ფინალური 3 კრიპტოლოგია

**1. რამდენი გასაღები გვაქვს ღია გასაღებიან კრიპტოგრაფიაში:**

ა) 1; ბ) 2; გ) 3; დ) 4.

**2. ადვილად გამოთვლის ქვეშ შემდგომში ვიგულისხმებთ:**

ა) არ არსებობს *y* *f* (*x*) ფუნქციის გამოთვლის ექსპონტენციალური ალგორითმი;

ბ) არსებობს *y* *f* (*x*) ფუნქციის გამოთვლის ექსპონტენციალური ალგორითმი;

გ) არ არსებობს *y* *f* (*x*) ფუნქციის გამოთვლის პოლინომური ალგორითმი;

დ) არსებობს *y* *f* (*x*) ფუნქციის გამოთვლის პოლინომური ალგორითმი.

**3. ამოცანს, რომლის დროსაც მოცემულია *a* , *n* და *x* და უნდა ვიპოვოთ**

**ისეთი მთელი *m* (თუ ის არსებობს), რომ *x* *a m*(mod *n*), ეწოდება:**

ა) დისკრეტული ახარისრების ამოცანა ;

ბ) უწყვეტი ლოგარითმირების ამოცანა ;

გ) დისკრეტული ლოგარითმირების ამოცანა ;

დ) უწყვეტი ახარისხების ამოცანა.

**4. სინქრონიზებად ნაკადურ შიფრებს უწოდებენ:**

ა) დამშიფრავი და გამშიფრავი გამების სინქრონიზაციას;

ბ) დამშიფრავი და გამშიფრავი გენერატორების სინქრონიზაციას;

გ) ესეთი არ არსებობს;

დ) ა) და ბ).

**5. ზოგადად დაშიფრვა ეწოდება:**

ა) შეტყობინების ფორმის, მისი სახის ცვლილებას;

ბ) შეტყობინების ფორმის გადაყვანას ორობით კოდში;

გ) შეტყობინების ფორმის შეცვლას ”ენიგმით”;

დ) ყველა სწორია.

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

ა) კრიპტოლოგია; ბ) კრიპტოანალიზი;

გ) კრიპტოსპექტრი; დ) კრიპტოგრაფია.

7. **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.

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

ა) კავშირის არხის ფიზიკური გაუმჯობესებით:

ბ) გამგზავნის ტრენინგით; გ) მიმღების ტრენინგით;

დ) გასაღების საშუალებით.

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

ა) ნაკადური; ბ) ბლოკური; გ) ქსელური;

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

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

ა) 3; ბ) 4; გ) 5; ბ) 6;

 11. **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.

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

ა) მოთხოვნა ანბანზე; ბ) მონაცემთა სირთულე;

გ) დამუშავების სირთულე; დ) მოთხოვნა მეხსიერების მიმართ.

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

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

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

ა) ძლიერი ძალა (ძძ); ბ) ლომის ძალა;

გ) უხეში ქმედება; დ) უხეში ძალა.

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

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

16. 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.

17 . კომპიუტერული კრიპტოგრაფიის ალგორითმები მუშაობენ:

ა) ბიტებზე; ბ) 33 სიმბოლურ ანბანზე;

გ) 26 სიმბოლურ ანბანზე; დ) ბაიტებზე.

18. ცალხმოვანი (ომოფონური)ჩანაცვლებითი შიფრია:

ა) შიფრი, რომელიც ღია ტექსტის ყოველ სიმბოლოს ცვლის შიფროტექსტის შესაბამის სიმბოლოთი;

ბ) შიფრი, რომელის დროსაც 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;

გ) შიფრი, რომელის დროსაც [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;

დ) შიფრი, რომელის დროსაც ღია ტექსტის ყოველი სიმბოლო ჩაინაცვლება რამდრნიმედან რომელიმე ერთი კონკრეტული შიფრით.

19. მარტივ სვეტურ გადანაცვლებადი ( 6Х7) შიფრით ღია ტექსტი ”მზეო ამოდი ამოდი ნუ ეფარები გორასა” იცვლება შემდეგი რა სახის შიფროტექსტით:

ა) ”მოდფგ ზდიაო ეი რრ ო აუბს ამ ია მოე რეა ”;

ბ) ”მო ზდიაო დფგეი რრ ო რეა აუბს ამ ია მოე ”;

გ) ”მოდფგ ზდიაო ეი რრ ო რეა აუბს ამ ია მოე ”;

ს) ”იაო მოდფგ ზდეი რრ ო რეა აუბს ამ ია მოე ”.

20. რომელი არაა სწორი მარტივი XOR -სთვის

ა) 0 0=1 ; ბ) 0 1=1 ; გ) 1 0=1; დ) 1 1=0

21. რომელია კორექტული: შიფრი მედეგია (მდგრადია) (ამორჩეული ღია ტექსტის შეტევისადმი), თუ:

ა) მისთვის არ არსებობს გატეხვის ისეთი ალგორითმები, რომელიც უფრო სწრაფია, ვიდრე გასაღებთა სრული გადარჩევის გატეხვა;

ბ) მისთვის არსებობს გატეხვის ისეთი ალგორითმები, რომელიც უფრო სწრაფია, ვიდრე გასაღებთა სრული გადარჩევის გატეხვა;

გ) მისთვის არაა ცნობილი გატეხვის ისეთი ალგორითმები, რომელიც უფრო სწრაფია, ვიდრე გასაღებთა სრული გადარჩევის გატეხვა;

დ) მისთვის ცნობილი გატეხვის ისეთი ალგორითმები, რომელიც უფრო სწრაფია, ვიდრე გასაღებთა სრული გადარჩევის გატეხვა.

22. ფეისტელის ქსელზე დაფუძნებულია არ არის კრიპტოსისტემა:

ა) DES- (Data Encryption Standard); ბ) RSA;

გ) ГОСТ 28147-89; დ) Rijndael .

**23. როდესაც შეტყობინებას თქვენი პარტნიორის სახელით აგზავნის სრულიად სხვა პირი, მაშინ ამის გამოსარიცხად არა გამოიყენება:**

ა) ინფორმაციის იდენტიფიკაცია;

ბ) ავტორობის იდენტიფიკაციია;

გ) ავტორობის აუთენტიფიკაცია;

დ) ინფორმაციის მთლიანობა.

**24. ღია გასაღებიან კრიპტოგრაფიაში არასაიდუმლო (დეშიფრაციის) გასაღები ცნობილია:**

ა) ინფორმაციული ურთიერთობის ერთი სუბიექტისათვის;

ბ) ინფორმაციული ურთიერთობის ორი სუბიექტისათვის;

გ) ინფორმაციული ურთიერთობის არცერთი სუბიექტისათვის;

დ) ყველასთვის.

**25. თუ *a=c(mod p*) და *b=c(mod p*) მაშინ**

ა) *a≠b(mod p*); ბ) *a=b(mod p*); გ) *a>b(mod p*); დ) *a<b(mod p*);

**26. რომელია ბლუმის რიცხვები:**

ა) 5 და 9 ; ბ) 7 და 11; გ) 15 და 12; დ) 23 და 30.

27. **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.

28. 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.

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

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

გ) encipher - decipher; დ) encipher – decipher .

**30.** **რა არის კრიპტოგრაფიული ალგორითმი:**

ა) მანქანური კოდი; ბ) მათემატიკური ფუნქ­ცია;

გ) ტიურინგის მანქანა; დ) პროგრამმა ენა ბეისიკზე.

**31. 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.

**32. კრიპტოანალიზის მცდელობას ეწოდება**:

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

**33. 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.

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

ა) სრული გატეხვა; ბ) უხეში გატეხვა;

გ) გლობალური დედუქცია; დ) ლოკალური დედუქცია.

35. **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.

36. **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.

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

ა) ტექსტის სიჭარბის; ბ) ტექსტის სიჭრელის;

გ) ტექსტია სიმარტივის; დ) ტექნიკური ტექსტის.

**38.** **ალგორითმის ცალკეულ რეალიზაციას ეწოდება:**

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

**39. კომპიუტერული კრიპტოგრაფიის წარმოშობამდე კრიპტოგრაფია წარმოადგენდა:**

ა) ფსევდომეცნიერებას; ბ) ალგორითმს ნებისმიერ სიმბოლურ საფუძველზე;

გ) არ არსებობდა დ) ალგორითმს რიცხვით საფუძველზე.

**40. თუ შიფრში იცვლება არა ღია ტექსტი, არამედ სიმბოლოების რიგითობა, მას ეწოდება:**

ა) გადანაცვლებადი შიფრში; ბ) წანაცვლებითი შიფრში;

გ) შენაცვლებითი შიფრში; დ) ჩანაცვლებითი შიფრში.