**ლექცია № 2. კრიპტოლოგია. პროტოკოლი. მოთამაშეები. დახურული გასაღები**

კრიპტოგრაფიის დანიშნულებაა გარკვეული პრობლემის გადაწყვეტა. კრიპტოგ­რაფია ახდენს საიდუმლოების, ორიგინალობის შემოწმების,მთლიანობის პრობ­ლემების გადაწყვეტას. კრიპტოგრაფიული მეთოდები და ალგორითმები, თავის თავად არის აკადემიური ინტერესის საგანი, მაგრამ ამასთან საჭიროა მათი გამო­ყენება კონკრეტული პრობლემის მოსაგვარებლად.

**პროტოკოლი** - ესაა მოქმედებათა თანამიმდევრობა, რომელსაც მისდევს და ახორ­ციელებს ორი ან მეტი მხარე (ინგ. Party), რომელთაც სურთ გარკვეული ამოცანის გადაწყვეტა.

***”მოქმედებათა თანამიმდევრობა”*** - ნიშნავს, რომ პროტოკოლი სრულდება თავიდან ბოლომდე გარკვეული თანამიმდევრობით. ამასთან ყოველი ქმედება წინას დამთავ­რების შემდეგ იწყება.

***”ახორციელებს ორი ან მეტი მხარე”*** ნიშნავს, რომ პროტოკოლის რეალიზაცია საჭიროებს ორ ან მეტ ადამიანს, ანუ ერთი ადამიანი პროტოკოლის რეალიზაციას ვერ შეძლებს.

***”გარკვეული ამოცანის გადაწყვეტა”*** ნიშნავს, რომ პროტოკოლის რეალიზაციას მივ­ყავართ რომელიმე პრობლემის გადაწყვეტისკენ.

პროტოკოლი გააჩნია ასევე შემდეგი მახასიათებლები:

* პროტოკოლის ყოველმა მხარემ უნდა იცოდეს პროტოკოლი და მისი შემად­გენელი ნაწილები - თანამიმდევრული ქმედებები;
* პროტოკოლის ყოველი მხარე უნდა თანხმებოდეს პროტოკოლის დაცვაზე;
* პროტოკოლი უნდა იყოს არაწინააღმეგობრივი, ყოველი მოქმედება უნდა იყოს ისე გაწერილი და შესრულებული, რომ არ ტოვებდეს გაუგებრობებს;
* პროტოკოლი უნდა იყოს სრული, ყოველ შესაძლო სიტუაციას უნდა შეესა­ბამებოდეს ცალსახად განსაზღვრული ქმედება.

**კრიპტოგრაფიული პროტოკოლი** - ესაა პროტოკოლი, რომელიც იყენებს კრიპტოგ­რაფიას.

კრიპტოგრაფიული პროტოკოლის მხარეები:

***ალისა*** - ყველა პროტოკოლის პირველი მონაწილე (მხარე)

***ბობი*** - ყველა პროტოკოლის მეორე მონაწილე (მხარე)

კეროლი - სამი და ოთხი მონაწილის პროტოკოლის მესამე მხარე

დეივი - სამი და ოთხი მონაწილის პროტოკოლის მეოთხე მხარე

***ევა*** - თაღლითი (eavesdropper)

***მელორი*** - პროტოკოლების გამტეხი

ტრენტი - ნდობით აღჭურვილი შუამავალი

უოლტერი - კონტროლერი, იცავს ალისას და ბობს ზოგიერთ პროტოკოლში

პეგი - მოწმე

ვიქტორი - ამოწმებს ორიგინალობას

სიმეტრიული კრიპტოგრაფიის გამოყენებით ინფორმაციის გადაცემისას საქმე გვაქვს შემდეგი სახის პროტოკოლთან:

1. ალისა და ბობი ირჩევენ დაშიფრვის სისტემას;
2. ალისა და ბობი ირჩევენ გასაღებს;
3. ალისა შიფრავს თავისი შეტყობინების ღია ტექსტს დაშიფრვის ალგორითმისა და გასაღების მეშვეობით;
4. ალისა უგზავნის დაშიფრულ შეტყობინებას (შიფროტექსტს) ბობს;
5. ბობი ახდენს შიფროტექსტის დეშიფრირებას დაშიფრვის ალგორითმისა და გასაღების მეშვეობით რის შედეგადაც იღებს ღია ტექსტს.

ღია არხი

დეშიფრატორი

შიფრატორი

დახურული არხი

გასაღების წყარო

ნახატი 1. საიდუმლო კავშირის კლასიკური სქემა

*რა შეუძლია ევას*?

* თუ მას შეუძლია მხოლოდ ღია არხის გაკონტროლება და გადაცემული შიფ­როტექსტის მიტაცება პროტოკოლის IV ეტაპზე, მაშინ ის გამოყენებს კრიპტო­ანალიზს შიფროტექსტის მიმართ. ეს არის პასიური გატეხვა მხოლოდ შიფ­როტექსტის გამოყენებით, აქ გამოყენებული ალგორითმები კი არის ***მდგრადი*** (გატეხვის სირთულე) ნებისმიერი გამოთვლითი სიმძლავრეების მიმართ, რომელიც შეიძლება გა­მოიყენოს ევამ.
* ევას შეუძლია მიაყურადოს პროტოკოლის I და II ეტაპებს, და მაშინ მას ეცო­დინება ალგორითმი და გასაღები, ისევე როგორც ბობს. ამიტომ, როცა ის პროტოკოლის IV ეტაპზე მიიტაცებს შიფროტექსტს, მას იგი მარტივად გადა­აქცევს ღია ტექსტად.

*რა შეუძლია მელორის*?

* მას შეუძლია დააზიანის კავშირი პროტოკოლის IV ეტაპზე, და მაშინ ალისა ვერ გადასცემს ბობს შეტყობინებას.
* მას შეუძლია მიიტაცოს ალისას შეტყობინება, და მის ნაცვლად თავისი გაუგზავნოს ბობს.
* თუ მელორიმ იცის გასაღები (მიიტაცა რა ინფორმაცია პროტოკოლის II ეტაპზე), მას შეუძლის დაშიფროს თავისი შეტყობინება და გადაუგზავნოს ბობს, ამასთან ბობი ვერ მიხვდება რომ ეს შეტყობინება არაა ალისასგან.
* თუ მელორიმ არ იცის გასაღები, მას შეუძლის ნებისმიერად დაშიფროს ან არც დაშიფროს თავისი შეტყობინება და გადაუგზავნოს ბობს, დეშიფრი­რებისას ბობი აბდაუბდას მიიღებს. ბობი კი ჩათვლის, რომ რახან შეტყო­ბინება ალისასგანაა, ჩათვლის, რომ ან ალისას, ან ქსელს სერიოზული პრობლემები აქვს.

სიმეტრიულ კრიპტოსისტემას აქვს შემდეგი პრობლემები:

* გასაღებების განაწილება უნდა ხდებოდეს საიდუმლოდ. ეს სერიოზული საკითხია. ხშირად გასაღებები კურიერს გადააქვს.
* თუ გასაღები კომპრომენტირებულია (მოპარულია, გაშიფრულია,მიღებულია წამებით ან მოქრთამვით), მაშინ ევას შეუძლია ამ გასაღებით დაშიფრული ყველა შეტყობიმების დეშიფრირება. მას ასევე შეუძლია ინფორმაციის გადა­ცემის ერთ-ერთ მხარედ გადაიქცეს და გაავრცელოს მცდარი შეტყობინებები.
* იმ დაშვებაში, რომ ყოველი წყვილი იყენებს განსხვავეულ გასაღებს, მაშინ მონაწილეთა რიცხვის გაზრდისას იზრდება გასაღებების რიცხვიც. ქსელი n მხარით საჭიროებს n(n-1)/2 გასაღებს. მაგალითად ქსელი 10 მონაწილით საჭიროება 45 სხვადასხვა გასაღებს, 100 მონაწილისთვის საჭიროა 4950 გასა­ღები. ეს კი ბევრია და იქმნება პრობლემა გასაღებების შექმნისა და მისი საიდუმლოდ შენახვისა. ამ პრობლემის გადაწყვეტა შესაძლებელია მხარეთა რაოდენობის შემცირებით, ეს კი ხშირად არასასურველია და შეუძლებელი.

განვიხილოთ დახურული გასაღებით შეტყობინების გადაცემა. ვთქვათ ალისა გა­დასცემს ბობს შეტყობიმებას ღია არხით, მაგრამ მას უსმენს ევაც. სეანსის დაწყების წინ ალისამ და ბობმა დახურული არხით ერთმანებს გადასცეს გასაღები (დავუშვათ საკურიერო მომსახურეობით) ან მათ წინასწარ იცოდნენ ეს გასაღები.

რადგანაც დაშიფრვა უძველეს დროს წარმოიშვა, მოვიყვანოთ მაგალითი იმ გასაღე­ბისა რომლითაც სარგებლობდა **გაი იულიუს ცეზარი**. ამასთან ”გადმოვაქართუ­ლოდ” იგი. დავუშვათ იგზავნება ქართული ღია ტექსტი რომელშიც გამოიყენება 33 ასო, რომელიც გადავნომროთ:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 **ა** | 2 **ბ** | 3 **გ** | 4 **დ** | 5 **ე** | 6 **ვ** | 7 **ზ** | 8 **თ** | 9 **ი** | 10 **კ** | 11 **ლ** |
| 12 **მ** | 13 **ნ** | 14 **ო** | 15 **პ** | 16 **ჟ** | 17 **რ** | 18 **ს** | 19 **ტ** | 20 **უ** | 21 **ფ** | 22 **ქ** |
| 23 **ღ** | 24 **ყ** | 25 **შ** | 26 **ჩ** | 27 **ც** | 28 **ძ** | 29 **წ** | 30 **ჭ** | 31 **ხ** | 32 **ჯ** | 33 **ჰ** |

გაი იულიუს ცეზარი გასაგზავნ ტექსტში ყოველ ასოს ცვლიდა მესამე მომდევნო ასოთი და ასეთნაირად ღებულობდა შიფროტექსტს. ვნახოთ რა სახეს მიიღებს ასეთნაირად კოდირებული მისი სენტენცია - „**მოვედი, ვნახე, გავიმარჯვე**“. ამ შემთვევაში ასო „**მ**“(12) შეიცვლება მისგან სამი ერთეულით მარჯვნივ მდგომი „**პ**“(15) ასოთი - ღია ტექსტი გადაიქცევა ამდაგვარად შემდეგი სახის შიფროტექ­სტად (*კრიპტოგრამად*) - „**პრითზმ, იჟდათ, ვდიმპდუბით**“ . შემდგომში სხვა ისტორიული პირები თავიანთ ღია ტექსტს შიფრავდნენ 4, 5 და ა.შ., ასოთა გადაადგილებით. ამიტომ ასეთი ტიპის დაშიფრვა ჩავწეროდ ზოგადი სახით

**C=(M+K)mod33**  (2.1)

სადაც M და C - ასოთა ნომერია ანბანში, შესაბამისად ღია ტექსტსა და შიფროტექ­სტში, K - რომელიღაც მთელი რიცხვია, რომელიც შიფრის კოდია - გასაღები, გაი იულიუს ცეზარის შემთხვევაში K=3. ზოგადად **a mod b** არის **a** მთელი რიცხვის **b** მთელ რიცხვზე გაყოფის ნაშთი, ამასთან ნაშთი აიღება სიმრავლიდან {0,1,2,3,...b-1}. მაგალითად - 13 **mod** 5 = 3. იმისათვის რომ მოვახდინოთ დეშიფრირება, უნდა გამოვიყენოთ პირუკუ ალგორითმი

**M =(C -K)mod33**  (2.2)

განვიხილოთ შემთხვევა, როცა ევა აწარმოებს კრიპტოანალიზს. დატჩმან ა. კერკხოფ­სის კრიპტოანალიზის ძი­რითადი დებულების თანახმად - 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, ევას შეტევები დეშიფრირებისთვის - გატეხვისთვის, მიმართულია გასაღების - შიფრის კოდის გასაგებად.

განვიხილოთ ღია ტექსტი (სიტყვა)-„**გასაღები**“, კეისრის კოდირებით მივი­ღებთ შიფროტექსტს - „**ვდფდჩთემ**“. რა შეიძლება მოიმოქმედოს ევამ, რომ გატეხოს გასაღები - ყველაზე მარტივია გადაარჩიოს გასაღების ყველა შესაძ­ლებელი ვარიანტები და მიღებული შედეგების ანალიზის საშუალებით დაადგინოს ღია ტექსტი ( ამ მეთოდს **„უხეში ძალა“** ეწოდება - **brute-force attack**); განვიხილოთ ეს ვარიანტები ცხრილში:

ცხრილი 1. სიტყვა „**ვდფდჩთემ“** -ის დეშიფრირება გასაღებების გადარჩევით

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| K | M |  | K | M |
| 1 | ეგუგშ |  | 18 |  |
| 2 | დბტ |  | 19 |  |
| 3 | გასაღები |  | 20 |  |
| 4 | ბჰრ |  | 21 |  |
| 5 |  |  | 22 |  |
| 6 |  |  | 23 |  |
| 7 |  |  | 24 |  |
| 8 |  |  | 25 |  |
| 9 |  |  | 26 |  |
| 10 |  |  | 27 |  |
| 11 |  |  | 28 |  |
| 12 |  |  | 29 |  |
| 13 |  |  | 30 |  |
| 14 |  |  | 31 |  |
| 15 |  |  | 32 |  |
| 16 |  |  | 33 |  |
| 17 |  |  |  |  |

როგორც ცხრილია 1 -დან ჩანს, რომ გამოყენებულ იქნა გასაღები K=3 და დაშიფრუ­ლია სიტყვა ”გასაღები”, ამასთან იმისთვის რონ ფასაღების სხვა მნიშვნელობები შეგვემოწმებინა, ჩვენ არ დაგვჭირდა ყველა- რვავე ასოს დეშიფრირება, რადგანაც უმეტეს შემთხვევაში - პირველი-ორო ასოს დეშიფრირების ანალიზისას, ეს გასაღე­ბი გამოირიცხებოდა, რადგანაც ქართულ სიტყვათა მარაგში ასეთი დასაწყისის მქონე სიტყვები არ არსებობს.

ამ მაგალითიდან ჩანს, რომ განხილული შიფრი სრულიად არამდგრადია: მისი გა­ტეხვისთვის საკმარისია გავაანალიზოთ შეტყობინების პირველი რამდენიმე ასო, რის შემდეგადაც დაშიფრვის გასაღები K ცალსახად განისაზღვრება - ანუ ცალსა­ხადაც მოხდება ღია ტექსტის აღდგენა.

რა არის განხილული შიფრის არამდგრადობის მიზეზე და როგორ შეიძლება მისი მდგრადობის ამაღლება? ამისთვის, და შედარებითი ანალიზის ჩასატარებლად გან­ვიხილოთ კიდევ ერთი მაგალითი: ვთქვათ ალისამ შემნახველ საკანში შეინახა მნიშვნელოვანი დოკუმენტები; შემნახველ საკანს აქვს ხუთდეკადიანი (ხუთი პო­ზიცია, თითოეულს 10 (ვთქვათ - ციფრები) სხვადასხვა შესაძლო მნიშვნელობით) კოდირებული გასაღები. ალისას სურს ბობს მიაწოდოს ციფრების ეს კომბინაცია, რომელიც შემნახველ საკანს გააღებს. ალისამ გამოიყენა ცეზარის დაშიფრვის ანალოგი იმ ანბანის მიმართ, რომელიც 10 ციფრისგან შესდგება:

**C=(M+K)mod10**  (2.3)

ვთქვათ ალისამ გაუგზავნა ბობს შიფროტექსტი 97531. ევა ცდილობს მის გაშიფ­რვას, ამისთვის ის მიმდევრობით იყენებს შიფრის ყველა შესაძლო მნიშვნელობას. ევამ შედეგად მიიღო შემდეგი ცხრილი 2.

**ცხრილი 2. 97531 შეტყობინების დეშიფრირება უხეში ძალით**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| k | m |  | k | m |
| 1 | 86420 |  | 6 | 31975 |
| 2 | 75319 |  | 7 | 20864 |
| 3 | 64208 |  | 8 | 19753 |
| 4 | 53197 |  | 9 | 08642 |
| 5 | 42086 |  | 0 | 97531 |

მიღებული შედეგები ტოლფასოვანია და რომელიმე მათგანის ღია ტექსტად მიჩ­ნევა შეუძლებელია, ანუ გასაღებ ცალსახად ვერ მოიძებნა. მანამ სანამ ევა შიფრო­ტექსტს მიიტაცებდა, მას შეეძლო ცალ-ცალკე განეხილა ერთ ერთი კოდი 105 შესა­ძლო კომბინაციებიდან. შიფროტექსტის მიტაცების შემდეგ კი კომბინაციების რაო­დენობა შემცირდა 10-მდე. ამ კონკრატულა შემთხვევაში გასაღებებს სულ 10 მნიშ­ვნელობა შეიძლება ჰქონდეს და ამიტომაა, რომ ალისა და ბობი ძლიერ გასა­იდუმლოებას არც ელოდებიან.

ეხლა შევადაროთ მოყვანილი ორი მაგალითი. პირველ შემთხვევაში ტექსტი ქარ­თულ ენაზეა და ამიტომ ის ექვემდებარება მრავალ წესს: სხვადასხვა ასოს, მათ კომპინაციებს აქვთ სხვადასხვა ალბათობები (ზოგჯერ ნულის ტოლიც კი); ამ წე­სებს - თვისებეს ეწოდობება ტექსტის სიჭარბე. სწორედ ამის გამო მოხდა გასაღე­ბის შედარებით ადვილი გატეხვა. მეორე მაგალითში კი ყველა შეაძლო ვარიანტი თა­ნაბრად ალბათურია და გასაღების გატეხვა ვერ ხერხდება - ანუ კოდური გასაღების ენა არ შეიცავს სიჭარბეს (ინფორმაციულ სიჭარბეს). კლოდ შენონმა, ამერიკელმა მეცნიერმა, თავის ნაშრომში - ”კავშირის თეორია საიდუმლო სისტემებში”( იხ. К.**Шеннон** **РАБОТЫ** **ПО** **ТЕОРИИ** **ИНФОРМАЦИИ** **И** **КИБЕРНЕТИКЕ,** ИЗДАТЕЛЬ­СТВО ИНОСТРАННОЙ ЛИТЕРАТУРЫ, Москва, 1963 ან ორიგინალში Claude Shannon "[Communication Theory of Secrecy Systems](http://en.wikipedia.org/wiki/Communication_Theory_of_Secrecy_Systems)" <http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf> ) შემოთავაზებულია სიჭარბის გაზომვის რაოდენობრივი მახასიათებელი და მისი გამოთვლა.

მოყვანილ მაგალითებში საქმე გვაქვს გატეხვასთან მხოლოდ შიფროტექსტის გამო­ყენებით. მაგრამ ზოგჯერ შესაძლებელია გატეხვა ჩატარდეს ცნობილი ღია ტექსტის საშუალებითაც (*გატეხვა ღია ტექსტის გამოყენებით).* ამ შემთხვევაში ევა შეადარებს რა წყვილს ”ღია ტექსტი - შიფროტექსტი”, ეცდება იპოვოს გასაღები, რითაც მერე ის ყველა შიფროტექსტს გატეხავს, რომელსაც ალისა მიაწვდის ბობს.

ზოგჯერ შესაძლებელია უფრო სერიოზული შეტევის განხორციელება კრიპტოსის­ტემაზე, როცა ვთქვათ ევას აქვს საშუალება თავად შეადგინოს ღია ტექსტები და მიიღოს მათი შესატყვისი შიფროტექსტები, და მათი მეშვეობით ეცდება გასაღების გარეხვა. ასე მაგალითად მეორე მსოფლიო ომის დროს ამერიკელებმა მოისყიდეს დაცვა და იაპონიის საელჩოდან ორი დღით მოიპარეს დაშიფრვის მანქანა. ამდენად მათ ჰქონდათ საშუალება ამ მანქანისათვის მიეწოდებინათ რამდენიმე ღია ტექსტი, შემდეგ მიეღოთ შესაბამისი შიფროტექსტები. (არ მოხდა ამ დაშიფრვის მანქანის დაშლა, რათა არ გამჟღავნებულიყო მანქანის გატაცება და არ მომხდარიყო გასაღე­ბების შეცვალა)

ეხლა დავუბრუნდეთ თემას, თუ როგორ შეიძლება კეისრის დაშიფრვის ალგორით­მის მდგრადობის ამაღლება. პირველი რაც მოიაზრება - ეს გასაღებების შესაძლო მნიშვნელობების, ანუ რაოდენობის გაზრდა. მაგალითად ვთქვათ ღია ტექსტში ყო­ველ ასოს შევუსაბამოთ თავისი გასაღები, კერძოთ თუ კი ვიტყვით, რომ ყოველ ასოს, რომელსაც აქვს კენტი ნომერი მიესადაგოს გასაღები k1 , ხოლო ლუწ პოზიცი­აზე მყოფ ასოს – k2 . მაშინ საიდუმლო გასაღები K=(k1, k2) შეადგება ორი რიცხვის­გან და შესაძლო გასაღებების რაოდენობა იქნება 332= 1089. ეხლა თუ გამოვიყენებთ პირველ მაგალითში გასაღებს K= (3,1) -ს , მივიღებთ:

”**გასაღები**” (3,1) ”**ვდტდჩთგმ**” (2.4)

ეს მეთოდი შეიძლება განვაზოგადოდ გასაღების ნებისმიერ სიგრძეზე K=(k1,k2,k3,…., kn). როცა n=10, გასაღებების სრული გადარჩევა - ანუ უხეში ძალის მეთოდი აზრს კარგავს, რადგანაც 3310= 1 531 578 985 264 449 ≈ 1,5х1015 შესაძლო კომბინაციაა განსახილველი.

მაგრამ მიუხედავად ასეთი დიდი რაოდენობის კომბინაციებისა, სიჭარბის არსე­ბობის შემთხვევაში შესაძლებელია ამ გასაღების გატეხვაც, ასე მაგალითად თუ გამოვიყენებთ ქართული ანბანის ასოთა სიხშირულ მახასიათებელს, ანუ რომელო ასო რა სიხშირით გამოიყენება ქართულ სიტყვაში, ”ი”ასოს განსაკუთრებული პო­ზიცია სიტყვის ბოლოს და ა.შ. ამდენად სიფროტექსტის **ვდტდჩთგმ** -ისბოლო ასო ”მ”, დიდის ალბათობით არის ”ი”-ს დაშიფრვა. რადგან ”ი” კენტია, ხოლო ”ი” -ს და ”მ”-ის რიგითი მნიშვნელობაა 9 და 12 შესაბამისად , ფორმულიდან M =(C – k1)mod33, სადაც M = 9; C=12 9=(12- k1) mod33; k1=(12-9) mod33=3

მივმართოდ ეხლა ასოთა სიხშირულ გამოყენებას. ეყველაზე ხშირად ქართულ სიტყვებში ფგამოიყენება ასო ”ა”. ჩავთვალოდ ეხლა, რომ შიფროტექსტში ყველაზე ხშირად გამოყენებული ასო ”დ” არის ”ა”-ს დაშიფრვა, რადგანაც ”ა”-ს კენტი ნომერო აქვს აქაც ვრწმუნდებით რომ, k1=3; მივუსადაგოთ ეხლა კროკტოანალიზისთვის k1 -ის ეს მნიშვნელობა და ვიპოვოტ ღია ტექსტი, ვღებულობთ ” გაჟაღეჰი”. ამდენად ცალცასხად k2-ის პოვნა ვერ ხერხდება, მაგრამ ამ შემთხვევაში შეიძლება უხეში ძა­ლით ვიპივოთ ყველა შესაძლო ვარიანტები ამ შესაძლო (3,1), (3,2), .... (3,32),(3,33) გასაღებებისთვის.

შევნიშნოთ, რომ ჩვენ დაშიფრვას ვახდენდით ანბანში კენტ და ლუწ ადგილას გან­ლაგებილი ასოების მიხედვით. შესაძლებელია ასევე თავად შეტყობინებაში კენტ და ლუწ ადგილეზე მყოფი ასოების ცალ-ცალკე დაშიფრვა - ამ შემთხვევაში იმავე K= (3,1) გასაღებით სიტყვა ”**გასაღები**” დაიშიფრება ”**ვბფბჩვგმ**” , ამ შემთხვევაში ადვილად იქნება ნაპოვნი უკვე k2, ხოლო k1 -ის პოვნა უხეში ძალითაა შესაძლებელი.

ეხლა ვეცადოთ გავართულოთ კრიპტოანალიზისთვის ასოთა სიხშირის გამოყენება. ამისთვის შევაწყვილოს ასოები შეტყობინებაში - ღია ტექსტში, ავრიოთ ისინი და ასეთნაირად დავმალოთ მათი გამოჩენის ინდივიდუალური მახასიათებლები. ისევ გამოვიყენოთ გასაღები K=(k1, k2) და ვიტყვით რომ ისინი შეტყობინებაში ასოების რიგითობის (კენტი-ლუწის) მიხედვით გამოიყენება. დაშიფრვას კი მოვახდენთ ბლოკების მიხედვით - ორ-ორი სიმბოლოთი mi, mi+1 (ასოთი) , მაგალითად ასეთი:

M1=m1+m2 ,

M2=m2+M1 ,

c1= M1+ k1,

c2= M2+ k2,

M3=m3+m4 ,

M4=m4+M3 ,

c3= M3+ k1,

c4= M4+ k2,

……….

………..

Mi=mi+mi+1 ,

Mi+1=mi+1+Mi ,

ci= Mi+ k1,

ci+1= Mi+1+ k2, (mod 33) (2.4)

სადაც mi - შეტყობინებაში (ღია ტექსტში) კენტ პოზიციაზე მყოფი ასოა, mi+1 - ლუწ­ზე. ci და ci+1 შიფროტექსტის ასოებია, k1=3; k2=1.

დეშიფრაცია ხდება პირუკუ ალგორითმით:

Mi= ci - k1+mi+1 ,

Mi+1= ci+1 - k2, +Mi ,

mi = Mi -mi+1,

mi+1= Mi+1 - Mi (mod 33) (2.5)

ვნახოთ როგორ შეიცვლება ”გასაღები” დაშიფრვის ამ ალგორითმით

M1=გ(3)+ა(1)=დ(4) ,

M2=ა(1)+დ(4)=ე(5) ,

c1= დ(4) + 3= ზ(7),

c2= ე(5) + 1= ვ(6),

M3=ს(18)+ა(1)=ტ(19) ,

M4=ა(1)+ტ(19)=უ(20) ,

c3= ტ(19)+ 3=ქ(22),

c4= უ(20) + 1= ფ(21),

M5=m5+m6 = ღ(23)+ე(5)= ძ(28),

M6=m6+M5 =ე(5)+ ძ(28)=ჰ(33),

c5= M5+ k1= ძ(28)+3=ხ(31) ,

c6= M6+ k2=ჰ(33)+1=ა(1),

M7=m7+m8 =ბ(2)+ი(9)=ლ(11),

M8=m8+M7 = ი(9)+ლ(11)=უ(20),

c7= M7+ k1=ლ(11)+3=ო(14),

c8= M8+ k2=უ(20)+1=ფ(21),

შუალედური გარდაქმნა ”გასაღები” -ს დაშიფრავს ” დეტუძჰლუ” შიფროტექსტად, ხოლო შემდეგ მას გარდაქმნის საბოლოო ”ზვქფხაოფ” შიფროტექსტად

**გასაღები** **დეტუძჰლუ** **ზვქფხაოფ** (2.6)

კეისრის შიფრის გატეხვა ღია ტექსტის პირობებში ევასთვის პრობლემას არ წარმო­ადგენს - კერძოდ როცა K= (3,1) და ევას აქვს წყვილი (”**გასაღები**” ,”**ვბფბჩვგმ**”) მაშინ იგი მარტივად გამოთვლის გასაღებს k1=ვ(6)-გ(3)=3; k2=ბ(2)-ა(1)=1.

მაგრამ თუ კი გამოვიყენებთ დაშიფრვის (2.4) ალგორითმს მაშინ წყვილი (”**გასაღე­ბი**”, ”**ზვქფხაოფ”**) არ იძლევა უშუალოდ გამოთვალო გასაღები, მაგრამ თუ კი ევა გამოიყენებს (2.4) ალგორითმის პირველ-ორ ოპერაციას, მაშინ ის მიიღებს წყვილს (”**დეტუძჰლუ**” , ”**ზვქფხაოფ**”) და უკვე ამისთვის იპოვნის გასაღებს.

ამ შემთხვევაში როგორ გავურთულოთ ევას კრიპტოანალიზის ჩატარების საშუალე­ბა? იდეა იმაში მდგომარეობს, რომ ორჯერ ჩავატაროთ (2.4) ალგორითმის - შიფრის გამოყენება - მაშინ მივიღებთ

**გასაღები** **ზვქფხაოფ**  **ჟუნჯბაღყ** (2.7)

ამდენად, როცა ევას აქვს წყვილი (**გასაღები,ჟუნჯბაღყ**) მას გაუჭირდება გასაღების გატეხვა, რადგან დაშიფრვის ალგორითმი არაა ცხადი ( მან არ იცის როგორ მიიღოს შუალედური მნიშვნელობა - **ზვქფხაოფ**, რადგან გამოყენებული იქნა მისთვის უცნობი საიდუმლო დასაღები.

(2.7) სქემაში (2.4) ალგორითმის ცალკეულ რეალიზაციას სიფრის რაუნდი ან ციკლი ეწოდება. რეალურ შიფრებში გამოიყენება ანალოგიური პროცედურები: გარდაქმნა სიმბოლოების უფრო დიდი სიგრძის ჯაჭვზე, უდრო დიდი სიგრძის გასაღებით, დიდი ბლოკებითა და რაუნდების რაოდენობით - ყველაფერი ეს კი ზრდის ალგო­რითმის მდგრადობას.