Azərbaycan Respublikası Elm və Təhsil Nazirliyi
Lənkəran Dövlət Universiteti

"Təsdiq edirəm"
Tədris məsələləri üzrə prorektor v.i.e:
_____ dos. Zaur Məmmədov
"07" yanvar 2026-cı il

Fənn sillabusu

İxtisasın şifri və adı: 6006017 İnformasiya təhlükəsizliyi
Fakültə: Aqrar və mühəndislik
Kafedra: Texnologiya və texniki elmlər
I. Fənn haqqında məlumat:
Fənnin adı: Kriptoqrafiyanın əsasları ("Kriptoqrafiyanın əsasları" işçi fənn proqramı, Lənkəran Dövlət Universitetinin Texnologiya və texniki elmlər kafedrasının 07.01.2026-cı il 5 №-li protokoluna əsasən)
Kodu: İPF-B19
Tədris ili: III tədris ili, (2025-2026)
Semestr: VI(yaz)
Tədris yükü: 45 (30 saat mühazirə, 15 saat laboratoriya)
Təhsilalma forması: Əyani
Tədris dili: Azərbaycan dili
AKTS üzrə kredit: 5 kredit
II. Müəllim haqqında məlumat:
Soyadı, adı, ata adı, elmi dərəcəsi və elmi adı:
Mühazirə müəllimi: Məlikzadə Tural Tofiq oğlu
Laboratoriya müəllimi:Nuruzadə Arzu Əli qızı
Kafedranın ünvanı: Lənkəran şəhəri Füzuli 170 a, LDU-nun 1 saylı tədris binası
Məsləhət günləri və saatı:
E-mail ünvanı: tural1996t@gmail.com arzu.nuruzade96@gmail.com
III. Tövsiyə olunan dərslik, dərs vəsaiti və metodik vəsaitlər:

1. Orucəliyev A., *Kriptoqrafiyanın əsasları* (Bakı, 2019)
2. Prof.dr.Yadigar İmamverdiyev *Kriptoqrafiyanın əsasları üzrəə mühazirələr toplusu* Bakı: AzTU Press nəşriyyatı, 2025
3. Prof, Yadigar İmamverdiyev., Kriptoqrafiyanın əsasları (Bakı, 2019)
4. Məmmədov F.H., Orucova M.Y., *Informasiya təhlükəsizliyi və təminatı* (Bakı, 2022)
5. Zhiyong Zheng – Modern Cryptography, Volume 1 – Springer – 2023 – https://link.springer.com/book/10.1007/978-981-19-0920-7
6. Zhiyong Zheng, Kun Tian, Fengxia Liu – Modern Cryptography, Volume 2 – Springer – 2024 – https://link.springer.com/book/10.1007/978-981-19-7644-5

IV. Prerekvizit fənlər: Fənnin tədrisi üçün öncədən başqa bir fənnin tədrisinə zərurə yoxdur.
V. Korekvizit fənlər: Fənnin tədrisi ilə eyni zamanda başqa fənnin tədrisinə ehtiya yoxdur.
VI. Fənnin təsviri və məqsədi: Bu kurs çərçivəsində tələbələr ənənəvi kritoqrafiyanı yaranması ve inkişafına dair qısa tarixi, aktuallığını, tətbiq sahələrini və mövcu problemlərini, həmçinin müasir kriptosistemlər və şifrləmə üsulları ilə birlikdə kriptoqrafiyan informasiya təhlükəsizliyinin hansı prinsiplərini necə təmin etdiyini öyrənirlər. Kursda blo axın və açıq açarlı şifrləmə alqoritmaları ilə yanaşı qabaqcıl kriptoqrafik alqoritmlər icm edilir, bu alqoritmlərin praktiki tətbiqləri ilə əlaqəli məlumatlar verilir.

VII. Davamiyyətə verilən tələblər: Fənn üzrə semestr ərzində buraxılmış audit saatlarının ümumi sayı LDU-nun Elmi Şurasının 16 may 2024-cü il tarixli qərarına uyğun olaraq davamiyyət meyarları nəzərə alınmaqla müəyyən olunmuş həddən yuxarı olduqda halda tələbə həmin fəndən imtahana buraxılmır, onun həmin fənn üzrə akademik borcu qalır.

VIII. Qiymətləndirmə: Fənn üzrə tələbələrin biliyi 100 ballıq sistemlə qiymətləndirilir. Yəni tələbənin fənn üzrə toplaya biləcəyi balın maksimum miqdarı 100-ə bərabərdir. Bu balın yarısı (50 balı) tələbənin semestr müddətində fəaliyyətinin nəticəsinə (cari qiymətləndirmə), digər yarısı isə (digər 50 balı) imtahanın nəticəsinə (aralıq qiymətləndirmə) görə verilir.

Fənn üzrə cari qiymətləndirmənin nəticəsinə görə verilən maksimum 50 bala aşağıdakılar daxildir:

- 20 bal - seminar dərslərində fəaliyyətinə görə;
- 30 bal - kollokviumların nəticələrinə görə.

Qiymətləndirmə zamanı LDU-nun Elmi Şurasının 16 may 2024-cü il tarixli qərarına uyğun olaraq qiymətləndirmə meyarları nəzər alınır.

İmtahanda qazanılan balların maksimum miqdarı 50-dir. İmtahan yazılı şəkildə aparılır və imtahan biletinə bir qayda olaraq fənn üzrə tədris olunan mövzulara aid 5 sual daxil edilir. Hər sual maksimum 10 bal olmaqla qiymətləndirilir (aşağıda qeyd olunan qiymət meyarına əsasən) ki, bu da toplamda fənn üzrə aralıq qiymətləndirmənin nəticəsinə görə verilən maksimum 50 balı təşkil edir.

Qiymət meyarları aşağıdakılardır:

- 10 bal - tələbə keçilmiş materialı dərindən başa düşür, cavabı dəqiq və hərtərəflidir;
- 9 bal - tələbə keçilmiş materialı tam başa düşür, cavabı dəqiqdir və mövzunun məzmununu tam açа bilir;
- 8 bal - tələbə cavabında ümumi xarakterli bəzi qüsurlara yol verir;
- 7 bal - tələbə keçilmiş materialı yaxşı başa düşür, lakin nəzəri cəhətdən bəzi məsələləri əsaslandıra bilmir;
- 6 bal - tələbənin cavabı əsasən düzgündür;
- 5 bal - tələbənin cavabında çatışmazlıqlar var, mövzunu tam əhatə edə bilmir;
- 4 bal - tələbənin cavabı qismən doğrudur, lakin mövzunu izah edərkən bəzi səhvlərə yol verir;
- 3 bal - tələbənin mövzudan xəbəri var, lakin fikrini əsaslandıra bilmir;
- 1-2 bal - tələbənin mövzudan qismən xəbəri var;
- 0 bal - cavab yoxdur.

Tələbənin fənn üzrə aralıq qiymətləndirmə balının (imtahanda topladığı balın) miqdarı 17-dən az olmamalıdır. Əks təqdirdə tələbənin fənn üzrə aralıq qiymətləndirmə balı cari qiymətləndirmə balına (semestr ərzində tədris fəaliyyəti nəticəsində topladığı bala) əlavə olunmur.

Fənn üzrə cari və aralıq qiymətləndirmənin ümumi nəticəsinə görə tələbənin biliyi yekun olaraq aşağıdakı kimi qiymətləndirilir:

Bal aralığı (göstərilən ballar daxil olmaqla)	Hərflə işarəsi	Sözlə yazılışı
91-100 bal	A	əla
81-90 bal	B	çox yaxşı
71-80 bal	C	yaxşı
61-70 bal	D	kafi
51-60 bal	E	qənaətbəxş
51-baldan aşağı	F	qeyri-kafi

IX. Davranış qaydalarının pozulması:

Tələbə Universitetin Daxili intizam qaydalarını pozduqda onun barəsində mövcud qanunvericilik çərçivəsində müvafiq tədbir görüləcəkdir.

X. Təqvim mövzu planı:

Mühazirə: 30 saat; laboratoriya: 15 saat; **Cəmi: 45 saat.**

№	Tədris olunan mövzuların məzmunu	Saat	Tarix
		Mühazirə	
1	**Mövzu № 1. Kriptoqrafiyanın tarixi və əsas anlayışları** Plan 1. Kriptoqrafiya termini, onun yaranma tarixi. 2. İnformasiya təhlükəsizliyi prinsipləri: məxfilik, bütövlük, identifikasiya, autentifikasiya. 3. Kriptoqrafiyanın müasir rolu və tətbiq sahələri (elektron imza, e-dövlət, maliyyə, rabitə və s.)	2	
2	**Mövzu № 2. Şifrələmə üsulları** Plan 1. Sezar şifrələmə üsulu 2. Qronsfeld şifrələmə üsulu 3. Əvəz etmə şifrələmə üsulu 4. Çoxəlifbalı şifrələmə üsulu	2	
3	**Mövzu № 3. Klassik şifrələrin kriptoanalizi** Plan 1. Kriptoanalizin yaranma tarixi və inkişafı 2. Kriptoanalizin məqsədi və informasiya təhlükəsizliyində rolu 3. Tezlik analizi və statistik metodlar	2	
4	**Mövzu № 4. Axın şifrələri və onların tətbiqləri** Plan 1. Axın şifrələri anlayışı və onların iş prinsipləri 2. Axın şifrələrinin növləri və əsas xüsusiyyətləri 3. Axın şifrələrinin tətbiq sahələri	2	
5	**Mövzu № 5. Simmetrik şifrələmə alqoritmləri** Plan 1. DES (Data Encryption Standard) 2. AES (Advanced Encryption Standard)	2	
6	**Mövzu № 6. Blok şifrələmədə işləmə rejimləri** Plan 1. Blok şifrələmə anlayışı və növləri 2. Blok şifrələmədə işləmə rejimlərinin rolu və tətbiq sahələri	2	
7	**Mövzu № 7. Simmetrik və Asimmetrik kriptoqrafiya arasındakı fərqlər** Plan 1. Simmetrik kriptoqrafiya anlayışı, üstünlükləri və çatışmazlıqları 2. Asimmetrik kriptoqrafiya anlayışı, üstünlükləri və çatışmazlıqları 3. Hibrid şifrələmə - SSL / TLS	2	
8	**Mövzu № 8. Açıq açarlı kriptoqrafiya və PKİ əsasları** Plan 1. Açıq açarlı kriptoqrafiyanın anlayışı və iş prinsipi	2	

	2. PKİ (Public Key Infrastructure) əsasları 3. Açıq açarlı kriptoqrafiyanın tətbiq sahələri: (elektron imza, şifrəli rabitə və s)		
9	**Mövzu № 9. Heş funksiyaları və məlumatın bütövlüyü** Plan 1. Kriptoqrafik heş funksiyalarının xassələri 2. Məlumatın bütövlüyü və yoxlanılması 3. Heş alqoritmlərinin növləri (MD5, SHA-1, SHA-256 və s.)	2	
10	**Mövzu № 10. Autentifikasiya və inkar edilməzlik mexanizmi** Plan 1. Autentifikasiya anlayışı və məqsədi 2. Non-repudiation (inkar edilməzlik) mexanizmi	2	
11	**Mövzu № 11. Şifrəli rabitə protokolları** Plan 1. Şifrəli rabitə anlayışı və məqsədi 2. SSL/TLS protokolunun əsas prinsipləri və iş mexanizmi 3. IPSec protokolunun strukturu və funksiyaları	2	
12	**Mövzu № 12. Blokçeyn və kriptovalyutalarda kriptoqrafiya** Plan 1. Blokçeyn anlayışı və əsas prinsipləri 2. Kriptoqrafiyanın Blockçeyn tətbiqi	2	
13	**Mövzu № 13. Post-kvant kriptoqrafiyası və qabaqcıl protokollar** Plan 1. Post-kvant kriptoqrafiyasının tarixi və inkişafı 2. Qabaqcıl protokollar və kvant müqavimətli alqoritmlər	2	
14	**Mövzu № 14. Kriptoqrafiya alqoritmlərinin tətbiqləri və gələcək perspektivləri** Plan 1. Kriptoqrafiya alqoritmlərinin əsas tətbiq sahələri (maliyyə, bank, e-dövlət, rabitə) 2. Kriptoqrafiyanın gələcək rolu və perspektivləri	2	
15	**Mövzu № 15. Sertifikatlar və açar infrastrukturunun inkişafı** Plan 1. Açar infrastrukturunun tarixi: X.509 sertifikatları və sertifikatlar zənciri. 2. Sertifikatın verilməsi, yenilənməsi və ləğvi prosesləri (OCSP). 3. Rəqəmsal təhlükəsizlik siyasətləri: sertifikat etibarlılığı, milli və beynəlxalq təhlükəsizlik normaları.	2	
Cəmi		**30 saat**	

№	Tədris olunan mövzuların məzmunu	Saat	Tarix

		Laboratoriya	
1	**Mövzu № 1.** Kriptoqrafiyanın tarixinin, əsas anlayışlarının öyrənilməsi, şifrələmə üsulları (Sezar, Qronsfeld, əvəz etmə və çoxəlifbalı şifrələmə) ilə mətnin əl ilə və proqram vasitəsilə şifrələnməsi və deşifrələnməsi	2	
2	**Mövzu № 2.** Klassik şifrələrin kriptoanalizi, axın şifrələrinin tətbiq edilməsi	2	
3	**Mövzu № 3.** Simmetrik şifrələmə alqoritmlərindən (DES və AES) istifadə etməklə şifrələnmənin tətbiqi və müxtəlif blok şifrələmədə işləmə rejimlərinin nəticələrinin müqayisəsinin aparılması	2	
4	**Mövzu № 4.** Simmetrik və asimmetrik kriptoqrafiya əsasında açar yaradılması və açıq açar mexanizmi ilə məlumat mübadiləsinin həyata keçirilməsi (PKİ)	2	
5	**Mövzu № 5.** Heş funksiyalarından istifadə etməklə məlumatın bütövlüyünün yoxlanılması, autentifikasiya prosesinin icrası və inkaredilməzlik mexanizminin tətbiqi	2	
6	**Mövzu № 6.** Şifrəli rabitə protokolları əsasında şifrəli rabitənin qurulması və blokçeyn texnologiyasında kriptoqrafik mexanizmlərin tətbiqi	2	
7	**Mövzu № 7.** Post-kvant kriptoqrafiyası və qabaqcıl protokolların tətbiqi, kriptoqrafiya alqoritmlərinin tətbiqi nümunələrinin icrası və gələcək perspektivlərin təhlili	2	
8	**Mövzu № 8.** Sertifikatlar-onların verilməsi, yenilənməsi və ləğvi prosesləri ilə iş və açar infrastrukturunun idarə edilməsi	1	
Cəmi		**15saat**	

XI. Fənn üzrə tələblər:

- Klassik və müasir kriptoqrafiyanı, simmetrik və asimmetrik şifrləmə sistemlərini fərqləndirməlidir.
- Konfidensiallıq, tamlıq, autentifikasiya və inkar edilməmənin kriptoqrafik təminatını bilməlidir.
- Blok və axın şifrləri, əsas alqoritmləri və tətbiq sahələrini tanımalıdır.
- Açıq açarlı alqoritmlər və PKI haqqında əsas biliklərə malik olmalıdır.
- Heş funksiyalarının rolunu və rəqəmsal imzalardakı əhəmiyyətini başa düşməlidir.
- Qabaqcıl kriptoqrafik protokolların tətbiqləri barədə ümumi anlayışa sahib olmalıdır.

XII. Fənnin tədrisi üçün nəzərdə tutulan tədris və öyrənmə metodları:

Təlim prosesində fərqli tədris metodlarından istifadə edilməlidir. Bu metodlar tələbəyönü yanaşmanı və tələbələrin təlim prosesindəki fəal rol oynamasını təşviq etməlidir. İstif edilə biləcək tədris və öyrənmə üsullarına aşağıdakıları nümunə olaraq göstərmək olar:

– mühazirələr,

– təcrübi tapşırıqlar:

- təqdimatlar və müzakirələr,
- problemlərə əsaslanan tədris:
- rol oyunlar hesabatlar:
- qrup qiymətləndirməsi:
- ekspert metodu;
- simulyasiyalar;

XIII. Fənn üzrə təlim nəticələri:

FTN 1- Klassik ve müasir kriptoqrafiya arasındakı fərqləri bilməli, klassik şifrlərin kriptoanalizi metodları ilə tanış olmalıdır. Simmetrik ve asimmetrik şifrləmə sistemlərinin fərqlərini bilməlidir.

FTN 2- Informasiya təhlükəsizliyi prinsiplərindən konfidensiallıq və tamlığın, o cümlədəen autentikasiya və inkar edilməmə prinsiplərinin kriptoqrafik üsullarla necə təmin olunduğunu bilməlidir.

FTN 3- Blok şifrlər və axın şifrlər arasındakı fərqləri, onlara uyğun alqoritmlər və bu alqoritmlərin tətbiq sahələrini bilməlidir.

FTN 4-Açıq açarlı şifrlərlə əlaqəli alqoritmləri, onlarin tətbiqlərini bilməlidir. Açıq açar infrastrukturu haqda məlumatlı olmalıdır.

FTN 5- Heş funksiyalarının xususiyyətlərini bilməli onlardan istifadə edilərək tamlığın necə təmin edildiyini və rəqəmsal imzalardakı mahiyyətini bilməlidir

FTN 6-Qabaqcıl kriptoqrafik protokolları və onların tətbiqlərini bilməlidir.

XIV. Tələbələrin fənn haqqında fikrinin öyrənilməsi:

XV. Kollokvium sualları:

I. Kollokvium sualları

1. Kriptoqrafiya termini, onun yaranma tarixi.
2. İnformasiya təhlükəsizliyi prinsipləri: məxfilik, bütövlük, identifikasiya, autentifikasiya.
3. Kriptoqrafiyanın müasir rolu və tətbiq sahələri (elektron imza, e-dövlət, maliyyə, rabitə və s.)
4. Sezar şifrələmə üsulu
5. Qronsfeld şifrələmə üsulu
6. Əvəz etmə şifrələmə üsulu
7. Çoxəlifbalı şifrələmə üsulu
8. Kriptoanalizin yaranma tarixi və inkişafı
9. Kriptoanalizin məqsədi və informasiya təhlükəsizliyində rolu
10. Axın şifrələrinin növləri və əsas xüsusiyyətləri

II. Kollokvium sualları

1. DES (Data Encryption Standard)
2. AES (Advanced Encryption Standard)
3. Blok şifrələmə anlayışı və növləri
4. Blok şifrələmədə işləmə rejimlərinin rolu və tətbiq sahələri
5. Simmetrik kriptoqrafiya anlayışı, üstünlükləri və çatışmazlıqları
6. Asimmetrik kriptoqrafiya anlayışı, üstünlükləri və çatışmazlıqları
7. Hibrid şifrələmə - SSL / TLS

8. Açıq açarlı kriptoqrafiyanın anlayışı və iş prinsipi
9. Kriptoqrafik heş funksiyalarının xassələri
10. Autentifikasiya anlayışı və məqsədi

XVI. İmtahan sualları:

1. Kriptoqrafiya termini, onun yaranma tarixi
2. İnformasiya təhlükəsizliyi prinsipləri: məxfilik, bütövlük, identifikasiya, autentifikasiya
3. Kriptoqrafiyanın müasir rolu və tətbiq sahələri (elektron imza, e-dövlət, maliyyə, rabitə və s.
4. Sezar şifrələmə üsulu
5. Qronsfeld şifrələmə üsulu
6. Əvəz etmə şifrələmə üsulu
7. Çoxəlifbalı şifrələmə üsulu
8. Kriptoanalizin yaranma tarixi və inkişafı
9. Kriptoanalizin məqsədi və informasiya təhlükəsizliyində rolu
10. Tezlik analizi və statistik metodlar
11. Axın şifrələri anlayışı və onların iş prinsipləri
12. Axın şifrələrinin növləri və əsas xüsusiyyətləri
13. Axın şifrələrinin tətbiq sahələri
14. DES (Data Encryption Standard)
15. AES (Advanced Encryption Standard)
16. Blok şifrələmə anlayışı və növləri
17. Blok şifrələmədə işləmə rejimlərinin rolu və tətbiq sahələri
18. Simmetrik kriptoqrafiya anlayışı, üstünlükləri və çatışmazlıqları
19. Asimmetrik kriptoqrafiya anlayışı, üstünlükləri və çatışmazlıqları
20. Hibrid şifrələmə - SSL / TLS
21. Açıq açarlı kriptoqrafiyanın anlayışı və iş prinsipi
22. PKİ (Public Key Infrastructure) əsasları
23. Açıq açarlı kriptoqrafiyanın tətbiq sahələri: (elektron imza, şifrəli rabitə və s)
24. Kriptoqrafik heş funksiyalarının xassələri
25. Məlumatın bütövlüyü və yoxlanılması
26. Heş alqoritmlərinin növləri (MD5, SHA-1, SHA-256 və s.)
27. Autentifikasiya anlayışı və məqsədi
28. Non-repudiation (inkar edilməzlik) mexanizmi
29. Şifrəli rabitə anlayışı və məqsədi
30. SSL/TLS protokolunun əsas prinsipləri və iş mexanizmi
31. IPSec protokolunun strukturu və funksiyaları
32. Blokçeyn anlayışı və əsas prinsipləri
33. Kriptoqrafiyanın Blockçeyn tətbiqi
34. Post-kvant kriptoqrafiyasının tarixi və inkişafı
35. Qabaqcıl protokollar və kvant müqavimətli alqoritmlər
36. Kriptoqrafiya alqoritmlərinin əsas tətbiq sahələri (maliyyə, bank, e-dövlət, rabitə
37. Kriptoqrafiyanın gələcək rolu və perspektivləri
38. Açar infrastrukturunun tarixi: X.509 sertifikatları və sertifikatlar zənciri
39. Sertifikatın verilməsi, yenilənməsi və ləğvi prosesləri (OCSP).
40. Rəqəmsal təhlükəsizlik siyasətləri: sertifikat etibarlılığı, milli və beynəlxalq təhlükəsizlik normaları.

"Kriptoqrafiyanın əsasları" fənninin sillabusu **6006017 - "İnformasiya təhlükəsizliyi"** ixtisasının təhsil proqramı, tədris planı və bu fənnin işçi fənn proqramı əsasında tərtib edilmişdir.
Sillabus **"Texnologiya və texniki elmlər"** kafedrasında müzakirə edilərək təsdiq edilmişdir **(07.01.2026-cı il, protokol № 5).**

Fənn müəllimi: **Tural Məlikzadə,**

Arzu Nuruzadə

Kafedra müdiri: **Dos Rəşad Əliyev**