***კრიპტოლოგია. ლექცია №3. ჩანაცვლება და გადაადგილება. ბლოკური შიფრები. ფეიშტელის (ფეისტელის) სქემა***

**ჩანაცვლება და გადაადგილება**.

კომპიუტერული კრიპტოგრაფიის წარმოშობამდე კრიპტოგრაფია წარმოადგენდა ალგორითმებს სიმბოლურ საფუძველზე. ანუ, კრიპტოგრაფიული ალგორითმები ან ჩაანაცვლებდნენ ერთ სიმბოლოს მეორეთი ან გადაადგილებდნენ სიმბოლოებს. მაგალითად გაიხსენეთ ცეზარის ალგორითმი. იმ დროს საუკეთესო ალგორითმები აკეთებდნენ ორივეს - ჩანაცვლებას და გადაადგილებას ერთდროულად.

დღესდღეობით, რა თქმა უნდა, კრიპტოგრაფიული ალგორითმების სირთულემ მოიმატა, მაგრამ ე.წ. ფილოსოფია იგივე დარჩა. ცვლილება კი შეეხო იმას, რომ კომპიუტერული კრიპტოგრაფიის ალგორითმები მუშაობენ არა სიმბოლოებზე, არამედ ბიტებზე ( 0 ან 1), მაგალითად სიმბოლოების- ანბანის ზომა (33 ქართული­დან, 26 ინგლისურიდან) შემცირდა ორამდე. დღემდე უმეტესი კრიპტოგრაფი­ული ალგორითმები იყენებენ ჩანაცვლებისა და გადაადგილების კომბინირებას.

*ჩანაცვლებითი შიფრები*.

ჩანაცვლებითი შიფრები ეწოდება ისეთ შიფრებს, რომლებიც ღია ტექსტის ყოველ სიმბოლოს შიფროტექსტში ცვლის სხვა სიმბოლოთი. მიმღები მოახდენს რა შიფროტექსტის ჩანაცვლების ინვერტირებას, მიიღებს ღია ტექსტს. კლასიკურ კრიპტოგრაფიაში არსებობს ოთხი ტიპის ჩანაცვლებითი შიფრები:

1. **მარტივი ჩანაცვლებითი შიფრი** ან მონოანბანური შიფრი - ესაა შიფრი, რომელიც ღია ტექსტის ყოველ სიმბოლოს ცვლის შიფროტექსტის შესაბამის სიმბოლოთი. მისი მაგალითია ცეზარის შიფრი. ამ შემთხვევაში შიფროტექსტის ანბანი არის ღია ტექ­სტის ანბანი 3 ერთეულით წანაცვლებული.

მარტივი ჩანაცვლებითი შიფრი ადვილათ ტყდება, რადგანაც მას ახასიათებს ინ­ფორმაციული სიჭარბე - ეს შიფრი ვერ მალავს სხვადასხვა სიმბოლოების გამოყენების ალბათობებს ღია ტექსტში. ღია ტექსტის აღსადგენად ამ შემთხვევაში კვალიფიცირე­ბულ კრიპტოანალიტიკოს სჭირდება მხოლოს ანბანის ცოდნა.

2. **ცალხმოვანი (ომოფონური)** ჩანაცვლებითი შიფრი მსგავსია მარტივი ჩანაცვლები­თი შიფრის, იმ განსხვავებით, რომ ღია ტექსტის ყოველ სიმბოლოს (ღია ტექსტია ანბანის ასოს) შეესაბამება შიფროტექსტის (შიფროტექსტის ანბანის) არა ერთი სიმ­ბოლო, არამედ ამ სიმბოლოთა რამდენიმე ვარიანტი, რომელთაგანაც ყოველი ცალ­სახად შეესაბამება საწყის სიმბოლოს ღია ტექსტიდან. მაგალითად ”ა”-ს შეიძლება შევუსაბამოთ ან 5, ან 14, ან 31-ს; ”ბ”-ს შეესაბამენა ან 7, ან 15, ან 41 - შიფრირების დროს ეს ყველაფერი შეიძლება ასე ჩავწეროთ: ”ა” 🡪 {5;14;31} და ”ბ” 🡪{7;15;41}. დე­შიფრირების დროს გვაქვს {5;14;31}🡪”ა”და {7;15;41} 🡪 ”ბ”. ვთქვათ ღია ტექსტია ”ბა­ბაბა” ცალხმოვანი (ომოფონური)ჩანაცვლებითი შიფრით მივიღებთ ”15 14 41 5 7 31” ასეთ შიფროტექსტს.

ცალხმოვანი (ომოფონური)ჩანაცვლებითი შიფრი გამოიყენებოდა უკვე 1401 წელს მანტუას საჰერცოგოში (ჩრდილოეთ იტალია). მათი გატეხვა უფრო რთულია, ვიდრე მარტივი ჩანაცვლებითი შიფრის, იმისდა მიუხედავათ, რომ ისიც ვერ ფარავს ყველა სტატისტიკურ კანონზომიერებას ღია ტექსტის ენისა -ანბანისა. ცნობილი ღია ტექსტით შეტევისას ეს შიფროტექსტები ტრივიალურად გატყდება. შეტევა მხოლოდ შიფრიტექსტების გამოყენებით ცოტათი რთულია, და თანამედროვე კონპიუტერე­ბით მას რამდენიმე წამი სჭირდება.

3. **პოლიგრაფული ჩანაცვლებითი შიფრი.** პოლიგრაფულ ჩანაცვლების შიფრში [ღია ტექსტის](http://ka.wikipedia.org/wiki/%E1%83%A6%E1%83%98%E1%83%90_%E1%83%A2%E1%83%94%E1%83%A5%E1%83%A1%E1%83%A2%E1%83%98_%28%E1%83%99%E1%83%A0%E1%83%98%E1%83%9E%E1%83%A2%E1%83%9D%E1%83%92%E1%83%A0%E1%83%90%E1%83%A4%E1%83%98%E1%83%90%29) არა ერთი სიმბოლო, არამედ სიმბოლოთა ჯგუფი იცვლება. მაგალიღად თუ გვაქვს ღია ტექსტში ”**აბბ**” მას შეიძლება შევუსაბამოთ ანუ ისინი ჩავნაცვლოთ ”**ცდს**”-თი, ხოლო ”**აბა**”-ს ” **ჰქჯ**”. ამ მეთოდის უპირატესობაა სიმბოლოთა სიხშირული განა­წილების გათანაბრება, თუმცა არასრულად. ამავე დროს ჩასანაცვლებელ ჯგუფთა დიდ სიმრავლის გამო რთულდება შიფროტექსტის კრიპტოანალიზი. მაგ. ქართული ანბანისათვის, თუ ჩანაცვლება მოხდება წყვილ-წყვილად, მაშინ იარსებებს 33x33=1089 ჯგუფი.

პირველი პრაქტიკული დიგრაფული შიფრი ”სამართლიანი თამაში” – (Play-fair) გა­მოიგონა ***ჩარლზ ვიტსტოუნმა*** 1854 წელს, რომელიც ინგლისელებმა პირველ მსოფ­ლიო ომში გამოიყენეს. სხვა პოლიგრაფული შიფრები აღწერა ***ფელიქს დელასტელიმ*** 1901 წელს, მათ შორის ტრიგრაფული შიფრი.1929 წელს ლესტერ ჰილმა გამოიგონა **ჰილის შიფრი**, რომელშიც ხდებოდა სომბოლოთა დიდი ჯგუფების ჩანაცვლება, [წრფივი ალგებრის](http://ka.wikipedia.org/wiki/%E1%83%AC%E1%83%A0%E1%83%A4%E1%83%98%E1%83%95%E1%83%98_%E1%83%90%E1%83%9A%E1%83%92%E1%83%94%E1%83%91%E1%83%A0%E1%83%90) დახმარებით. ყოველი სიმბოლო განიხილება როგორც რიცხვი, A=0, B=1, C=2 და ა.შ. N სიმბოლოსგან შემდგარი ჯგუფი განიხილება, როგორც N გან­ზომილების ვექტორი, და მრავლდება N×N [მატრიცაზე](http://ka.wikipedia.org/wiki/%E1%83%9B%E1%83%90%E1%83%A2%E1%83%A0%E1%83%98%E1%83%AA%E1%83%90_%28%E1%83%9B%E1%83%90%E1%83%97%E1%83%94%E1%83%9B%E1%83%90%E1%83%A2%E1%83%98%E1%83%99%E1%83%90%29). ეს მატრიცა წარმოადგენს გასაღებს და დგება, იმ პირობით რომ ჰქონდეს შებრუნებული (რათა შესაძლებელი გახდეს დეშიფრაცია). ჰილის შიფრი ტყდება [ცნობილი ღია ტექსტის შეტევით](http://ka.wikipedia.org/w/index.php?title=%E1%83%A8%E1%83%94%E1%83%A2%E1%83%94%E1%83%95%E1%83%90_%E1%83%AA%E1%83%9C%E1%83%9D%E1%83%91%E1%83%98%E1%83%9A%E1%83%98_%E1%83%A6%E1%83%98%E1%83%90_%E1%83%A2%E1%83%94%E1%83%A5%E1%83%A1%E1%83%A2%E1%83%98%E1%83%97&action=edit&redlink=1), ვინა­იდან მასში ხდება მხოლოდ წრფივი გარდაქმნები. კრიპტოანალიზის გასართულებ­ლად აუცილებელია შეტანილ იქნას არაწრფივი მათემატიკური გარდაქმნები, რასაც ე.წ. [ფეისტელის ქსელებამდე](http://ka.wikipedia.org/w/index.php?title=%E1%83%A4%E1%83%94%E1%83%98%E1%83%A1%E1%83%A2%E1%83%94%E1%83%9A%E1%83%98%E1%83%A1_%E1%83%A5%E1%83%A1%E1%83%94%E1%83%9A%E1%83%98&action=edit&redlink=1) მივყავართ. ეს უკანასკნელი კი თანამედროვე [ბლოკური შიფრების](http://ka.wikipedia.org/w/index.php?title=%E1%83%91%E1%83%9A%E1%83%9D%E1%83%99%E1%83%A3%E1%83%A0%E1%83%98_%E1%83%A8%E1%83%98%E1%83%A4%E1%83%A0%E1%83%94%E1%83%91%E1%83%98&action=edit&redlink=1) ძირითად მოდულს წარმოადგენს და ჩვენ მას ქვემოთ განვიხილავთ.

4. **პოლიანბანური ჩანაცვლებითი შიფრი**. პოლიალფაბეტური შიფრი შედგება რამ­დენიმე მარტივი ჩანაცვლებითი შიფრისგან. ღია ტექსტის ყოველი სიმბოლო ჩაინაც­ვლება რომელიმე ერთი კონკრეტული შიფრით. პოლიალფაბეტურ შიფრში გამოიყე­ნება ჩანაცვლების მრავალი ანბანი. ყველა ეს ანბანი ჩამოიწერება ერთ ცხრილში, რომელსაც **ტაბლო** ეწოდება. ლათინური ანბანისათვის, ტაბლო წარმოადგენს 26X26 განზომილების ცხრილს. თითოეულ ანბანში სიმბოლოების მიმდევრობა განსაზ­ღვრავს შიფრაციის პროცესს. ვინაიდან საკმარისად დიდი [ღია ტექსტისათვის](http://ka.wikipedia.org/wiki/%E1%83%A6%E1%83%98%E1%83%90_%E1%83%A2%E1%83%94%E1%83%A5%E1%83%A1%E1%83%A2%E1%83%98_%28%E1%83%99%E1%83%A0%E1%83%98%E1%83%9E%E1%83%A2%E1%83%9D%E1%83%92%E1%83%A0%E1%83%90%E1%83%A4%E1%83%98%E1%83%90%29), ანბან­თა გამოყენება შიფრაციის დროს მეორდება, ამიტომ ამ მეთოდით დაშიფრული ტექსტის გატეხვაც საკმაოდ იოლია.ამდენად ამ დაშიფრვის პროცეში ყოველი 26-ე სიმბოლო იმავე შიფრით იქნება დაშიფრული. ამ პატამეტრს **შიფრის პეროიდი** ეწო­დება. ასეთნაირად პოლიალფაბეტური ჩანაცვლების შიფრი, დისკების სახით პირვე­ლად აღწერილ იქნა 1568 წელს [***ლეონ ბატისტას***](http://ka.wikipedia.org/w/index.php?title=%E1%83%9A%E1%83%94%E1%83%9D%E1%83%9C_%E1%83%91%E1%83%90%E1%83%A2%E1%83%98%E1%83%A1%E1%83%A2%E1%83%90_%E1%83%90%E1%83%9A%E1%83%91%E1%83%94%E1%83%A0%E1%83%A2%E1%83%98&action=edit&redlink=1) მიერ. მას იყენებდა აშშ-ს არმია სამო­ქალაქო ომის დროს. შიფრი **მორბენალი გასაღებით** (წიგნის გასაღები), გამოიყენება ერთ ტექსტს მეორის დაშიფრვისთვის. ამ შემთხვევაში ამ შიფრის პერიოდი ტექსტის სიგრძის ტოლია.

# *გადანაცვლებადი შიფრი*

# გადანაცვლებად შიფრში იცვლება არა ღია ტექსტი, არამედ სიმბოლოების რიგითობა. მიღებული შედეგი ფაქტობრივად წარმოადგენს საწყისი ინფორმაციის სიმბოლოების *პერმუტაციას*. ქვემოთ ჩამოთვლილია გადანაცვლებადი შიფრის ზოგიერთი რეალი­ზაცია

**მარტივ სვეტურ გადანაცვლებად** შიფრში განსაზღვრული ზომის ცხრილში ღია ტექ­სტი იწერება ჰორიზონტალურად, ხოლო ვერტიკალურად იკითხება შიფროტექსტი. დეშიფრაციის პროცესში შიფროტექსტი იწერება იგივე ზომის ცხრილში ვერტიკალუ­რად, ხოლო ჰორიზონტალურად ამოიკითხება ღია ტექსტის ორიგინალი. მაგალი­თად, ვთქვათ დასაშიფრი ღია ტექსტია: ” მოდი ვნახოთ ვენახი” და გვაქვს ცხრილი 5X6 -ზე

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| მ | ო | დ | ი |  | ვ |
| ნ | ა | ხ | ო | თ |  |
| ვ | ე | ნ | ა | ხ | ი |

 ამ ცხრილში ვერტიკალურად ამოვიკითხოთ ასოები, მივიღებთ შიფროტექსტს - ”მნვოაედხნიოა თხვ ი” . დეშიფრაციის დროს თუ ეს შიფროტექსტი ჩაიწერება იგივე განზომილების ცხრილში ვერტიკალური მიმდევრობით, ბუნებრივია ჰორიზონტა­ლური ამოკითხვით აღდგება ორიგინალი ტექსტი. ამ შიფრში ცხრილის განზომილე­ბა (სვეტების და მწკრივების რაოდენობა) წარმოადგენს [შიფრის გასაღებს](http://ka.wikipedia.org/wiki/%E1%83%92%E1%83%90%E1%83%A1%E1%83%90%E1%83%A6%E1%83%94%E1%83%91%E1%83%98_%28%E1%83%99%E1%83%A0%E1%83%98%E1%83%9E%E1%83%A2%E1%83%9D%E1%83%92%E1%83%A0%E1%83%90%E1%83%A4%E1%83%98%E1%83%90%29).

ამ შიფრის ერთერთი ვარიაცია გამოიყენებოდა [აშშ-ს სამოქალაქო ომში](http://ka.wikipedia.org/wiki/%E1%83%90%E1%83%A8%E1%83%A8-%E1%83%98%E1%83%A1_%E1%83%A1%E1%83%90%E1%83%9B%E1%83%9D%E1%83%A5%E1%83%90%E1%83%9A%E1%83%90%E1%83%A5%E1%83%9D_%E1%83%9D%E1%83%9B%E1%83%98), რომელშიც სიმბოლოების ნაცვლად სიტყვების გადანაცვლება ხდებოდა. განსაკუთრებით მნიშ­ვნელოვანი სიტყვები ჩანაცვლდებოდა შესაბამისი კოდური სიტყვებით. ასევე შიფ­როტექსტის გართულების მიზნით შესაძლებელია შეტყობინებას დამატებოდა სხვა­დასხვა უაზრო და არაფრისმომცემი სიტყვები.

მარტივ სვეტურ გადანაცვლებად შიფრში შეტევა ეფუძნება სიმბოლოთა სიხშირული განაწილების პრინციპს.

### სვეტებად გადანაცვლება

ამ შიფრში ხდება ღია ტექსტის ჩაწერა ცხრილად ჰორიზონტალურად, ხოლო ამოკით­ხვა ვერტიკალურად (მარშრუტის მსგავსად). გასხვავება იმაში მდგომარეობს, რომ ცხრილის განზომილებას და ამოკითხვის მიმდევრობას გასაღებად არჩეული სიტყვა განსაზღვრავს. კერძოდ, სვეტების რაოდენობა განისაზღვრება გასაღების სიმბოლო­ების რაოდენობით, ხოლო ამოკითხვის მიმდევრობა - ანბანში ამ სიმბოლოების ნომ­რით. მაგ. ღია ტექსტად ავიღოთ წინა მაგალითში გამოყენებული ფრაზა, ხოლო გასა­ღებად სიტყვა „ქართველი“. შედგება ცხრილი 8 სვეტით:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ქ** | **ა** | **რ** | **თ** | **ვ** | **ე** | **ლ** | **ი** |
| **8** | **1** | **7** | **4** | **3** | **2** | **6** | **5** |
| მ | ო | დ | ი |  | ვ | ნ | ა |
| ხ | ო | თ |  | ვ | ე | ნ | ა |
| ხ | ი |  |  |  |  |  |  |

შიფროტექსტია - ”ოოივე ვ ი აა ნნ დთ მხხ”. მის გასაშიფრად საჭიროა შევადგინოთ მარტიცა 8X5, რომლის სვვეტების რაოდენობა განისაზღვრება გასაღების სიგრძით, ხოლო მწკრივების რაოდენობა გამოითვლება შიფროტექსტის სიგრძის გაყოფით გა­საღების სიგრძეზე 24/8=3. შიფროტექსტი ჩამოიწერება ცხრილში სვეტებად, ხოლო სვეტები გადალაგდება გასაღების სიმბოლოების ანბანური ნომრის მიხედვით. შედე­გად მივიღებთ პირვანდელ ცხრილს, საიდანაც ინფორმაციის ჰორიზონტალური ამო­კითხვით აღდგება ორიგინალი ღია ტექსტი. შიფრაციის აღწერილი მეთოდი გასული საუკუნის შუა წლებამდე გამოიყენებოდა, როგორც უფრო რთული შიფრაციის პრო­ტოკოლების ერთერთი შემადგენელი ნაწილი.

### ორმაგი გადანაცვლება

გადანაცვლებადი შიფრი შედარებით იოლად ტყდება, თუ მოხდება შიფროტექსტის ჩამოწერა სვეტებად, შემდეგ კი სვეტებიდან შესაძლო ანაგრამების ძიება. ამიტომ ხში­რად გამოიყენებოდა ორმაგი გადანაცვლება, ანუ გადანაცვლების ოპერაციის გამეო­რება ორჯერ. გადანაცვლებისათვის იყენებდნენ ერთიდაიგივე, ზოგჯერ კი სხვადას­ხვა გასაღებს. აღნიშნულ მეთოდს მიმართავდნენ გერმანელები I და II მსოფლიო ომის დროს, ასევე დანიელები, ფრანგები, ინგლისელები და ამერიკელები. ორმაგი გადა­ნაცვლების შიფრი ყველაზე დახვეწილ შიფრაციის ალგორითმად ითვლებოდა ([VIC შიფრის](http://en.wikipedia.org/wiki/VIC_cipher) გამოგონებამდე), რომლის გამოყენებაც იოლად შეიძლებოდა საველე პირო­ბებში.

ვინაიდან გადანაცვლება არ მოქმედებს ღია ტექსტში სიმბოლოების სიხშირულ მახა­სიათებლებზე, მარტივი გადანაცვლებადი შიფრის გატეხვა შედარებით იოლია სიხ[­შირული ანალიზით](http://ka.wikipedia.org/w/index.php?title=%E1%83%A1%E1%83%98%E1%83%AE%E1%83%A8%E1%83%98%E1%83%A0%E1%83%A3%E1%83%9A%E1%83%98_%E1%83%90%E1%83%9C%E1%83%90%E1%83%9A%E1%83%98%E1%83%96%E1%83%98&action=edit&redlink=1). თუ შიფროტექსტის სიმბოლოების სიხშირული მახასიათებლე­ბი მეტნაკლებად ემთხვევა იმ ენის სიხშირულ მახასიათებლებს, რომელზეც ღია ტექ­სტია დაწერილი, მაშინ აშკარა ხდება გადანაცვლების გამოყენება შიფრში. შემდგომ ხდება შიფროტექსტის ფრაგმენტების გადაადგილება აზრობრივად გამართული რა­იმე ტექსტის ფრაგმენტის მოძიების მიზნით. წარმატების შემთხვევაში ხდება გადა­ნაცვლების მიმდევრობის დახვეწა და განვრცობა მთელ შიფროტექსტზე, რითაც სა­ბოლოოდ აღდგება ორიგინალი ღია ტექსტი. გადანაცვლებადი შიფრის კრიპტოანა­ლიზი განსაკუთრებით იოლია კომპიუტერების და ე.წ. [გენეტიკური ალგორითმების](http://ka.wikipedia.org/w/index.php?title=%E1%83%92%E1%83%94%E1%83%9C%E1%83%94%E1%83%A2%E1%83%98%E1%83%99%E1%83%A3%E1%83%A0%E1%83%98_%E1%83%90%E1%83%9A%E1%83%92%E1%83%9D%E1%83%A0%E1%83%98%E1%83%97%E1%83%9B%E1%83%94%E1%83%91%E1%83%98&action=edit&redlink=1) გამოყენებით.

## შეთავსება სხვა მეთოდებთან

გადანაცვლებადი შიფრის საიმედოობის ასამაღლებლად, ხშირად გამოიყენება მისი შეთავსება სხვა კრიპტოგრაფიულ მეთოდებთან. მაგ. [ჩანაცვლებადი შიფრის](http://ka.wikipedia.org/wiki/%E1%83%A9%E1%83%90%E1%83%9C%E1%83%90%E1%83%AA%E1%83%95%E1%83%9A%E1%83%94%E1%83%91%E1%83%90%E1%83%93%E1%83%98_%E1%83%A8%E1%83%98%E1%83%A4%E1%83%A0%E1%83%98) შეთავსე­ბა გადანაცვლებად შიფრთან აღმოფხვრის ორივე ალგორითმის სისუსტეებს - ჩანაც­ვლება ართულებს სიხშირულ ანალიზს, ხოლო გადანაცვლება ართულებს შიფრო­ტექსტში ჩანაცვლების აღმოჩენას. კრიპტოანალიზს კიდევ უფრო ართულებს ე.წ. და­ყოფის მეთოდის გამოყენება, როდესაც ღია ტექსტის ყოველი სიმბოლო გადანაცვლე­ბისას და ჩანაცვლებისას იყოფა 2 ან მეტ სხვა სიმბოლოებად. ასეთი შიფრის მაგალი­თია ზემოაღნიშნული [**VIC** შიფრი](http://en.wikipedia.org/wiki/VIC_cipher). კომპიუტერულ ალგორითმებში ხშირად გამოიყე­ნება ღია ტექსტის სიმბოლოების გარდაქმნა ბინარულ ფორმატში, ბიტებზე გადანაც­ვლების და ჩანაცვლების ოპერაციები და შემდეგ ბაიტების უკუგარდაქმნა სომბოლო­ებად შესაბამის ASCII კოდებში. მრავალი თანამედროვე [ბლოკური შიფრი](http://ka.wikipedia.org/w/index.php?title=%E1%83%91%E1%83%9A%E1%83%9D%E1%83%99%E1%83%A3%E1%83%A0%E1%83%98_%E1%83%A8%E1%83%98%E1%83%A4%E1%83%A0%E1%83%98&action=edit&redlink=1) იყენებს მსგავს, მაგრამ გაცილებით რთულ მეთოდიკას.

გერმანული შიფრი **ADFCVX** , რომელიც პირველ მსოფლიო ომში გამოიყენებოდა, წარმოადგენდა გადანაცვლებადი და მარტივი ჩანაცვლების შიფრების კომბინაციას. თავის დროზე ეს შიფრი ძალიან რთული იყო, მიუხედავად ამისა იგი ფრანგი ***ჟორჟ პენვენ***ის მიერ იყო გატეხილი.

 **ენიგმა** — გერმანული წარმოების პორტატიული ელექტრომექანიკური მანქანა, ის იყენებს როტორებს, საიდუმლო ინფორმაციის კოდირებისათვის და\ან დეკოდირები­სათვის.

**მარტივი XOR**

XOR – ეს არის ოპერაცია ”არის გამორიხცვა”. იგი ოპერაციაა ბიტებზე

0 0=0

0 1=1

1 0=1

1 1=0

ასევე

a a=0

abb=a

**ბლოკური შიფრი**

ბლოკური შიფრი შეიძლება განვსაზღვროთ როგორც K გასაღებზე დამოკიდებული n ორობითი სიმბოლოებისგან შემდგარი X სიტყვის გარდაქმნა. სიტყვის (ბლოკის) გარ­დაქმნა შიფრის საშუალებით ავღნიშნოთ Y-ით.

ამდენად, ბლოკური შიფრი - ესაა შებრუნებადი ფუნქცია E (ანუ ისეთი ფუნქცია, რომლის შებრუნებული არსებობს). EK ფუნქციის კონკრეტული სახე განისაზღვრება K გასაღებით,

Y= EK(X), X= E K -1 (Y) ყველა X-ის თვის.

აქ E K -1 არის დეშიფრირების გარდაქმნა და ეწოდება შებრუნებული შიფრი. კრიპტო­გრაფიის ბლოკური შიფრი უნდა აკამყოფილებდეს გარკვეულ მოთხოვნებს. პირველ რიგში უნდა იყოს მოთხოვნა, რომ შიფრი უნდა იყოს მდგრადი ამორჩეული ღია ტექ­სტის გამოყენებით გატეხვის მცდელობისადმი. ეს კი ავტომატურად ნიშნავს იმას, რომ იგი მდგრადი იქნება ცნობილი ღია ტექსტის გამოყენებით გატეხვის მცდელო­ბისადმი. შევნიშნოთ, რომ ამორჩეული ღია ტექსტის გამოყენებით გატეხვის მცდე­ლობისას გასაღებების სრული გადარჩევის შემთხვევაში ყველა შიფრი გატყდება. ამიტომ შეიძლება დავაზუსტოთ, თუ რას ნიშნავს შიფრის მდგრადობა (მედეგობა).

შიფრი მედეგია (მდგრადია) (ამორჩეული ღია ტექსტის შეტევისადმი), თუ კი მის­თვის არ არსებობს გატეხვის ისეთი ალგორითმები, რომელიც უფრო სწრაფია, ვიდრე გასაღებთა სრული გადარჩევის გატეხვა.

მაგრამ რეალურად დღესდღეობით არაა დამტკიცებული არცერთი ცნობილი დაშიფ­რვის ამ განმარტების შესაბამი მედეგობა. ამიტომ მედეგობის ეს განმარტება ჩამოვაყ­ალიბოთ შემდეგნაირად.

***შიფრი მედეგია (მდგრადია***) (ამორჩეული ღია ტექსტის შეტევისადმი), თუ კი მის­თვის არაა ცნობილი გატეხვის ისეთი ალგორითმები, რომელიც უფრო სწრაფია, ვიდ­რე გასაღებთა სრული გადარჩევით გატეხვა.

**ფეისტელის ქსელი**

როგორც ვიცით ბლოკური შიფრი გარდაქმნის ღია ტექსტის n-ბიტურ ბლოკს შიფრო­ტექსტის n-ბიტურ ბლოკ ში.ბლოკების n სიგრძე აკმაყოფილებს პირობას n= 2 m , სა­დაც m ნატურალური რიცხვია. იმისთვის, რომ გარდაქმნა იყოს შექცევადი, ყოველი ბლოკი უნდა გარდაიქმნეს უნიკალურ დაშიფრულ ბლოკში. ბლოკის მცირე ზომისას ჩანაცვლება ცუდად დაფარავს ღია ტექსტის სტატისტიკურ განსაკუთრებულობებს. თუ ბლოკს აქვს სიგრძე 64, მაშინ ის უკვე კარგად დამალავს ღია ტექსტის სტატისტი­კურ განსაკუთრებულობებს.მაგრამ ეს არასკმარისია, რადგანაც ამ შემთხვევაში გარ­დაქმნა იქმნება თავად გასაღები, და ის არ იქნება ეფექტური. განსაკუთრებულად სა­ინტერესოა ფეისტელის ქსელი, რადგანაც ისინი აკმაყოფილებენ სიმეტრიული ალგო­რითმის მოთხოვნას და მეორეს მხრივ არიან კომპაქტური და მარტივი.

 ფეისტელის ქსელს აქვს შემდეგი სტრუქტურა. შემავალი ბლოკი იყოფა რამდენიმე თანაბარი სიგრძის რამდენიმე ქვებლოკად, რომელთაც განშტოებები ეწოდება. თუ კი ბლოკს აქვს სიგრძე 64, მაშინ გამოიყენება ორი განშტოება, თითოეული 32 ბიტიანი ქვებლოკით. თითოეული განშტოება გარდაიქმნება - დაიშიფრება მეორისგან დამო­უკიდებლად. რის შემდეგაც მოხდება ყველა განშტოებების ციკლური გადაადგილება მარცხვნივ. ასეთი გარდაქმნა ხდება რამდენიმეჯერ - ციკლის ან რაუნდის მეშვეობით.

Li-1

Ri-1

Ki

F

Li-1

Ri-1

ნახარი 1. ფეისტელის ქსელის I-ური რაუნდი

ფუნქცია F -ს ეწოდება *წარმომქმნელი*. ყოველი რაუნდი შედგება F ფუნქციის გამოთ­ვლებისაგან ერთი განშტოებისთვის და ბიტური ოპერაციის - XOR მოქმედება. F-ის სახისას და მეორე განშტოებისა. ამის მერე განშტოებები იცვლიან ადგილს ამასთან ერთი განშტოება უცვლელად გადმოდის (მარჯვენა -მარცხენაში).ითვლება, რომ რა­უნდის ოპტიმალური რაოდენობა 8-დან-32-მდე. რაუნდების გაზრდა ზრდის კრიპ­ტოსისტემის მდგრადობას - მედეგობას. ამიტომაცაა, რომ ფეისტელის ქსელი ასე პო­პულარული გახდა.

 ფეისტელის ქსელი არის შექცევადი, მიუხედავად იმისა, თუ კი ასეთი არაა F ფუნ­ქცია, ანუ არ არსებობს F-1 , რადგანაც დეშიფრირებისთვის არა საჭირო F-1 -ის გა­მოთვლა. დეშიფრირებისთვის საჭიროა იგივე ალგორითმი, მაგრამ შესასვლელზე მოიცემა შიფროტექსტი. დღესდღეობით გამოიყენება 128-ბიტიანი ბლოკი ოთხი განშტოებით. ის რომ იზრდება განშტოებები და არა განშტოების ზომები, უჩვენებს იმას, რომ 32 ბიტიანმა განშტოებამ თავის თავი კარგად წარმოაჩინა.

ფეისტელის ქსელის საფუძველზე შექმნილ დაშიფრვის ალგორითმებისთვის მთავარია F ფუნ­ქცია. აქვე შევნიშნოთ, რომ ყოველ რაუნდში განცხვავებულიგასაღები მოისაზრება.

 ფეისტელის ქსელზე დაფუძნებულია სხვადასხვა ცნობილი სიმეტრიული კრიპტოსისტემები.

ჯერ კიდევ სულ ახლო წარსულში DES- (Data Encryption Standard) იყო სტანდარტად მიჩნეული აშშ-ში 1977 წლიდან. მისი ბლოკის სიგრძე 64 ბიტია, გასაღების სიგრძე 56 ბიტი, 16 რაუნდი. იგი ორი ათეული წლის განმავლობაში იყო სტანდარტი, ამჟამად კი, მიუხედავათ იმისა, რომ არაერთი შეტევებისა DES -ზე იგი არ გატეხილა, მაინც კომპიუტერული ტექნიკის სიმძლავრეების გაზრდასთან ერთად გასაღების სრული გადარჩევით შესაძლებელია მისი გატეხვა. ასე მაგალითად, 1993 წელს გამოქვეყნდა ტექნიკური აღწერილობა იმ სისტემისა, რომელიც ერთ მილიონ დოლარადაა შეფასებული, და რომლის მეშვეობითაც DES-ის ნებისმიერი გასაღები გატყდება 7 საათში. ამიტომაც ახალი სისტემების პროექტირებაში ის აღარ გამოიყენება. აშშ-ში 2001 წელს გამოცხადებული კონკურსში გამარჯვებულის საფუძველზე შეიქმნა ბლოკური შიფრირების ახალი სტანდარტი AES (Advanced Encryption Standard), რომლის საფუძველია შიფრი Rijndael, შექმნილი ბელგიელი სპეციალისტების მიერ.

საბჭოთა კავშირის უშიშროება გასული საუკუნის 70 წლებიდან მუშაობდა ბლოკურ შიფრებზე რომელიც ფეისტელის ქსელს ეფუძნებოდა და შემდეგ ამ სახელითაა ცნობილი ГОСТ 28147-89 და მიღებულია რუსეთის სტანდარტად 1989 წლიდან - მას აქვს ბლოკის სიგრძე 64 ბიტი, გასაღების სიგრძე 256 ბიტი, 32 რაუნდი.

AES (Advanced Encryption Standard) -ის ავტორებია ბელგიელი მეცნიერები ვინსენტ რეიმენი (Vincent Rijmen. დაიბ. 1970 წ. ) და იოან დამანი (Joan Daemen . დაიბ. 1965 წ.) , აქვს ბლოკის სიგრძე 128 ბიტი, გასაღების სიგრძე 128, 192 ან 256 ბიტი; 10, 12 ან 14 რაუნდი, იმისდა მიხედვით როგორია გასაღების სიგრძე.

AES (Advanced Encryption Standard) Rijndael (რეინდალის)- ს არითმეტიკა . განსხვავებით DES- ისაგან , Rijndael- ში ყველა ოპერაცია , რომელიც სრულდება დასაშიფრ ბლოკზე , ეფუძნება არითმეტიკას FG(28 ) ველში , ამიტომ აქ შევიძლია ალგორითმის სუსტი და ძლიერი მხარეები შევაფასოთ. ალგებრიდან ჩვენთვის ცნობილია , რომ ერთი და იგივე რიგის ყველა სასრული ველი იზომორფულია და ერთმანეთისაგან განსხვავდებიან მხოლოდ ელემენტების წარმოდგენით. Rijndael- ში მიღებულია კლასიკური, პოლინომური წარმოდგენა, სადაც რიცხვები წარმოიდგინება რვაბიტიანი (ბაიტიანი) ვექტორების სახით . რაიმე ბაიტი b, რომლიც შედგება b7 , b6 , …, b0 ბიტებისაგან, წარმოადგენს პოლინომს კოეფიციენტებით {0,1} სიმრავლიდან , რომელსაც აქვს შემდეგი სახე :

b7 X7+ b6 X6 +….+ b0

ამასთან, კომპიუტერში ინახება მხოლოდ ვექტორი, რომელიც შედგენილია ამ პოლინომის კოეფიციენტებისაგან და რომელიც აღიქმება როგორც თექვსმეტობითი რიცხვი. მაგალითად, ბაიტი, რომლის თექვსმეტობითი მნიშვნელობაა (57)hex  და ორობითი მნიშვნელობა კი 01010111, შეესაბამება პოლინომს

 X6+ X4 + X2 +X+1

ასეთი წარმოდგენის პირობებში ორი პოლინომის შეკრების ოპერაცია პრაქტიკულად წარმოადგენს მსგავსი წვერების კოეფიციენტების XOR- ით შეკრებას .

 პოლინომურ წარმოდგენაში FG(28 ) ველში რიცხვების გამრავლება შეესაბამება პოლინომების გამრავლებას რომელიმე მერვე ხარისხის დაუყვანადი ბინარული პოლინომის მოდულით. Rijndael- ში ასეთ პოლინიმად აღებულია

 M(X)= X8+ X4 + X2 +X+1

გამრავლების მიმართ ერთეულოვანი ელემენტია (01)hex  შეკრებისაგან განსხვავებით, გამრავლების დროს უკვე აღარ გვაქვს მარტივი ოპერაცია ბიტების დონეზე. იმისათვის, რომ ადვილად განხორციელდეს გამრავლების ოპერაცია, ავტორებმა გამოიყენეს თვისება, რომ ორობით სისტემაში რიცხვის ორზე გამრავლება ტოლფასია რიცხვის ერთი თანრიგით მარცხნივ წაძვრის და შემდეგ, თუ საჭიროა უნდა მოვახდინოთ XOR- ით შეკრება (1B)hex  -თან (ეს რიცხვი პოლინომურ წარმოდგენაში ტოლია მოდულის ფუძის). *xtime*( ) აღნიშნულია ფუნქცია რომელიც ანხორციელებს გამრავლებას x - ზე ამ მეთოდით . მაშინ n - ჯერ ამ ფუნქციის გამოყენებით შესაძლებელია მივიღოთ xn - ზე გამრავლების შედეგი და შემდეგ x -ის სხვადასხვა ხარისხების შეკრებით მივიღოთ ველის ნებისმიერი ელემენტი. მაგალითად, დავუშვათ, გვინდა გავმოვთვალოთ (57)hex. (13)hex . ვიქცევით შემდეგნაირად, რადგანაც

(13)hex =(01)hex(02)hex(10)hex

ჯერ xtime( ) ფუნქციის საშუალებით გამოვთვალოთ შემდეგი სიდიდეები :

 (57)hex .(02)hex= xtime(57)= (AE)hex

(57)hex .(04)hex= xtime(AE)= (47)hex

(57)hex .(08)hex= xtime(47)= (8E)hex

(57)hex .(10)hex= xtime(8E)= (07)hex

მაშინ

(57)hex .(13)hex=(57)hex.( (01)hex(02)hex(10)hex)= (57)hex(AE)hex(07)hex=(FE)hex

Rijndael- ში პოლინომი შეიძლება განიმარტოს აგრეთვე F28 [X ] რგოლიდან. ასეთ შემთხვევაში ოცდათორმეტ ბიტიან სიტყვას შეესაბამება მესამე ხარისხის პოლინომი, რომლის კოეფიციენტებსაც წარმოადგენენ რვაბიტიანი რიცხვები, ამასთან კოეფიციენტების მინიჭება ხდება შებრუნებით. ანუ, თუ ოცდათორმეტბიტიანი სიტყვა დაყოფისას გვაძლევს ოთხ რიცხვს

 a0 a1 a2 a3

მაშინ პოლინომს აქვს სახე :

a3 X3+ a2 X2 +a1 X1 +a0

ალგორითმში შემოტანილი არითმეტიკა ემთხვევა არითმეტიკას F28 [X ] რგოლში მოდულით

M(x)=x4 +1=(x+1)4

 საინტერესოა, რომ (x+1)4 არ არის დაუყვანადი პოლინომი და ამიტომ შესაძლებელია გვქონდეს ნოლის გამყოფები, ანუ პოლინომს არ გააჩნდეს შებრუნებული პოლინომი, მაგრამ ალგორითმში ისეა შერჩეული ფიქსირებული პოლინომი, რომ მას გააჩნია შებრუნებული პოლინომი ამ მოდულით. ასეთი მოდულის გამოყენება განაპირობა იმან, რომ

Xi mod (X+1)4 =Ximod4

რაც ცხადია ამარტივებს მოდულის გამოთვლას.

ალგორითმში პოლინომის გამრავლება ამ ფიქსირებულ პოლინომზე და პოლინომის გამრავლება x ერთწევრზე შეიძლება მატრიცების საშუალებით, კერძოდ:

a(x) (b(x)=d(x)mod(x+a)4  

სადაც a(x) ფიქსირებული პოლინომია, მატრიცულად ტოლია

$\left[\begin{array}{c}d\_{0}\\d\_{1}\\d\_{2}\\d\_{3}\end{array}\right]$=$\left[\begin{array}{c}a\_{0} a\_{3} a\_{2} a\_{1}\\a\_{1} a\_{0} a\_{3} a\_{2}\\a\_{2} a\_{3} a\_{0} a\_{1}\\a\_{3} a\_{2} a\_{1} a\_{0}\end{array}\right]\left[\begin{array}{c}b\_{0}\\b\_{1}\\b\_{2}\\b\_{3}\end{array}\right]$

x b(x) შეესაბამება მატრიცული ნამრავლი

$\left[\begin{array}{c}c\_{0}\\c\_{1}\\c\_{2}\\c\_{3}\end{array}\right]$=$\left[\begin{array}{c}00 00 00 01\\01 00 00 00\\00 01 00 00\\00 00 01 00 \end{array}\right]\left[\begin{array}{c}b\_{0}\\b\_{1}\\b\_{2}\\b\_{3}\end{array}\right]$

ეს განმარტებები გაგვიადვილებს ალგორითმის გაგებას

ეს ალგორითმი განსხვავებით DES- საგან მიეკუთვნება იმ მცირერიცხოვან ბლოკურ ალგორითმებს, რომელიც არ იყენებენ ფეინსტელის სქემას. მას საფუძვლად უდევს ე. წ. “კვადრატის” არქიტექტურა . ეს სახელწოდება არქიტექტურამ მიიღო კრიპტოალგორითმ კვადრატისაგან, რომელიც 1996 წელს შექმნეს იმავე ავტორებმა ლარს კნუდსენთან ერთად. ალგორითმს შეუძლია იმუშაოს 192, 128 და 256 ბიტიან ბლოკებთან (თუმცა სტანდარტს წარმოადგენს 128 ბიტიანი ბლოკი). გასაღების სიგრძე ასევე შეიძლება იყოს 192, 128 და 256 ბიტის სიგრძის, ამასთან შესაძლებელია სხვადასხვა სიგრძის ბლოკებთან სხვადასხვა სიგრძის გასაღებების გამოყენება .

 ვინაიდან ალგორითმში ფაქტობრივად სრულდება ორი მარტივი ოპერაცია – XOR- ით შეკრება და ბაიტების ინდექსირებული ამოღება მეხსიერებიდან, ალგორითმი შეიძლება ეფექტურად იყოს რეალიზებული ყველა ცნობილი პლატფორმისა და აპარატურისათვის. ალგორითმში რაუნდების რაოდენობა დამოკიდებულია ბლოკისა და გასაღების ზომებზე. ეს დამოკიდებულება მოცემულია სპეციალური ცხრილით.

**შებრუნებული ოპერაციების არსებობა**. როგორც უკვე აღვნიშნეთ, განსხვავებით DES- ისაგან, Rijndael- ი არ არის აგებული ფეისტელის სქემის მიხედვით, მისი არქიტექტურა არის ე . წ . კვადრატი და მასში ყოველი გარდაქმნა ემორჩილება ზევით განხილულ არითმეტიკულ ოპერაციებს. ფეისტელის სქემა, როგორც ეს აღნიშნული იყო DES- ის განხილვის დროს, თვითონ არის შებრუნებადი სქემა და არა აქვს მნიშ­ვნელობა როგორი სახის ფუნქცია გამოიყენება დასაშიფრად. რადგანაც კვადრატულ არქიტექტურას აღარ გააჩნია ასეთი თვისება, იმისათვის, რომ დეშიფრაციის პროცესი წარიმართოს დაშიფრვის სიმეტრიულად საჭიროა დაშიფრვის პროცესში გამოყენე­ბულ ოპერაციებს გააჩნდეთ შებრუნებული ოპერაციები, პრაქტიკულად ეს იმას ნიშ­ნავს, რომ დაშიფრვისა და დეშიფრაციის პროცედურები აღარ ემთხვევა ერთმანეთს .

 ცხრილი - რაუნდების დამოკიდებულება გასაღების და ბლოკის ზომებზე .

|  |  |  |  |
| --- | --- | --- | --- |
| გასაღების ზომაბლოკის ზომა | **128** | **192** | **256** |
| **128** | **10** | **12** | **14** |
| **192** | **12** | **12** | **14** |
| **256** | **14** | **14** | **14** |