O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

Ro‘yxatga olindi: № 8/9(750/751)
2025-yil “29” 04.

“TASDIQLAYMAN”
O‘quv ishlari bo‘yicha prorektor
Dj.Sulaymonov
2025-yil “29” 04

KRIPTOGRAFIYA USULLARI FANINING

O‘QUV DASTURI

Bilim sohasi:	600 000	-	Axborot-kommunikatsiya texnologiyalari
Ta’lim sohasi:	610 000	-	Axborot-kommunikatsiya texnologiyalari
Ta’lim yo‘nalishi:	60610300	-	Axborot xavfsizligi (Axborot kommunikatsiya texnologiyalari va servis)

Toshkent 2025

Fan/modul kodi	O‘quv yili	Semestr	ECTS – Kreditlar
CRYM18MBK	2025-2026	5	8
Fan/modul turi	**Ta’lim tili**		**Xaftadagi dars soatlari**
Majburiy	O‘zbek/rus		6.4

1.	Fanni nomi	Auditoriya mashg‘ulotlari (soat)	Mustaqil ta‘lim (soat)	Jami yuklama (soat)
	Kriptografiya usullari	**96**	**144**	**240**

2. I. Fanning mazmuni

Fanni o‘qitishdan maqsad – talabalarga axborot xavfsizligini ta’minlashda muhim rol o‘ynaydigan klassik va zamonaviy kriptografik algoritmlar, protokollar, shifrlash usullari, xesh funksiyalar, raqamli imzo va ochiq kalitlar infratuzilmasi bo‘yicha nazariy bilimlar va amaliy ko‘nikmalarni shakllantirishga qaratilgan.

Fanning vazifasi — talabalarni klassik va zamonaviy shifrlash usullari, simmetrik va ochiq kalitli kriptografik algoritmlar, shifrlash rejimlari, psevdotasodifiy sonlar generatorlari, oqimli shifrlash, xesh funksiyalar, elektron raqamli imzo tizimlari, ochiq kalitlar infratuzilmasi hamda zamonaviy kriptografiyaning istiqbolli yo‘nalishlari bo‘yicha nazariy bilimlar va amaliy ko‘nikmalarga ega bo‘lishga tayyorlashdan iborat.

II. Asosiy nazariy qism (ma‘ruza mashg‘ulotlari)

II.1. Fan tarkibiga quyidagi mavzular kiradi:

1-mavzu: Klassik shifrlash usullari

O‘rniga qo‘yish, o‘rin almashtirish shifrlari. Shifrlashning asosiy tushunchalari. Rotor mashinalari. Vijiner va vernam shifri.

2-mavzu: Simmetrik blokli shifrlar

Simmetrik shifrlar tasnifi. Blokli shifrlarni qurish usullari. Blokli shifrlarning parametrlari. DES shifrlash standarti.

3-mavzu: AES shifrlash standarti (4 soat)

Matematik asosi. Konkursdagi baholash mezonlari. Rijndael algoritmi.

4-mavzu: Simmetrik shifrlash algoritmlari qo‘llanish rejimlari (4 soat)

Blokli shifrlash rejimlari (ECB, CBC, CFB, OFB, CTR). Autentifikatsiya qilingan shifrlash rejimlari.

5-mavzu: Zamonaviy blokli shifrlar (8 soat)

3DES, Blowfish. Camellia. Milliy shifrlash standarti. GOST 28147-89 algoritmi.

6-mavzu: Psevdotasodifiy sonlar generatori (4 soat)

Tasodifiy va psevdotasodifiy sonlar. Tasodifiy bitni hosil qilish. ANSI X9.17, FIPS 186 algoritmi. RSA, Blum-Blum-Shub psevdotasodifiy bitlar generatori.

7-mavzu: Oqimli simmetrik shifrlar (6 soat)

Algoritmlarning tasnifi. FSR va LFSRga asoslangan oqimli shifrlash algoritmlari. SEAL algoritmi. RC4 algoritmi. A5/1 oritm

8-mavzu: Ochiq kalitli kriptografiya va RSA algoritmi.

Ochiq kalitli kriptografiyaning ishlash prinsipi. RSA algoritmi. Qo'llanilish sohasi. El-Gamal algoritmi.

9-mavzu: Turli ochiq kalitli kriptografiya algoritmlari (4 soat)

Diffi – Xelman kalitlarni taqsimlash protokoli. Elliptik egri chiziqqa asoslangan Diffi – Xelman kalitlarni taqsimlash protokoli.

10-mavzu: Xesh funksiyalar va ma'lumotlar yaxlitligi (6 soat)

Kriptografik xesh funksiyalar, bir tomonlama va siquvchi funksiyalar. Kalitsiz va kalitli xesh funksiyalar. MD5 xesh algoritmi. SHA oilasiga mansub xesh algoritmlar.

11-mavzu: Elektron raqamli imzo algoritmi (8 soat)

ERI mexanizmi, asosiy tushunchalar. RSA va El-Gamalga asoslangan ERI tizimlari. DSA standarti. GOST R 34.10-2012. Milliy ERI standarti.

12-mavzu: Ochik kalitlar infratuzilmasi

Ochiq kalitlarni ro'yxatga olish markazi. X.509 sertifikati. PKI oid standartlar (PKCS seriyasi).

13-mavzu: Kriptografiyaning zamonaviy sohalari (8 soat)

Bulutli hisoblashda kriptografik algoritmlardan foydalanish. Kvant kriptografiyasi. Biometrik – kriptografiya. Yengil kriptografik algoritmlar.

III. Amaliy mashg'ulotlar bo'yicha ko'rsatma va tavsiyalar

Amaliy mashg'ulotlar bo'yicha quyidagi mavzular tavsiya etiladi.

1. Bir qiymatli o'rniga qo'yishga asoslangan shifrlar tahlili hamda ularni CrypTool vositasi orqali amalga oshirish (4 soat).
2. N bitli skremblerni qurish va takrorlanish davrini hisoblash hamda ularni CrypTool vositasi orqali amalga oshirish (4 soat).
3. Chiziqli teskari aloqali registrlarni surishga asoslangan (LFSR) generatorlar va ularni CrypTool vositasi orqali amalga oshirish (4 soat).
4. Tasodifiy sonlar generatorlari va ularni CrypTool vositasi orqali tasodifiylikka tekshirish (4 soat).
5. Oqimli shifrlash algoritmlarini CrypTool vositasi orqali amalga oshirish (4 soat).
6. CrypTool vositasi orqali blokli shifrlar yordamida ma'lumotlarni shifrlash (4 soat).
7. CrypTool vositasi orqali ochiq kalitli shifrlash algoritmi yordamida ma'lumotlarni shifrlash (4 soat).
8. CrypTool vositasi orqali ma'lumotlarni xesh qiymatini hisoblash (4 soat).
9. CrypTool vositasi orqali ERI hosil qilish.
10. CrypTool vositasi orqali X.509 sertifikatini hosil qilish.

IV. Mustaqil ta'lim va mustaqil ishlar

Mustaqil ta'lim uchun tavsiya etiladigan topshiriqlar:

1. Tarmoqda uzatilayotgan axborot konfidensialligini ta'minlashda kriptografik algoritmlardan foydalanish holati..
2. Tarmoqda uzatilayotgan axborot yaxlitligini ta'minlashda kriptografik algoritmlardan foydalanish holati.

	3. Pollibiya kvadrati va affin tizimidagi Sezar usulining kriptotahlili. 4. Sigaba (SIGABA) shifrlash mashinasi va uning kriptotahlili. 5. Kriptografik himoya vositalarini ishlab chiqaruvchilar (Philips va Siemens misolida). 6. Twofish blokli shifrlash algoritmi va uning kriptotahlili. 7. Camellia blokli shifrlash algoritmi va uning kriptotahlili. 8. IDEA blokli shifrlash algoritmi va uning kriptotahlili. 9. GOST R 28147-89 blokli shifrlash algoritmi va uning kriptotahlili. 10. Salsa20 oqimli shifrlash algoritmi va uning kriptotahlili. 11. SHA2 oilasi xesh funksiyalari va ularning tahlili. 12. Blokcheyn texnologiyasining kriptografik asosi. 13. Tarmoqda uzatilayotgan axborot konfidensialligini ta'minlashda ochiq kalitli kriptografik algoritmlardan foydalanish holati. 14. Tarmoqda uzatilayotgan axborot yaxlitligini ta'minlashda ochiq kalitli kriptografik algoritmlardan foydalanish holati. 15. SSH protokoli va unda kriptografik algoritmlardan foydalanish holati. 16. Mamlakatimizda ochiq kalitlarni ro'yxatga olish markazlari va ularning vazifalari. 17. Ochiq kalitlar infratuzilmasi va uning asosiy maqsadi. 18. Ochiq kalitli kriptografik algoritmlardan bulutli hisoblash tizimlarida foydalanish. 19. Kvant kriptografiyasiga asoslangan kalitlarni taqsimlash protokollari. 20. Simmetrik va ochiq kalitli kriptografik tizimlarning ma'lumotlarni shifrlashdagi afzallik va kamchiliklari. 21. Gibrid shifrlash usullari va ularni qurish. 22. RSA ochiq kalitli shifrlash algoritmining kriptotahlili. 23. Diffi-Xelman kalitlarni ochiq taqsimlash protokoli va uning xavfsizlik tahlili. 24. Ochiq kalitli shifrlash algoritmlariga asoslangan autentifikatsiyalash protokollari.
3.	**V. Fan o'qitilishining natijalari (shakllanadigan kompetensiyalar)** Fanni o'zlashtirish natijasi talaba: • kriptografiyaning asosiy tushunchalarini aytib bera oladi; • kriptografiyani axborotni himoyalashdagi o'rnini tushuntirib bera oladi; • xesh funksiya va uni axborotni himoyalashdagi o'rnini tushuntira oladi; • shifrlarni yaratishda kriptografik akslantirishlardan foydalana oladi; • simmetrik kriptografiya himoya vositalaridan axborotni himoyalashda foydalana oladi; • ochiq kalitli kriptografik algoritmlardan amalda foydalana oladi; • ma'lumotlarni yaxlitligini ta'minlashda ERI algoritmlaridan amalda foydalana oladi; • simmetrik va ochiq kalitli shifrlash algoritmlarini dasturiy ta'minotini yaratish ko'nikmalariga ega bo'ladi;

	• elliptik egri chiziqlar va unga asoslangan algoritmlarni amaliyotda qo‘llay oladi; • kriptografiyaning zamonaviy sohalari haqida aytib bera oladi.
4.	**VI. Ta‘lim texnologiyalari va metodlari:** • ma‘ruzalar; • amaliy ishlarni bajarish va xulosalash; • interfaol keys-stadilar; • blits-so‘rov; • guruhlarda ishlash; • taqdimotlarni qilish; • jamoa bo‘lib ishlash va himoya qilish uchun lohiyalash.
5.	**VII. Kreditlarni olish uchun talabalar:** Fanga oid nazariy va uslubiy tushunchalarni to‘la o‘zlashtirish, tahlil natijalarini to‘g’ri aks ettira olish, o‘rganilayotgan jarayonlar haqida mustaqil mushohada yuritish va nazorat uchun berilgan vazifa va topshiriqlarni bajarish, yakuniy nazoratni topshirish.
6.	**Asosiy adabiyotlar** 1. Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography, Second Edition, CRC Press/ Taylor & Francis Group, Year: 2015. 2. Hans Delfs, Helmut Knebl. Introduction to Cryptography: Principles and Applications, Third Edition, Springer, Year: 2015, ISBN: 3662479737. 3. Mihir Bellare and Phillip Rogaway. Introduction to Modern Cryptography, 2005. 4. Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet. 5. Akbarov D. Y. “Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi” – Toshkent, 2008 – 394 bet. **Qo‘shimcha adabiyotlar** 6. James S. Kraft, Lawrence C. Washington. An Introduction to Number Theory with Cryptography, Second Edition, 2018, International Standard Book Number-13: 978-1-1380-6347-1 (Hardback). 7. Jeffrey Hoffstein, Jill Pipher Joseph, H. Silverman. An Introduction to Mathematical Cryptography, Second Edition, 2014, Springer New York Heidelberg Dordrecht London. 8. Lawrence C. Washington. Elliptic Curves Number Theory and Cryptography, Second Edition, 2008, International Standard Book Number-13: 978-1-4200-7146-7 (Hardcover). 9. Victor Shoup, A Computational Introduction to Number Theory and Algebra, creativecommons.org/licenses/by-nd-nc/3.0. 10. Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. An Introduction to Mathematical , Cryptography, January 19, 2015. 11. Kiberxavfsizlik asoslari: O‘quv qo‘llanma / S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: “Iqtisod-Moliya”, 2021. – 228 b.
7.	Fan dasturi Muhammad al-Xorazmiy nomidagi Toshkent axborot

	texnologiyalari universiteti Kengashining 2021-yil 29.04- 6/4 dagi -son bayonnomasi bilan tasdiqlangan.
8.	**Fan/modul uchun mas'ullar:** Z.T. Xudoykulov – TATU, "Kriptologiya" kafedrasi mudiri, PhD, dotsent. U.R. Mardiyev – TATU, "Kriptologiya" kafedrasi katta o'qituvchisi
9.	**Taqrizchilar** O.P. Axmedova - "UNICON.UZ" MCHJ - Fan-texnika va marketing tadqiqotlari markazi, Kriptografiya ilmiy tadqiqot bo'limi boshlig'i, t.f.n. O.M. Allanov - Kiberxavfsizlik va kriminalistika kafedrasi mudiri, t.f.f.d.(PhD), dotsent.