კრიპტოლოგია. ქვიზი № 1

1. **რას ეწოდება ინფორმაციის უსაფრთხო გადაცემა :**

ა) ევა ვერ მიიტაცებს ალისასგან ბობისთვის გაგზავნილ შეტყობინებას;

ბ) ევა მიიტაცებს ალისასგან ბობისთვის გაგზავნილი შეტყობინებას ნაწილს;

გ) შეტყობინების მიმტაცებელი (ევა), ვერ ჩაწვდება მიტაცებული შეტყობინ­ების არსს;

დ) ინფორმაციის უსაფრთხო გადაცემა არ არსებობს.

**2. საწყის შეტყობინებას, რომლის გადაცემაც სურთ, ეწოდება:**

ა) ფაილი; ბ) ღია ტექსტი;

გ) საიდუმლო ტექსტი; დ) დასაშიფრი ტექსტი.

**3. ზოგადად დაშიფრვა ეწოდება:**

ა) შეტყობინების ფორმის, მისი სახის ცვლილებას;

ბ) შეტყობინების ფორმის გადაყვანას ორობით კოდში;

გ) შეტყობინების ფორმის შეცვლას ”ენიგმით”;

დ) ყველა სწორია.

4. დაშიფრვის შედეგად ვღებულობთ;

ა) შიფრატორს; ბ) საიდუმლო კოდს;

გ) შიფროტექსტს; დ) შიფროფაილს.

5. დეშიფრირება ეს არის:

ა) საიდუმლო ტექსტის გარდაქმნა ღია ტექსტად;

ბ) შიფროტექსტის გარდაქმნა ღია ტექსტად;

გ) შიფროფაილის გარდაქმნა ღია ტექსტად;

დ) დასაშიფრი ტექსტის გარდაქმნა საიდუმლო კოდში.

6. **უსაფრთხო შეტყობინებების ხელოვნებასა და მეცნიერებას ეწოდება**:

ა) კრიპტოლოგია; ბ) კრიპტოანალიზი;

გ) კრიპტოსპექტრი; დ) კრიპტოგრაფია.

 7. **შიფროტექსტების „გატეხვის“ ხელოვნებასა და მეცნიერებას** **ეწოდება**:

ა) კრიპტოლოგია; ბ) კრიპტოანალიზი;

გ) კრიპტოსპექტრი; დ) კრიპტოგრაფია.

8. **უსაფრთხო შეტყობინებების და შიფროტექსტების „გატეხვის“ ხელოვნებასა და მეცნიერებას** **ეწოდება**:

ა) კრიპტოლოგია; ბ) კრიპტოანალიზი;

გ) კრიპტოსპექტრი; დ) კრიპტოგრაფია.

**9. ინგლისურ ლიტერატურაში მიღებულია გამო­ყე­ნებულ იქნას ტერმინი დაშიფრვა - დეშიფრებ-ის აღსანიშნავათ:**

ა). encrypt – decrypt; ბ) encrypt – decipher;

გ) encipher - decipher; დ) encipher - decipher

10**. რას მიშნავს E(M)=C მათემატიკური ჩანაწერი კრიპტოლოგიაში:**

ა) აინშტაინის მასისა და ენერგიის E=MC2 ფორმულის ანალოგს;

ბ) დაშიფრვის ფუნქციის მოქმედებას;

გ) დეშიფრირების ფუნქციის მოქმედებას;

დ) არაფერს.

11. **რას მიშნავს D(C)=M მათემატიკური ჩანაწერი კრიპტოლოგიაში:**

ა) აინშტაინის მასისა და ენერგიის E=MC2 ფორმულის ანალოგს;

ბ) დაშიფრვის ფუნქციის მოქმედებას;

გ) დეშიფრირების ფუნქციის მოქმედებას;

დ) არაფერს.

**12.** **შეტყობინებათა კონფიდენციალობის გარდა კრიპტოგრაფია არ გამოიყენება შემდეგი დანიშნულებებისთვის**:

ა) ორიგინალობის შესამოწმებლად; ბ) მთლიანობის შესამოწმებლად;

გ) ავტორობის არაუარყოფობისთვის; დ) მოწყვლადობის შესაოწმებლად.

**13.** **რა არის კრიპტოგრაფიული ალგორითმი:**

ა) მანქანური კოდი; ბ) მათემატიკური ფუნქ­ცია;

გ) ტიურინგის მანქანა; დ) პროგრამმა ენა ბეისიკზე.

14. ***შეზღუდული* კრიპტოგრაფიული ალგორითმი დაფუძნებულია:**

ა) გასაღების საიდუმლოობაზე; ბ) მიმღების საიდუმლოობაზე;

გ) ალგორითმის საიდუმლოობაზე; დ) გამგზავნის საიდუმლოობაზე.

**15.** **თანამედროვე კრიპტოგრაფიაში უნივერსალური ალგორითმის პრობ­ლემის მოგვარება ხდება:**

ა) კავშირის არხის ფიზიკური გაუმჯობესებით:

ბ) გამგზავნის ტრენინგით; გ) მიმღების ტრენინგით;

დ) გასაღების საშუალებით.

**16. კრიპტოსისტემა ეს არის:**

ა) ყველა ქვემოთ ჩამოთვლილი; ბ) ღია ტექსტი და შიფროტექსტი;

გ) გასაღებები; დ)ალგორითმი.

**17. სიმეტრიული ან პირობითი ალგორითმების თვისებაა:**

ა) დაშიფრვის და დეშიფრირების გასაღებები დამოუკიდებელნი არიან;

ბ) დაშიფრვის და დეშიფრირების გასაღებები დამოკიდებელნი არიან;

გ) დაშიფრვის გასაღები არსებობს, დეშიფრირების არა;

დ) დეშიფრირების გასაღები არსებობს, დაშიფრვის არა.

**18**. **ალგორითმები საიდუმლო ან ერთი გასაღებით, ეს არის:**

ა) როცა დაშიფრვის გასაღები არსებობს, დეშიფრირების არა;

ბ) როცა დეშიფრირების გასაღები არსებობს, დაშიფრვის არა;

გ) როცა დაშიფრვის და დეშიფრირების გასაღები არ არსებობს;

დ) როცა დაშიფრვის და დეშიფრირების გასაღები ერთი და იგივეა.

**19. სიმეტრიული ალგორითმები არ იყოფიან შემდეგ კატეგორიად:**

ა) ნაკადური; ბ) ბლოკური; გ) ქსელური;

დ) ლოკალური; ე) ”ა” და ”ბ” ; ვ) ”გ” და ”დ”.

**20.** ა**სიმეტრიული ან ღია გასაღების ალგორითმების თვისებაა:**

ა) დაშიფრვის და დეშიფრირების გასაღებები დამოუკიდებელნი არიან;

ბ) დაშიფრვის და დეშიფრირების გასაღებები დამოკიდებელნი არიან;

გ) დაშიფრვის გასაღები არსებობს, დეშიფრირების არა;

დ) დეშიფრირების გასაღები არსებობს, დაშიფრვის არა.

**21. კრიპტოანალიზის მცდელობას ეწოდება**:

ა) კომპრომენტაცია; ბ) გატეხვა; გ) გახსნა; დ) დევალვაცია.

**22. კრიპტოანალიზის ძი­რითადი დებულებით, რომელიც ჩამოაყალიბა XIX საუკუნეში დატჩმან ა. კერკხოფ­სმა - უსაფრთხოება სრულად განისაზღვრება:**

ა) ალგორითმით; ბ) შიფროტექსტი;

გ) გასაღებით; დ)შეტყობინების ხასიათი.

**23. კრიპტოანალიტიკური გატეხვის რამდენი ძირითადი ტიპია:**

ა) 3; ბ) 4; გ) 5; ბ) 6;

**24. რას ნიშნავს** **გატეხვა მხოლოდ შიფროტექსტის გამოყენებით;**

ა) კრიპტოანალიტიკოს შეუძლია ამოარჩიოს არა მარტო დასაშიფრი ტექსტი, არამედ ამის მერე შეუძლია გააკეთოს მომდევნო არჩევანი დაშიფრვის შედეგად მიღებულ რეზულტატებზე დაყრდნობით.

ბ) 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

გ) 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.

დ) 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.

**25. რას ნიშნავს** **გატეხვა ღია ტექსტის გამოყენებით;**

ა) კრიპტოანალიტიკოს შეუძლია ამოარჩიოს არა მარტო დასაშიფრი ტექსტი, არამედ ამის მერე შეუძლია გააკეთოს მომდევნო არჩევანი დაშიფრვის შედეგად მიღებულ რეზულტატებზე დაყრდნობით.

ბ) 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

გ) 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.

დ) 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.

**26. რას ნიშნავს** **გატეხვა ამორჩეული ღია ტექსტის გამოყენებით.;**

ა) კრიპტოანალიტიკოს შეუძლია ამოარჩიოს არა მარტო დასაშიფრი ტექსტი, არამედ ამის მერე შეუძლია გააკეთოს მომდევნო არჩევანი დაშიფრვის შედეგად მიღებულ რეზულტატებზე დაყრდნობით;

ბ) 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;

გ) 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;

დ) 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.

27. **რას ნიშნავს** **ადაპტიური** **გატეხვა ღია ტექსტის გამოყენებით:**

ა) კრიპტოანალიტიკოს შეუძლია ამოარჩიოს არა მარტო დასაშიფრი ტექსტი, არამედ ამის მერე შეუძლია გააკეთოს მომდევნო არჩევანი დაშიფრვის შედეგად მიღებულ რეზულტატებზე დაყრდნობით;

ბ) 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;

გ) 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;

დ) 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.

**28. ალგორითმის უსაფრთხოების ხარისხი დამოკიდებულია:**

ა) ალგორითმის გატეხვის ფასი უფრო დიდია, ვიდრე დაშიფრული ინფორმაციის ფასი;

ბ) ალგორითმის გატეხვის დრო, მეტია იმ დროზე, რომლის განმავლობაშიც საჭიროა შეტყობინების საიდუმლოდ შენახვა;

გ) მონაცემთა რაოდენობა, რომელიც ერთი გასაღებითაა დაშიფრული ნაკლებია იმ მონაცემთა რაოდენობაზე, რომელიც საჭიროა ალგორითმის გატეხვაზე;

დ) ყველა ზემოთ ჩამოთვლილზე.

**29. ალგორითმების გატეხვის კატეგორია არ არის:**

ა) სრული გატეხვა; ბ) გლობალური დედუქცია;

გ) უხეში გატეხვა; დ) ლოკალური დედუქცია.

**30. გატეხვის სირთულე არ შეიძლება გაიზომოს შემდეგი საშუალებით:**

ა) მოთხოვნა ანბანზე; ბ) მონაცემთა სირთულე;

გ) დამუშავების სირთულე; დ) მოთხოვნა მეხსიერების მიმართ.