

**O'ZBEKISTON RESPUBLIKASI O'LIY
TA'LIM, FAN VA INNOVATSIYALAR
VAZIRLIGI**



**SHAROF RASHIDOV NOMLI
SAMARQAND DAVLAT**



Ro'yxatga olindi:

№ **88-60610200**
2024-yil **10.25**

"KRIPTOGRAFIYA"

rektori

R.I. Xalmuradov

KRIPTOGRAFIYA USULLARI

FAN DASTURI

Bilim sohasi:	60000–Axborot-kommunikatsiya texnologiyalari
Ta'lim sohasi:	610000–Axborot-kommunikatsiya texnologiyalari
Ta'lim yo'nalishi:	60610200 – Axborot xavfsizligi

Sharof Rashidov nomidagi Samarqand davlat universiteti "60610200–
Axborot xavfsizligi" yo'nalishining ishchi o'quv rejasidagi "Kriptografiya
usullari" fanining fan dasturiga

TAQRIZ

"Kriptografiya usullari" fani dasturi zamonaviy axborot xavfsizligini ta'minlashda muhim
rol o'ynaydi. Fan kriptografiya asoslarini, shifrlash va shifrdan chiqarish jarayonlarini,
hamda turli xil kriptografik algoritmlar va protokollarni o'z ichiga oladi. Dasturda simmetrik
va assimetrik kriptografiya, hash funksiyalari va raqamli imzolar kabi asosiy mavzular
chuqur yoritilgan.

Fan dasturi nazariy bilimlar bilan birga amaliy mashg'ulotlarni ham o'z ichiga oladi.
Talbalar kriptografik algoritmlarni real tizimlarda qanday qo'llashni o'rganishadi, masalan,
AES, RSA va SHA-256 kabi standartlardan foydalanish orqali. Bu amaliy mashg'ulotlar
talbalar uchun kriptografiyaning amaliyotida qanday ishlatishni tushinishiga yordam beradi,
bu esa ularning malakasini oshiradi.

Dasturda, shuningdek, kriptografiyaning zamonaviy yondashuvlari, jumladan, kvant
kriptografiyasi va blockchain texnologiyalari kabi yangi yo'nalishlar ham ko'rib chiqilgan.
Bu yangiliklar talabalarni kriptografiyaning kelajagi haqida o'ylashga undaydi va ularga
zamonaviy muammolarni hal qilishda qo'shimcha bilim beradi.

Umuman olganda, "Kriptografiya usullari" fani dasturi haliqat nazariy bilimlarni, balki
amaliy ko'nikmalarni ham berishga qaratilgan. Axborot xavfsizligini ta'minlashda
kriptografiyaning ahamiyatini inobatga olganda, mazkur dastur o'quvchilarning bu sohadagi
bilim va ko'nikmalarini rivojlantirish uchun yaxshi tashkil etilgan.

Sharof Rashidov nomidagi
Samarqand davlat universiteti
"Sun'iy intellekt va axborot tizimlari"
Kafedrası PhD dotsenti:

F. Nazarov



Fan/modul kodi KRU1506	O'quv yili 2025- 2026	Semestr 5	ECTS—Kreditlar 6
Fan/modul turi Majburiy fan	Ta'lim tili O'zbek	Haftadagi dars soatlari 4	
1. Fan nomi	Auditoriya mashg'ulotlari (soat)	Mustaqil ta'lim (soat)	Jami (soat)
Kriptografiya usullari	78	102	180
2. I. Fanning mazmuni Fanni o'qitishdan maqsad — talabalarga va mutaxassislariga axborot xavfsizligini ta'minlash bo'yicha asosiy tamoyillarni tushuntirish va zamonaviy kriptografik texnologiyalardan foydalanish ko'nikmalarini shakllantirishdir. Fanning vazifasi — talabalarga raqamli dalillarni aniqlash, to'plangan ma'lumotlarni asosida hujum manbasini aniqlash va saqlash vositalaridan foydalanilgan holda ma'lumotlarni tiklash, noqonuniy axborot o'g'irlanishini bartaraf etish va kompyuter jinoyati sodir etilganda tergov usullari va ekspert faoliyati ahamiyatini ochib berishi. II. Asosiy nazariy qism (ma'ruza mashg'ulotlari) II.1. Fan tarkibiga quyidagi mavzular kiradi: Kriptografiyaning Tarixi va Asosiy Tushunchalar Kriptografiya Asoslari va Modelar Simmetrik Kalitli Shifrlash Usullari Kriptografiyaning matematik asosi Assimetrik Kalitli Shifrlash Usullari Hesh-Funksiyalar va Ularning Qo'llanilishi Raqamli Imzolar va Autentifikatsiya Kriptografik Protokollar Kriptoanaliz Asoslari Simmetrik blokli shifrlash algoritmlari. Blowfish algoritmi. Simmetrik kriptografik algoritmlar. Oqimli shifrlash algoritmlari. Ochiq kalitli kriptografik tizimlar. RSA algoritmi. Ochiq kalitli kriptografik tizimlar. El-Gamal algoritmi. Kriptografiyada Matematik Asoslar Zamonaviy Kriptografiya va Kelajakdagi Istiqbollar III. Amaliy mashg'ulotlar bo'yicha ko'rsatma va tavsiyalar Amaliy mashg'ulotlar uchun quyidagi mavzular tavsiya etiladi: Simmetrik shifrlash algoritmini implementatsiya qilish Klassik shifrlar: afzalligi va bardoshligi RSA algoritmini dasturlash va shifrlash/deshifrlash jarayonlarini amalga oshirish			

RSA algoritmini dasturlash va shifrlash/deshifrlash jarayonlarini amalga oshirish.	
Hesh-funksiyalarni implementatsiya qilish va ularning qo'llanilishi	
Raqamli imzo tizimini yaratish	
TLS/SSL protokolining simulyatsiyasi	
Kriptoanaliz usullarini qo'llash	
Elliptic curve cryptography (ecc) algoritmini implementatsiya qilish	
Blok shifrlash rejimlarini taqqoslash	
Kvant kriptografiyasi asoslarini eksperimentlar bilan o'rganish	
Kriptografik protokollarini sinovdan o'tkazish	
Oqimli shifrlash algoritmlari.	
O'zbekiston Respublikasining ERI algoritmi	
Kalitlarni taqsimlash algoritmlari	
Ma'lumotlarni xeshlash va parol bazasini himoyalash	
IV. Laboratoriya mashg'ulotlar bo'yicha ko'rsatma va tavsiyalar	
Laboratoriya mashg'ulotlar uchun quyidagi mavzular tavsiya etiladi:	
Matn ma'lumotlarni himoyalashda klassik o'rnatilgan va o'rnatilmashtirish algoritmlaridan foydalanish.	
Vernam va Vijnier shifrlari asosida dasturiy modul ishlab chiqish.	
DES simmetrik kriptotizimi dasturiy modulini ishlab chiqish.	
Rijndael simmetrik kriptotizimi dasturiy modulini ishlab chiqish.	
A5/1 va RC4 shifrlash algoritmi dasturiy modulini ishlab chiqish.	
V. Mustaqil ta'lim va mustaqil ishlar	
Mustaqil ta'lim uchun tavsiya etiladigan mavzular:	
1. Enigma shifrlash mashinasi.	
2. Bir martali "bloknot".	
3. Venona proekti.	
4. "Kodlar kitobi" shifri.	
5. Kriptografik tizimlarning tavsifi.	
6. Analitik usullarga asoslangan shifrlash algoritmi.	
7. WEP protokolida foydalanilgan RC4 algoritmining tahlili.	
8. Blowfish algoritmi tahlili.	
9. CAMELLIA shifrlash algoritmi.	
10. SHA – 256 – xesh funksiya algoritmi.	
11. HMAC tizimlari.	
12. Kalitlarni generatsiyalash algoritmlari.	
13. Kriptotahlil usullari	
14. Axborotni xavfsizligini ta'minlashda kriptografiyaning o'rni.	
15. Kriptografik vositalar va ularning tasnifi.	
16. O'zbekistonda kriptografiya sohasida olib boriladigan ishlar.	
17. Checkli maydonda ko'p hadlar ustida amallar (AES misolida).	

18.	Parametrlar algebra muammosi va undagi asosiy amallar.
19.	Bulutli hisoblash tizimlarida foydalaniladigan kriptografik algoritmlar.
20.	Faktorlar muammosi va uni yechish usullari.
21.	Diskret logarifmlash muammosi va uni yechish usullari.
3.	VI. Fan o'qitilishining natijalari (shakllanadigan kompetensiyalar) Fan o'qitilishining natijalari (shakllanadigan kompetensiyalar) Fanni o'zlashtirish natijasida talaba: - fanni o'rganish uchun talabalardan algoritmlash, dasturlash asoslarini va zamonaviy dasturlash tillarini; - bir tomonlama funksiyalarini; - xabarlamni haqiqiylikni tekshirish kodlarini; - aralash kriptotizimlarini; - kalitlarni generatsiyalash protokollarini bilishi va ulardan foydalana olishi; - axborotni himoyalash vositalari bilan tanish bo'lishi, ularning texnologiyalarini baholash, autentifikatsiyalash, identifikatsiyalash usullari, elektron raqamli imzo to'g'risida ko'nikmalariga ega bo'lishi kerak.
4.	VII. Ta'lim texnologiyalari va metodlari: • ma'ruzalar; • interfaol keys-stadilar; • seminarlar (mantiqiy fikrlash, tezkor savol-javoblar); • guruhlarda ishlash; • taqdimotlar qilish; • individual loyihalar; • jamoa bo'lib ishlash va ximoya qilish uchun loyihalar.
5.	VII. Kreditni olish uchun talablar: Fanga oid nazariy va uslubiy tushunchalarni to'la o'zlashtirish, tahlil natijalarini tegishli to'g'ri aks ettira olish, o'rganilayotgan jarayonlar haqida mustaqil mushohada yuritish, amaliy mashg'ulotlarda berilgan masalalar dasturini tuzish va joriy, oraliq nazarot shakllarida berilgan vazifa va topshiriqlarni bajarish, yakuniy nazarot bo'yicha yozma ishini topshirish.
6.	Asosiy adabiyotlar: 1. Yusupov S. Y. G'ulomov, Nasrullayev B, Raqamli kriminalistika: O'quv qo'llanma: - Tashkent, "Aloqachi" 2019 294 bet.

2.	1. Мельникова, И.З. Информатика. Учебное пособие / И.З. Мельникова. — М.: «Академия» 2022. Qo'shimcha adabiyotlar: 1. O'zbekiston Respublikasi Prezidentining 2022 yil 28 yanvardagi PF-60-son "2022–2026-yillarga mo'ljallangan yangi O'zbekistonning taraqqiyot strategiyasi to'g'risida" gi Farmoni 2. Bill Nelson, Amelia Phillips, Christopher Stewart Guide to Computer Forensics and Investigations: Processing Digital Evidence, Sixth Edition Boston, MA 02210, 2019, USA 3. Umad S. Hassan, Security and Data Reliability in Cooperative Wireless Networks. © 2018 by Taylor & Francis Group, LLC 4. Richard Boddington, Practical Digital Forensics. First published: May 2016. Birmingham B3 2PB, UK, 545 Axborot manbalari (saytlar): 5. https://www.unode.org/documents/e4/Cybercrime_Module_4_Introduction_to_Digital_Forensics_RU.pdf 6. http://jnhicholl.org/Cryptanalysis/Tools/ 7. https://www.cryptool.org/en/cto/ 8. www.athenaforensics.co.uk/ 9. www.securitylab.ru/ 10. https://blackarch.org/crypto.html 11. www.criminologycareers.about.com/ 12. www.nij.gov/topics/forensics/evidence/digital/
7.	Fan dasturi Samarqand davlat universiteti O'quv-uslubiy kengashining 2024- yil <u>24</u> <u>avgust</u> dagi <u>1</u> -son bayonnomasi bilan ma'qullangan.
8.	Fan/modul uchun mas'ullar: I.R.Rahmatullayev – SamDU, "Kompyuter ilmlari va texnologiyalari fanlari" kafedrası dotsenti, texnika fanlari bo'yicha falsafa doktori (PhD)
9.	Taqrizchilar: F.Nazarov – texnika fanlari falsafa doktori, kafedra mudiri (tel:(99)0636901) A. Abdugarimov – TATU SF "Kompyuter tizimlari" kafedrası dotsenti, texnika fanlari falsafa doktori, PhD.

Rais:

Kafedra mudiri:

Fakultet kengashi raisi

Kelishildi

O'quv ishlar bo'yicha prorektor:

S. Axtulqulov

M.Q. Nurmatov

F. M. Nazarov



TAQRIZ

"Kriptografiya usullari" fani dasturi zamonaviy axborot xavfsizligini ta'minlashda muhim rol o'ynaydi. Fan kriptografiya asoslarini, shifrlash va shifrdan chiqarish jarayonlarini, hamda turli xil kriptografik algoritmlar va protokollarni o'z ichiga oladi. Dasturda simmetrik va assimetrik kriptografiya, hash funksiyalari va raqamli imzolar kabi asosiy mavzular chuqur yoritilgan.

Fan dasturi nazariy bilimlar bilan birga amaliy mashg'ulotlarni ham o'z ichiga oladi. Talabalar kriptografik algoritmlarni real tizimlarda qanday qo'llashni o'rganishadi, masalan, AES, RSA va SHA-256 kabi standartlardan foydalanish orqali. Bu amaliy mashg'ulotlar talabalar uchun kriptografiyaning amaliyotida qanday ishlab chiqarishni tushunishga yordam beradi, bu esa ularning malakasini oshiradi.

Dasturda, shuningdek, kriptografiyaning zamonaviy yondashuvlari, jumladan, kvant kriptografiyasi va blockchain texnologiyalari kabi yangi yo'nalishlar ham ko'rib chiqilgan. Bu yangiliklar talabalarni kriptografiyaning kelajagi haqida o'ylashga undaydi va ularga zamonaviy muammolarni hal qilishda qo'shimcha bilim beradi.

Umuman olganda, "Kriptografiya usullari" fani dasturi nafaqat nazariy bilimlarni, balki amaliy ko'nikmalarni ham berishga qaratilgan. Axborot xavfsizligini ta'minlashda kriptografiyaning ahamiyatini inobatga olganda, mazkur dastur o'quvchilarning bu sohada bilim va ko'nikmalarini rivojlantirish uchun yaxshi tashkil etilgan.

TATU "Kompyuter tizimlari"
kafedrasi dotsenti

A. Abduraimov

