კრიპტოლოგია. ქვიზი № 2

1. **რა არის კრიპტოგრაფიული პროტოკოლი :**

ა) აუთენტიფიკაციის და გასაღების გაცვლის მექანიზმები;

ბ) ის რაც სიმეტრიულ შიფრაციისას უზრუნველყოფს მონაცემების გაცვლას პროგრამულ დონეზე;

გ) მოქმედებათა თანამიმდევრობა, რომელსაც მისდევს და ახორ­ციელებს ორი ან მეტი მხარე (ინგ. Party), რომელთაც სურთ გარკვეული ამოცანის გადაწყვეტა;

დ) ინფორმაციის უსაფრთხო გადაცემის ISO-ში დამტკიცებული წესი.

**2. პროტოკოლის ქვემოთ მოყვანილი მახასიათებლებიდან რომელია ზედმეტი:**

ა) პროტოკოლი უნდა იყოს სრული, ყოველ შესაძლო სიტუაციას უნდა შეესა­ბამებოდეს ცალსახად განსაზღვრული ქმედება;

ბ) პროტოკოლი უნდა იყოს არაწინააღმეგობრივი, ყოველი მოქმედება უნდა იყოს ისე გაწერილი და შესრულებული, რომ არ ტოვებდეს გაუგებრობებს

გ) პროტოკოლის ყოველი მხარე უნდა თანხმებოდეს პროტოკოლის დაცვაზე;

დ) პროტოკოლის ყოველმა მხარემ უნდა იცოდეს პროტოკოლი და მისი შემად­გენელი ნაწილები - თანამიმდევრული ქმედებები.

ე) არცერთი; ვ) ყველა; ზ) ”ბ” და ”დ”.

**3. ვინ არ წარმოადგენს პროტოკოლის მხარეს:**

ა) ბობი; ბ) ალისა; გ) გედევანი; დ) მელორი.

**4. მოცემულია სიმეტრიული კრიპტოგრაფიის გამოყენებით ინფორმაციის** გადაცემის პროტოკოლი არეული თანამიმდევრობით, დაალაგეთ მოქმედებათა ნუმერაცია:

I. ალისა და ბობი ირჩევენ გასაღებს;

II. ალისა და ბობი ირჩევენ დაშიფრვის სისტემას;

III. ალისა უგზავნის დაშიფრულ შეტყობინებას (შიფროტექსტს) ბობს;

IV. ალისა შიფრავს თავისი შეტყობინების ღია ტექსტს დაშიფრვის ალგორითმისა და გასაღების მეშვეობით;

V. ბობი ახდენს შიფროტექსტის დეშიფრირებას დაშიფრვის ალგორითმისა და გასაღების მეშვეობით რის შედეგადაც იღებს ღია ტექსტს.

ა) I-III-II-V-IV; ბ) III-V-I-IV;

გ) II-I-IV-III-V; დ) V-I-II-IV-III.

5. **K -ს რა მნიშვნელობისთვის დაშიფრვა** **C=(M+K)mod33 -ს ეწოდება გაი იულიუსის კოდი; სადაც** სადაც M და C - ასოთა ნომერია ანბანში, შესაბამისად ღია ტექსტსა და შიფროტექ­სტში, K - რომელიღაც მთელი რიცხვია, რომელიც შიფრის კოდია - გასაღებიobisTvis დეშიფრირება ეს არის:

ა) 1; ბ) 2; გ) 3; დ) 4.

6. **მოცემულია**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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** |

და შიფროტექსტი „**ვდფდჩთემ**“, აღადგინეთ ღია ტექსტი დეშიფრირების **M =(C -K)mod33**  ალგორითმით, სადაც **K =5:**

ა) აჯჟჯუდჰი; ბ) აჯჟჯფგჰთ;

გ) აჟჯჟფგჰთ; დ) აჟჯჟუგათ.

**7. გასაღების გატეხვას - ყველა შესაძ­ლებელი ვარიანტების გადაარჩევით, ეწოდება:**

ა) ძლიერი ძალა (ძძ); ბ) ლომის ძალა;

გ) უხეში ქმედება; დ) უხეში ძალა.

8. **გ.ი. ცეზარის შიფრი:**

ა) ნაწილობრივ მდგრადია; ბ) სრულიად არამდგრადია;

გ) მდგრადია; დ) არამდგრადია.

**9. რის გამო ხდება გასაღე­ბის გატეხვა შედარებით ადვილი:**

ა) ტექსტის სიჭარბის; ბ) ტექსტის სიჭრელის;

გ) ტექსტია სიმარტივის; დ) ტექნიკური ტექსტის.

**10. როგორ შეიძლება კეისრის დაშიფრვის ალგორით­მის გართულება - მდგრადობის ამაღლება გატეხვის წინააღმდეგ:**

ა) გასაღების მნიშვნელობის k=3-ის 11 -ით შეცვლით;

ბ) გასაღების მნიშვნელობის k=3-ის 33 -ით შეცვლით

გ) ასეთი მეთოდი არ არსებობს;

დ) გასაღებების შესაძლო მნიშვნელობების რაოდენობის გაზრდა.

11. ღია ტექსტიდან - ”**გასაღები**” მიღებულია შიფროტექსტი ”**ვდტდჩთგმ**”, რისი ტოლია K=(k1, k2)**:**

ა) (1,3) ; ბ) (3,1) ; გ) (4,2) ; დ) (5,1) .

**12.** **კრიპტოანალიზისთვის ასოთა სიხშირის გამოყენებისგან თავის აცილებისთვის ხმარობენ:**

ა) სტოქასტურ დაშიფრვას პანელის მიხედვით;

ბ) დაშიფრვას პანელის მიხედვით;

გ) დაშიფრვას ბლოკების მიხედვით;

დ) სტოქასტურ დაშიფრვას შენონის მიხედვით.

**13.** **ალგორითმის ცალკეულ რეალიზაციას ეწოდება:**

ა) ტაიმი; ბ) სეტი; გ) პაკეტი; დ) რაუნდი.

**14. რა არ ზრდის ალგო­რითმის მდგრადობას:**

ა) ბლოკების გაზრდა; ბ) მონაწილეთა რაოდენობის გაზრდა;

გ) გასაღების სიგრძის გაზრდა; დ) რაუნდების რაოდენობის გაზრდა.

**15.** შიფროტექსტია - 97531 , ალგორითმი - **C=(M+K)mod10 , სადაც C,M,K - ციფრებია, ქვემოთ მოყვანილი ხუთნიშნა რიცხვებიდან, რომელი არ შეიძლება იყოს ღია ტექსტი :**

ა) 75319; ბ) 19753; გ) 42086; დ) 21531.