდე­ბენ ღია გასაღებს, ხოლო დეშიფრირების გასაღებს - დახურულს. დახუ­რულ გასაღებს ზოგჯერ უწოდებენ საიდუმლო გასაღებსაც.

თუ კი დაშიფრვა ხდება ღია გასაღებით და გამოიყენება აღნიშვნა

**EK(M)=C**

**DK(C)=M**

უნდა ვიგულისხმოთ, რომ დაშიფრვისა და დეშიფრირების **K** გასაღებები სხვადასხვაა.

ზოგჯერ დაშიფრვა ხდება დახურული გასაღებით, ხოლო დეშიფრირება ღიათი, ასეთი სიტუაციაა როცა გამოიყენება ციფრული ხელმოწერა.

**კრიპტოანალიზი**

როგორც უკვე ვიცით, კრიპტოგრაფიის ამოცანაა ისეთი შიფროტექსტის შექმნა, რომელსაც ვერ გახსნის, გატეხავს მოწინააღმდეგე, თაღლითი, მიმტაცებელი და სხვა. ანუ საჭიროა ღია ტექსტის დაფარვა, ან გასაღების საიდუმლოდ შენახვა ან ორივე ერთად. ამ შემთხვევაში იგულისხმება, რომ მოწინააღმდეგე სრულად აკონტროლებს გამგზავნსა და მიმღებს შორის არსებულ კავშირის ხაზს.

კრიპტოანალიზის ამოცანა კი პირიქითაა - ღია ტექსტის მიღება, გასაღე­ბის არცოდნის პირობებში. წარმატებით ჩატარებულმა კრიპტოანალიზმა უნდა გახსნას შიფროტექსტი, ან დადგინოს გასაღები და შედეგად აღად­გინოს ღია ტექსტი. თავიდან კრიპტოანალიზმა შეიძლება აღმოაჩინოს სუსტი წერტილები კრიპტოსისტემაში, რისი საშუალებითაც შემდგომში მიიღწევა სასურველი შედეგი. გასაღების გაგებას არა კრიპტოლოგიური ხერხებით ეწოდება **კომპრომენტაცია**.

კრიპტოანალიზის მცდელობას ეწოდება გატეხვა. კრიპტოანალიზის ძი­რითადი დებულება (ჩამოაყალიბა XIX საუკუნეში დატჩმან ა. კერკხოფ­სმა) - უსაფრთხოება სრულად განისაზღვრება გასაღებით. ანუ მოწინა­აღმდეგემ შეიძლება იცოდეს ალგორითმი, ჰქონდეს მისი აღწერილობა, შიფროტექსტი, გადასაცემი შეტყობინების ხასიათი და მაინც ვერ შეძლოს მისი გატეხვა გასაღების არქონის გამო.

არსებობს ოთხი ძირითადი ტიპი კრიპტოანალიტიკური გატეხვისა. მიჩნეულია, რომ მოწინააღმდეგემ იცის ალგორითმი.

1. **გატეხვა მხოლოდ შიფროტექსტის გამოყენებით**. კრიპტოანალიტიკოს შეიძლება ჰქონდეს რამდენიმე შეტყობინების შიფროტექსტი, რომელიც ერთი და იგივე ალგორითმითაა დაშიფრული. კრიპტოანალიტიკოსის ამოცანაა ღია ტექსტის აღდგენა რაც შეიძლება მეტი შეტყობინების, ან, რაც კიდევ უკეთესია, გატეხოს გასაღები (გასაღებები), რომლებიც დაშიფვრისთვის გამოიყენეს და მათი საშუალებით მოახდინოს იმ შიფროტექსტების დეშიფრირება, რომლებიც ამ გასაღებებითაა დაშიფრული. მოცემულია: **C1=Ek(P1), C2=Ek(P2),….Ci=Ek(Pi)** - მისაღებია: **P1, P2,… Pi, k** გასაღები; ან ალგორითმი, თუ როგორ უნდა განვსაზღვროთ **Pi+1 , Ci+1=Ek(Pi+1)** -დან.
2. **გატეხვა ღია ტექსტის გამოყენებით.** კრიპტოანალიტიკოს აქვს რამდენიმე შეტყობინების შიფროტექსტი და მათი შესაბამისი ღია ტექსტებიც. მისი ამოცანაა გასაღების მიღება, რომლებიც დაშიფრვისთვის გამოიყენეს, რათა შემდგომში მოახდონოს იმ შიფროტექსტების დეშიფრირება, რომლებიც ამ გასაღებითაა დაშიფრული. მოცემულია: **P1,****C1=Ek(P1), P2,C2=Ek(P2),….** **Pi,Ci=Ek(Pi) -** მისაღებია: **k** გასაღები; ან ალგორითმი, თუ როგორ უნდა განვსაზღვროთ **Pi+1 , Ci+1=Ek(Pi+1)** -დან.
3. **გატეხვა ამორჩეული ღია ტექსტის გამოყენებით.** კრიპტოანალიტიკოს აქვს წვდომა შიფროტექსტზე და რამდენიმე შეტყობინების ღია ტექსტებზეც. ეს იძლევა უფრო მეტ ვარიანტს გატეხვისა, ვიდრე გატეხვა ღია ტექსტის გამოყენებით, რადგანაც კრიპტოანალიტიკოს შეუძლია ამოარჩიოს ღია ტექსტის დასა­შიფრი ბლოკი, რაც უფრო მეტ ინფორ­მაციას მოგვცემს გასაღების შესახებ. ამოცანა მდგომარეობს გასაღების მიღებაში, რომლითაც გვაქვს დაშიფრული ტექსტი.

მოცემულია: **P1,****C1=Ek(P1), P2,C2=Ek(P2),….** **Pi,Ci=Ek(Pi)** სადაც კრიპტოანალიტიკოს შეუძლია შეარჩიოს **P1, P2,… Pi**

მისაღებია: ან K, ან ალგორითმი, თუ როგორ მივიღოთ **Pi+1** **Ci+1=Ek(Pi+1)**-დან

4. **ადაპტიური** **გატეხვა ღია ტექსტის გამოყენებით.** ესაა კერძო შემთხვევა გატეხვისა ამორჩეული ღია ტექსტის გამოყენებით. კრიპტოანალიტიკოს შეუძლია ამოარჩიოს არა მარტო დასაშიფრი ტექსტი, არამედ ამის მერე შეუძლია გააკეთოს მომდევნო არჩევანი დაშიფრვის შედეგად მიღებულ რეზულტატებზე დაყრდნობით. წინა შემთხვევისგან განსხვავებით, მას შეუძლია აიღჩიოს ღია ტექსტის უფრო მცირე ბლოკი, პირველი არჩევანის რეზულტატების გათვალისწინებით და ა.შ.

ჩამოთვლილი ოთხი ძირითადი კრიპტოანალიტიკური გატეხვისა, სულ მცირე კიდევ სამი გატეხვაა:

5. **გატეხვა ამორჩეული შიფროტექსტის გამოყენებით**. კრიპტოანალიტიკოს შეუძლია ამოარჩიოს სხვადასხავა შიფროტექ­სტები დეშიფრირებისთვის და აქვს წვდომა დეშიფრირებულ ღია ტექსტებზე. მაგალითად კრიპტოანალიტიკოს აქვს წვდომა ”შავ ყუთთან”, რომელიც ახდენს ავტომატურ დეშიფრირებას. ამოცანა მდგომარეობს გასაღების მიღებაში. მოცემულია **C1, P1=Dk(C1), C2**, **P2=Dk(C2),…. Ci, Pi=Dk(Ci**); მისაღებია - **k** გასაღები. ასეთი ტიპის გატეხვა მიესადაგება ღია გასაღების ალგორითმებს. ზოგჯერ ეს მეთოდი გამოიყენება სიმეტრიული ალგორითმებისათვისაც.

**6**. **გატეხვა ამორჩეული გასაღების გამოყენებით**. აქ კრიპტოანალიტიკოსი რაღაც გარეშე არსებული ინფორმაციის საფუძველზე ასკვნის კავშირებს სხვადასხვა გასაღებებს შორის.

**7**. **ბანდიტური კრიპტოანალიზი**. კრიპტოანალიტიკოსი ემუქრება, აშანტაჟებს ანაც აწამებს ვინმეს, მანამ არ მიიღებს გასაღებს. მოქრთამვას კრიპტოლოგიაში უწოდებენ გატეხვას გასაღების მოსყიდვით.

**ალგორითმების უსაფრთხოება**.

ალგორითმის უსაფრთხოების ხარისხი დამოკიდებულია იმაზე, თუ რამდენად რთულია ალგორითმის გატეხვა. თუ კი ალგორითმის გატეხვის ფასი უფრო დიდია, ვიდრე დაშიფრული ინფორმაციის ფასი, მაშინ ცხადია ალგორითმი უსაფრთხოა. თუ კი ალგორითმის გატეხვის დრო, მეტია იმ დროზე, რომლის განმავლობაშიც საჭიროა შეტყობიმების საიდუმლოდ შენახვა, მაშინაც ალგორითმი უსაფრთხოა. თუ კი მონაცემთა რაოდენობა, რომელიც ერთი გასაღებითაა დაშიფრული ნაკლებია იმ მონაცემთა რაოდენობაზე, რომელიც საჭიროა ალგორითმის გატეხვაზე, მაშინაც ალგორითმი უსაფრთხოა.

ალგორითმების გატეხვის კატეგორიები დაახარისხა ლარს კნუდსენმა:

* **სრული გატეხვა**. კრიპტოანალიტიკოსმა მიიღო გასაღები K, ისეთი, რომ **DK(C) =P**.
* **გლობალური დედუქცია**. კრიპტოანალიტიკოსმა მიიღო ალტერნატიული ალგორითმი A გასაღები K-ს გარეშე, რომელიც **DK(C)**-ს ექვივალენტურია.
* **ადგილობრიცი (ლოკალური) დედუქცია**. კრიპტოანალიტიკოსმა მიიღო მიტაცებული შიფროტექსტისთვის ღია ტექსტი.
* **ინფორმაციული დედუქცია**. კრიპტოანალიტიკოსმა მიიღო გარკვეული ინფორმაცია გასაღებზე ან ღია ტექსტზე. შესაძლებელია მიღებულ იქნეს გასაღების რამდენიმე ბიტი, მონაცემები ღია ტექსტის ფორმაზე და ა.შ.

ალგორითმს ეწოდება **უპირობოდ უსაფრთხო**, თუ კი იმისდა მიუხედა­ვად, თუ რამდენი შიფროტექსტი აქვს კრიპტოანალიტიკოსს, ღია ტექ­სტის მისაღებად მაინც არ არის საკმარისი ინფორმაცია. თუ კი გატეხვა ხდება გასაღებების ყველა ვარიანტების მოსინჯვით, მას ეწოდება გატეხვა **უხეში ძალით**.

განსაკუთრებულ ინტერეს იწვევს კრიპტოსისტემები, რომელთა გატეხვა გამოთვლითი მეთოდებით რთულია. ალგორითმი ითვლება გამოთ­ვლით უსაფრთხო ( ან ძლიერი), თუ კი იგი არ შეიძლება გატეხილ იქნეს ამჟამად ან მომავალში არსებული რესურსების გამოყენებით. ”არსებული რესურსების” - ტერმინი არაზუსტია. გატეხვის სირთულე შეიძლება გაიზომოს, სხვადასხვა საშუალებით:

1. **მონაცემთა სირთულე**. მონაცემთა მოცულობა, რომელიც გატეხვის ოპერაციის დასაწყისში გამოიყენება.
2. **დამუშავების სირთულე**. დრო, რომელიც საჭიროა გატეხვისთვის. მას ასევე მუშაობის კოეფიციენტ ს უწოდებენ.
3. **მოთხოვნა მეხსიერების მიმართ**. გატეხვისთვის საჭირო მეხსიერების მოცულობა.

ემპირიული მეთოდით, გატეხვის სირთულე განისაზღვრება, ამ სამი მაჩვენებლიდან უდიდესი მნიშვნელობით.

სირთულე გამოისახება გარკვეული რაოდენობის მაჩვენებლით. თუ კი მოცემული ალგორითმისათვის დამუშავების სირთულე არის **2128**, მაშინ საჭიროა 2128 ოპერაცია გატეხვისთვის. მაგალითად თუ კი კომპიუტერი ასრულებს მილიონ ოპერაციას წამში, და გვაქვს მილიონი პარალელური პროცესორი, მაშინ გასაღების მისაღებად საჭირო იქნება **219** წელზე მეტი, რაც სამყაროს არსებობის დროზე მეტია.

გატეხვის სირთულე მუდმივია, მაშინ როცა, კომპიუტერების სიმძლავრე ყოველთვის მატულობას და ალგორითმის გამოცხადება უსაფრთხოდ, მხოლოდ იმიტომ, რომ ძნელია არსებული ტექნიკის პირობებში ამის გა­კეთება, არასაიმედოა. ამიტომაც გატეხვისადმი მდგრადი კრიპტოსის­ტემების პროექტირება ხდება იმაზე გათვლით, რომ დროთა განმავლო­ბაში გამოთვლითი სიმძლავრეები იზრდებიან.