ფინალური 4 კრიპტოლოგია

1. ღია გასაღებიან კრიპტოგრაფიაში საიდუმლო (დეშიფრაციის) გასაღები ცნობილია:

ა) ინფორმაციული ურთიერთობის ერთი სუბიექტისათვის;

ბ) ინფორმაციული ურთიერთობის ორი სუბიექტისათვის;

გ) ინფორმაციული ურთიერთობის არცერთი სუბიექტისათვის;

დ) ყველასთვის.

2. *a=b(mod p*) ნიშნავს;

ა) *a=b*x*p* ბ) *a*x*b=p* ; გ) *a:b=p* ; დ) *a%p=b%p* % - გაყოფა ნაშთით .

3. ცალმხრივ მიმართული ხაფანგიანი ფუნქცია ეწოდება:

ა) ისეთ *f k* : *X* *Y*ფუნქციას, რომლისთვისაც ისევე, როგორც ცალმხრივ მიმართული ფუნქციისთვის ცნობილი *x* -თვის ადვილია *y*  *f k*(*x*) გამოთვლა. რაც შეეხება მოცემული *y* -თვის ისეთი *x* -ის პოვნას, რომ დაკმაყოფილდეს *y*  *f k*(*x*) ტოლობას, ეს უკვე დამოკიდებულია საიდუმლო პარამეტრის ცოდნაზე;

ბ) ისეთ *f k* : *X* *Y*ფუნქციას, რომლისთვისაც ისევე, როგორც ცალმხრივ მიმართული ფუნქციისთვის ცნობილი *x* -თვის ადვილია *y*  *f k*(*x*) გამოთვლა. რაც შეეხება მოცემული *y* -თვის ისეთი *x* -ის პოვნას, რომ დაკმაყოფილდეს *y*  *f k*(*x*) ტოლობას, ეს უკვე დამოკიდებულია არაა საიდუმლო პარამეტრის ცოდნაზე;

გ) ისეთ *f k* : *X* *Y*ფუნქციას, რომლისთვისაც ისევე, როგორც ცალმხრივ მიმართული ფუნქციისთვის ცნობილი *x* -თვის რთულია *y*  *f k*(*x*) გამოთვლა. რაც შეეხება მოცემული *y* -თვის ისეთი *x* -ის პოვნას, რომ დაკმაყოფილდეს *y*  *f k*(*x*) ტოლობას, ეს უკვე დამოკიდებულია საიდუმლო პარამეტრის ცოდნაზე;

დ) ისეთ *f k* : *X* *Y*ფუნქციას, რომლისთვისაც ისევე, როგორც ცალმხრივ მიმართული ფუნქციისთვის ცნობილი *x* -თვის ადვილია *y*  *f k*(*x*) გამოთვლა. რაც შეეხება მოცემული *y* -თვის ისეთი *x* -ის პოვნას, რომ დაკმაყოფილდეს *y> f k*(*x*) უტოლობა, ეს უკვე დამოკიდებულია საიდუმლო პარამეტრის ცოდნაზე.

4. კრიპტომედეგობის რაოდენობრივი შეფასების კრიტერიუმი არა:

ა) ინფორმაციის რაოდენობა; ბ) დრო; გ) მეხსიერება; დ) სიჩქარე.

5. დაშიფრვის შედეგად ვღებულობთ;

ა) შიფრატორს; ბ) საიდუმლო კოდს;

გ) შიფროტექსტს; დ) შიფროფაილს.

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

ა) კრიპტოლოგია; ბ) კრიპტოანალიზი;

გ) კრიპტოსპექტრი; დ) კრიპტოგრაფია.

7. შეტყობინებათა კონფიდენციალობის გარდა კრიპტოგრაფია არ გამოიყენება შემდეგი დანიშნულებებისთვის:

ა) ორიგინალობის შესამოწმებლად; ბ) მთლიანობის შესამოწმებლად;

გ) ავტორობის არაუარყოფობისთვის; დ) მოწყვლადობის შესაოწმებლად.

8. კრიპტოსისტემა ეს არის:

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

გ) გასაღებები; დ)ალგორითმი.

9. ასიმეტრიული 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.

10. 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.

11. 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.

12. 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.

13. გ.ი. ცეზარის შიფრი:

ა) ნაწილობრივ მდგრადია; ბ) სრულიად არამდგრადია;

გ) მდგრადია; დ) არამდგრადია.

14. 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.

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.

16. შიფრებს, რომლებიც ღია ტექსტის ყოველ სიმბოლოს შიფროტექსტში ცვლის სხვა სიმბოლოთი ეწოდება:

ა) გადანაცვლებადი შიფრში; ბ) წანაცვლებითი შიფრში;

გ) შენაცვლებითი შიფრში; დ) ჩანაცვლებითი შიფრში;

17. პოლიგრაფული ჩანაცვლების შიფრშია

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.

18. მარტივ სვეტურ გადანაცვლებადი ( 6Х7) შიფრით ღია ტექსტი ”მოწინააღმდეგის საარტილერიო დანადგარი ა8 კვადრატშია გამართული” იცვლება შემდეგი რა სახის შიფროტექსტით:

ა)”ლაიომმღ სუენ წდარააიეაიდ8ნგროგ აკასიდრვაათ აიტ დ უ რგლ ააი ტმ შა ირ ”

ბ)”მღ ნგროგ აიტ აკასიდრვაათ დ უ რგლ ააი ტმ შა ირ ლაიომსუენ წდარააიეაიდ8 ”

გ)”8ნგროგ აიტ აკამღ ლაიომსუენ წდარააიეაიდსიდრვაათ დ უ რგლ ააი ტმ შა ირ ”

დ)”მღ ლაიომსუენ წდარააიეაიდ8ნგროგ აიტ აკასიდრვაათ დ უ რგლ ააი ტმ შა ირ ” .

19. რომელი არაა სწორი მარტივი XOR -სთვის

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

20. K გასაღებზე დამოკიდებული n ორობითი სიმბოლოებისგან შემდგარი X სიტყვის გარდაქმნა ეს არის :

ა) ბლოკური შიფრი; ბ) გადანაცვლების შიფრი;

გ) ჩანაცვლების შიფრი; დ) ტიხრული შიფრი.

21. Rijndael- ში ყველა ოპერაცია , რომელიც სრულდება დასაშიფრ ბლოკზე , ეფუძნება არითმეტიკას:

ა) FG(216 ) ველში; ბ) FG(24 ) ველში; გ) FG(28 ) ველში; დ) FG(256 ) ველში.

22. ბაიტი, რომლის თექვსმეტობითი მნიშვნელობაა (57)hex  შეესაბამება პოლინომს:

ა) X6+ X4 + X2 +X+1; ბ) X8+ X6+X4 + X2 +X+1;

გ) X8+ X6+X4 + X3 +X+1; დ) X7+ X6+X4 + X3 +X+1.

23. რამდენი გასაღები გვაქვს ღია გასაღებიან კრიპტოგრაფიაში:

ა) 1; ბ) 2; გ) 3; დ) 4.

24. 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.

25. 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.

26. სინქრონიზებად ნაკადურ შიფრებს უწოდებენ:

ა) დამშიფრავი და გამშიფრავი გამების სინქრონიზაციას;

ბ) დამშიფრავი და გამშიფრავი გენერატორების სინქრონიზაციას;

გ) ესეთი არ არსებობს;

დ) ა) და ბ).

27. ზოგადად დაშიფრვა ეწოდება:

ა) შეტყობინების ფორმის, მისი სახის ცვლილებას;

ბ) შეტყობინების ფორმის გადაყვანას ორობით კოდში;

გ) შეტყობინების ფორმის შეცვლას ”ენიგმით”;

დ) ყველა სწორია.

28. შიფროტექსტების „გატეხვის“ ხელოვნებასა და მეცნიერებას ეწოდება:

ა) კრიპტოლოგია; ბ) კრიპტოანალიზი;

გ) კრიპტოსპექტრი; დ) კრიპტოგრაფია.

29. 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.

30. თანამედროვე კრიპტოგრაფიაში უნივერსალური ალგორითმის პრობ­ლემის მოგვარება ხდება:

ა) კავშირის არხის ფიზიკური გაუმჯობესებით:

ბ) გამგზავნის ტრენინგით; გ) მიმღების ტრენინგით;

დ) გასაღების საშუალებით.

31. სიმეტრიული ალგორითმები არ იყოფიან შემდეგ კატეგორიად:

ა) ნაკადური; ბ) ბლოკური; გ) ქსელური;

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

32. კრიპტოანალიტიკური გატეხვის რამდენი ძირითადი ტიპია:

ა) 3; ბ) 4; გ) 5; ბ) 6;

 33. 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.

34. გატეხვის სირთულე არ შეიძლება გაიზომოს შემდეგი საშუალებით:

ა) მოთხოვნა ანბანზე; ბ) მონაცემთა სირთულე;

გ) დამუშავების სირთულე; დ) მოთხოვნა მეხსიერების მიმართ.

35. ვინ არ წარმოადგენს პროტოკოლის მხარეს:

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

36. გასაღების გატეხვას - ყველა შესაძ­ლებელი ვარიანტების გადაარჩევით, ეწოდება:

ა) ძლიერი ძალა (ძძ); ბ) ლომის ძალა;

გ) უხეში ქმედება; დ) უხეში ძალა.

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

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

38. 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.

39 . კომპიუტერული კრიპტოგრაფიის ალგორითმები მუშაობენ:

ა) ბიტებზე; ბ) 33 სიმბოლურ ანბანზე;

გ) 26 სიმბოლურ ანბანზე; დ) ბაიტებზე.

40. 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.