ფინალური 2 კრიპტოლოგია

**კითხვა 1. შეტყობინების ავტორის უარყოფის პრობლემის წინააღმდეგ ეფექტურია:**

ა) სიმეტრიული კრიპტოგრაფია;

ბ) ღია გასაღებიანი კრიპტოგრაფია;

გ) კეისრის შიფრი;

დ) კურიერის მომსახურება.

**კითხვა 2. ცალმხრივ მიმართული ფუნქციაა:**

ა) რომელსაც შებრუნებული არ გააჩნია;

ბ) ნებისმიერი *x**X* -თვის ადვილია *y* *f* (*x*) მნიშვნელობის გამოთვლა, მაგრამ თითქმის ყველა *y**E*( *f* ) -თვის ისეთი *x**X* -ის პოვნა, რომ შესრულდეს ტოლობა *y* *f* (*x*) არის რთული.

გ) ნებისმიერი *x**X* -თვის რთულია *y* *f* (*x*) მნიშვნელობის გამოთვლა, მაგრამ თითქმის ყველა *y**E*( *f* ) -თვის ისეთი *x**X* -ის პოვნა, რომ შესრულდეს ტოლობა *y* *f* (*x*) არის ასევე რთული.

დ) ნებისმიერი *x**X* -თვის ადვილია *y* *f* (*x*) მნიშვნელობის გამოთვლა, მაგრამ თითქმის ყველა *y**E*( *f* ) -თვის ისეთი *x**X* -ის პოვნა, რომ შესრულდეს ტოლობა *y* *f* (*x*) არის რთული.

კითხვა 3. *a 25*(mod *n*) ტოლია:

ა) (((((*a2* mod *n*) *a*)mod *n*)2 mod *n*)2 mod *n*)2 *a*)mod *n;*

ბ)(((((*a2* mod *n*) *a*)mod *n*)2 mod *n*) mod *n*)2 *a*)mod *n;*

გ)(((((*a2* mod *n*) *a*)mod *n*) mod *n*)2 mod *n*)2 *a*)mod *n;*

დ)(((((*a2* mod *n*) *a*)mod *n*)2 mod *n*)2 mod *n*) *a*)mod *n.*

კითხვა 4. ნაკადურ შიფრებში ხდება ღია ტექსტის:

ა) ყოველი მეოთხე ბიტის (ან ბაიტის) გარდაქმნა შიფროტექსტად მაშინვე, როდესაც ის შემოდის ალგორითმში. ;

ბ) თითოეული ბიტის გარდაქმნა შიფროტექსტად დროის ერთეულის შემდეგ, როდესაც ის შემოდის ალგორითმში.;

გ) თითოეული ბიტის (ან ბაიტის) გარდაქმნა შიფროტექსტად მაშინვე, როდესაც ის შემოდის ალგორითმში;

დ) ყოველი მეორე ბიტის (ან ბაიტის) გარდაქმნა შიფროტექსტად მაშინვე, როდესაც ის შემოდის ალგორითმში.

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

ა) ფაილი; ბ) ღია ტექსტი;

გ) საიდუმლო ტექსტი; დ) დასაშიფრი ტექსტი.

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

ა) კრიპტოლოგია; ბ) კრიპტოანალიზი;

გ) კრიპტოსპექტრი; დ) კრიპტოგრაფია.

7. **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.

8. ***შეზღუდული* კრიპტოგრაფიული ალგორითმი დაფუძნებულია:**

ა) გასაღების საიდუმლოობაზე; ბ) მიმღების საიდუმლოობაზე;

გ) ალგორითმის საიდუმლოობაზე; დ) გამგზავნის საიდუმლოობაზე.

**9**. **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.

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

ა) ალგორითმით; ბ) შიფროტექსტი;

გ) გასაღებით; დ)შეტყობინების ხასიათი.

11. **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.

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

ა) მოთხოვნა ანბანზე; ბ) მონაცემთა სირთულე;

გ) დამუშავების სირთულე; დ) მოთხოვნა მეხსიერების მიმართ.

13. **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”.

14. **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.

15. **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.

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

ა) ბლოკების გაზრდა; ბ) მონაწილეთა რაოდენობის გაზრდა;

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

17. რას აკეთებენ კრიპტოგრაფიული ალგორითმები:

ა) ჩაანაცვლებენ ერთ სიმბოლოს მეორეთი; ბ) გადაადგილებენ სიმბოლოებს;

გ) ა და ბ; დ) არცერთს.

18. მარტივი ან მონოანბანური 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 ” ეს ინტერნეტ გამოცდაა კრიპტოგრაფიაში დღეს” იცვლება შემდეგი რა სახის შიფროტექსტით:

ა) ”მკრე რ სნორად ეციფღიტდპიენ ატასტგ აოშ ეა გი ” ;

ბ)”სნორად ეცერმკრ იფღიტდპიენ ატასტგაოშ ეა გი ” ;

გ)”ერმკრ სნორად ეციფღიტდპიენ ა ეა გი ტასტგაოშ” ;

დ)”ერმკრ სნორად ეციფღიტდპიენ ატასტგაოშ ეა გი ” .

20. მოცემულია შიფროტექსტია - ”ოოივე ვ ი აა ნნ დთ მხხ”, შიფრი სვეტებად გადანაცვლება, გასაღებად არჩეულია რვა ასოიანი სიტყვა, რა ზომის ცხრილის გამოყენებაა საჭიროშიფროტექსტის ჩასაწერად?

ა) 8Х4; ბ) 7Х5; გ) 8Х3; დ) 7Х5.

21. რომელი არაა სწორი მარტივი XOR -სთვის

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

22. ფეისტელის ქსელს აქვს შემდეგი სტრუქტურა - რომელია არასწორი;

ა) შემავალი ბლოკი იყოფა რამდენიმე თანაბარი სიგრძის ქვებლოკებად;

ბ) შემავალი ბლოკი იყოფა რამდენიმე არათანაბარი სიგრძის ქვებლოკებად;

გ) თითოეული განშტოება გარდაიქმნება - დაიშიფრება მეორისგან დამოუკიდებლად;

დ)თითოეული ბლოკი გარდაიქმნება - დაიშიფრება მეორისგან დამოუკიდებლად.

23. 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.

**24. *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 .

25. **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.

26. **კრიპტომედეგობის რაოდენობრივი შეფასების კრიტერიუმი არა:**

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

27. დაშიფრვის შედეგად ვღებულობთ;

ა) შიფრატორს; ბ) საიდუმლო კოდს;

გ) შიფროტექსტს; დ) შიფროფაილს.

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

ა) კრიპტოლოგია; ბ) კრიპტოანალიზი;

გ) კრიპტოსპექტრი; დ) კრიპტოგრაფია.

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

ა) ორიგინალობის შესამოწმებლად; ბ) მთლიანობის შესამოწმებლად;

გ) ავტორობის არაუარყოფობისთვის; დ) მოწყვლადობის შესაოწმებლად.

**30. კრიპტოსისტემა ეს არის:**

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

გ) გასაღებები; დ)ალგორითმი.

**31.** 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.

**32. 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.

**33. 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.

34. **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.

35. **გ.ი. ცეზარის შიფრი:**

ა) ნაწილობრივ მდგრადია; ბ) სრულიად არამდგრადია;

გ) მდგრადია; დ) არამდგრადია.

**36.** **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.

**37.** 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.

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

ა) გადანაცვლებადი შიფრში; ბ) წანაცვლებითი შიფრში;

გ) შენაცვლებითი შიფრში; დ) ჩანაცვლებითი შიფრში;

**39. 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.

**40. 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 ” .