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

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

“TASDIQLAYMAN”
“Kiberxavfsizlik” fakulteti
dekani Sh.R. G‘ulomov
_____
2025-yil “___” _____

STEGONOGRAFIK ALGORITMLAR
fani bo‘yicha
SILLABUS

Bilim sohasi:	600000	– Axborot-kommunikatsiya texnologiyalari
Ta’lim sohasi:	610000	– Axborot-kommunikatsiya texnologiyalari
Ta’lim yo‘nalishi:	60611200	– Kiberxavfsizlik injiniringi
	60610300	– Axborot xavfsizligi (Axborot kommunikatsiya texnologiyalari va servis)

Toshkent – 2025

FAN SILLABUSI

Muhammad al-Xorazmiy nomidagi toshkent axborot texnologiyalari universiteti 60611200 – "Kiberxavfsizlik injiniringi" va 60610300 - Axborot xavfsizligi (Axborot kommunikatsiya texnologiyalari va servis) ta'lim yo'nalishlari

Fan nomi:	**Stegonografik algoritmlar**
Fan turi:	Tanlov fani
Fan kodi:	
Bosqich:	3
Semestr:	6
Ta'lim shakli:	Kunduzgi
Mashg'ulotlar shakli va semestrga ajratilgan soatlar:	180
Ma'ruza	42
Amaliy mashg'ulotlar	30
Laboratoriya mashg'ulotlari	-
Seminar	-
Mustaqil ta'lim	108
Sinov birligi miqdori:	6
Baholash shakli:	Imtixon
Fan tili:	O'zbek/rus

Fan maqsadi (FM)	
FM	talabalarga steganografiya, ya'ni ma'lumotni boshqa turdagi ma'lumotlar (matn, rasm, ovoz, video) ichiga yashirish san'ati va texnikalarini o'rgatish, uni kriptografiyaga muqobil fan sifatida tushuntirish, raqamli hujjatlar, tasvirlar va videolarni himoyalashda keng qo'llanilayotgan raqamli suv belgilarini (digital watermarking) yaratish va o'zgartirishlarga chidamli qo'shimcha ma'lumotni xavfsiz joylashtirish usullarini o'zlashtirishdan iborat.

Fanni o'zlashtirish uchun zarur boshlang'ich talablar	
1.	Yo'q.

Ta'lim natijalari (TN)	
TN1	steganografiyaning asosiy tushunchalari, axborot xavfsizligini ta'minlashda raqamli steganografiyaning o'rnini tushuntirib berish;

TN2	axborotni himoyalashda steganografiya usullari, zamonaviy steganografiya tizimlaridan amalda foydalana olish;
TN3	axborotni konteynerlar (tasvirlar, audiosignal, videotasvir)ga joylashtirish usullari va algoritmlarini qo‘llay olish;
TN4	axborot-kommunikatsiya tizimlarida steganografik axborotni asosiy manbalari va tashuvchilarini tushuntira olish hamda steganografik algoritmlardan foydalana olish;
TN5	steganografik tizimlarni stegoanaliz qilishning zamonaviy usullaridan foydalanish, stegonografiya algoritmlarining dasturlarini ishlab chiqish;
TN6	watermarking (raqamli beligilar)ni axborotni himoyalashda qo‘llanishi, watermarking tizimlari xususiyatlari va modellarini tavsiflab berish.

Fan mazmuni		
Mashg‘ulotlar shakli: ma’ruza (M)		**soat**
M1	**Stegonografik algoritmlar faniga kirish.** Steganografiya rivojlanishi, ahamiyati va qo‘llanilish sohalari. Steganografiyaning ta’riflari va asosiy terminlari. Steganografiya turlari va tizimlariga qo‘yiladigan talablar.	**2**
M2	**Raqamli signallar va ularga ishlov berish.** Analog – raqamli va raqamli-analog o‘zgartirgichlar, kvantlash, signal turlari: rasm (DFT, DCT, jpeg, png, gif), tovush (MP3, AAC) va video fayllar (MPEG-4, H.264, H.265) ni tasvirlash turlari, vaqt/makon sohalari, chastota sohasi, raqamli signallarni qayta ishlash dasturlari.	**4**
M3	**Ma’lumotni yashirish usullari.** Ma’lumotni grafik tasvirlarda yashirish usullari. Audio fayllarda ma’lumotlarni yashirish usullari. Video fayllarda ma’lumotlarni yashirish usullari.	**2**
M4	**Yashirin ma’lumotlarni matn, tasvirlarga joylashtirish algoritmlari.** Formatga asoslangan, lingvistik, tasodifiy va statistik generatsiyalash usullari. Rasmning fazoviy va chastota sohalarida ma’lumotlarni yashirish. Tasvirlarga joylashtirish algoritmlari.	**4**
M5	**Yashirin ma’lumotlarni audio signal va fayllarga joylashtirish algoritmlari.** Eng kam ahamiyatga ega bit, echo yashirish, juft kodlash, fazalarni kodlash, kengaytirilgan spektr.	**2**
M6	**Yashirin ma’lumotlarni video signal va fayllarga joylashtirish algoritmlari.** Eng kam ahamiyatga ega bit, echo yashirish, juft kodlash, fazalarni kodlash, kengaytirilgan spektr.	**4**
M7	**Tarmoq steganografiyasi.** TCP va IP segmentlarida ma’lumotlarning yashirin uzatish.	**2**
M8	**Stegotahlil usullari.** Stegonotahlil ketma-ketligi, ma’lumotni aniqlash, jinoiy sohalarda stegonotahlil. Statistik stegotahlil. Maqsadli stegotahlil. Ko‘r-ko‘rona stegotahlil. Steganografiyani aniqlash va tahlil qilish vositalari.	**4**

M9	**Steganografiya vositalari va ilovalar.** Ma'lumotni grafik tasvirlar, audio fayllar, video fayllar va tarmoq paketlariga yashirish vositalari va ilovalari.	**2**
M10	**Watermarking.** Watermarking rivojlanishi va qo'llanilish sohalari. Watermarking ta'riflari va asosiy terminlari. Watermarking tizimlari va xususiyatlari.	**2**
M11	**Watermarking modellari.** Aloqa tizimlari. Aloqaga asoslangan watermarking modeli, watermarkingning geometrik modellari.	**2**
M12	**Watermarking xavfsizlik muammolari.** Watermarking tizimlaridagi tahdid va zaifliklar. Watermarking tizimlariga qaratilgan hujumlar. Watermarking xafvsizligi va kriptografiya, kriptografik vositalar, kriptografiya va watermarking tizimlari orasidagi bog'liqlilik. Ruxsat etilmagan aniqlashdan himoyalash, ruxsat etilmagan qo'yishlardan himoyalash, ruxsat etilmagan o'chirib tashlashlardan himoyalash.	**2**
M13	**Qo'shimcha ma'lumotlar asosida watermarking.** Informativ biriktirish. Aniqlash ko'rsatkichini optimallashtirish, aniqlilik ko'rsatkichini optimallashtirish, informativ detektor, Dirty Paper kodlari.	**2**
M14	**Xatoliklarni tahlillash.** Xabar xatoliklari, yolg'ondan qabul qilish, yolg'ondan rad etish, xatoliklarga ta'sir qiluvchi parametrlar, ROC egri chizig'i.	**2**
M15	**Kontent autentifikatsiyasi.** Aniq autentifikatsiya, mo'rt watermarking tizimlari. Belgi qo'yish jarayoni imzolari, o'chirib tashlash mumkin bo'lgan watermarking tizimlari. Tanlovli autentifikatsiya, qonuniy va noqonuniy buzulishlar, yarim-mo'rt watermarking tizimlar.	**2**
M16	**Qalbakilikni aniqlash – kriminalistika usullari.** Optika, formatga asoslangan, geometrik, xromatik, statistik, pikselga asoslangan, CFA va demozaika, kamera javob funksiyasi va CRF, PRNU, mashinali o'qitish va JPEG.	**2**
M17	**Raqamli watermarking ilovalari.** Ma'lumotni grafik tasvirlar, audio fayllar, video fayllar va tarmoq paketlariga yashirish vositalari va ilovalari. Watermarking vositalari va ilovalari.	**2**
	Jami	**42**

Mashg'ulotlar shakli: amaliyot (A)		**soat**
A1	Audio signal va fayllarda ma'lumotlarni yashirish.	**4**
A2	Video signal va fayllarda ma'lumotlarni yashirish.	**4**
A3	Fayl tizimlarida va tarmoq paketlarida ma'lumotlarni yashirish.	**4**
A4	Himoyalangan hujjat, fayllarni buzish usullari va vositalaridan foydalanish.	**4**
A5	O'chirilgan fayllar va o'chirilgan bo'limlarni tiklash.	**2**

A6	Quick Stego dasturidan foydalanilgan holda ma'lumotlarni yashirish.	**2**
A7	OpenPuff dasturidan foydalanilgan holda ma'lumotlarni yashirish.	**4**
A8	Rasmda mualliflik huquqini ko'rsatuvchi watermark belgisini qo'yish va ma'lumotlarni yashirish.	**2**
A9	Axborotni kriptografik va stegonografik himoyasini ta'minlovchi vositani ishlab chiqish.	**4**
	Jami	**30**
	Mustaqil ish mavzulari (MI)	**soat**
Quyidagi mavzulardan ikkitasi bo'yicha mustaqil ish tayyorlanadi va topshiriladi.		*40*
M1	Amalda qo'llanilayotgan watermarking va stegonografiya ilovalarining tahlili.	
M2	Reed Solomon xatoliklarni tuzatish kodininh tahlili.	
M3	Stegonografik tizimlarga qaratilgan hujumlar.	
M4	Axborotning kriptografik himoyasi.	
M5	Kompyuter stegonografiyasi tarixi.	
M6	Tarmoq stegonografiyasi va uni amalga oshirish usullari.	
M7	Stegonografik algoritmlarning klassifikatsiyasi.	
M8	Stegonografik tizimlar ishlashida xatolik turlari.	
M9	Stegonografik tizimlarning kelajagi.	
M10	Video kontentda ma'lumotlarni yashirish usullari.	
M11	Rasm kontentda ma'lumotlarni yashirish usullari.	
Quyidagi mavzulardan biri bo'yicha taqdimot materiali tayyorlanadi va topshiriladi.		*48*
M12	MATLAB dasturini o'rnatish va unda rasm ma'lumotlar bilan ishlash ko'nikmalarini hosil qilish.	
M13	Xiao steganography stegonografik dasturiy vositasidan foydalanish.	
M14	Image steganography stegonografik dasturiy vositasidan foydalanish.	
M15	Steghide stegonografik dasturiy vositasidan foydalanish.	
M16	Crypture stegonografik dasturiy vositasidan foydalanish.	
M17	SteganographX Plus stegonografik dasturiy vositasidan foydalanish.	
M18	rSteg stegonografik dasturiy vositasidan foydalanish.	
M19	SSuite Picsel stegonografik dasturiy vositasidan foydalanish.	
Ma'ruza va amaliy mashg'ulotlarga tayyorgarlik ko'rish va berilgan topshiriqlarni bajarish.		*20*
	Jami	**108**

Talabaning fan bo'yicha o'zlashtirish ko'rsatkichini nazorat qilishda quyidagi mezonlar tavsiya etiladi:

a) 5 baho «a'lo» (90-100) olish uchun talabaning bilim darajasi quyidagilarga javob berishi lozim:

talaba mustaqil xulosa va qaror qabul qiladi, ijodiy fikrlay oladi, mustaqil mushohada yuritadi, olgan bilimini amalda qo'llay oladi, fanning (mavzuning) mohiyatini tushunadi, biladi, ifodalay oladi, aytib beradi hamda fan (mavzu) bo'yicha tasavvurga ega.

b) 4 baho «yaxshi» (70-89) olish uchun talabaning bilim darajasi quyidagilarga javob berishi lozim:

talaba mustaqil mushohada yuritadi, olgan bilimini amalda qo'llay oladi, fanning (mavzuning) mohiyatni tushunadi, biladi, ifodalay oladi, aytib beradi hamda fan (mavzu) bo'yicha tasavvurga ega.

d) 3 baho «qoniqarli» (60-69) olish uchun talabaning bilim darajasi quyidagilarga javob berishi lozim:

talaba olgan bilimini amalda qo'llay oladi, fanning (mavzuning) mohiyatni tushunadi, biladi, ifodalay oladi, aytib beradi hamda fan (mavzu) bo'yicha tasavvurga ega deb topilganda.

e) quyidagi hollarda talabaning bilim darajasi qoniqarsiz 2 baho (0-59) bilan baholanishi mumkin:

talaba fan dasturini o'zlashtirmagan, fanning (mavzuning) mohiyatini tushunmaydi hamda fan (mavzu) bo'yicha tasavvurga ega emas.

Reyting baholash turlari	**%**	**O'tkazish vaqti**
Oraliq nazorat:	**50**	
Amaliy mashg'ulotlarda faolligi, savollarga to'g'ri javob berganligi, amaliy topshiriqlarni bajarganligi uchun: • 1-amaliy ish uchun: 2% • 2-amaliy ish uchun: 2% • 3-amaliy ish uchun: 3% • 4-amaliy ish uchun: 3% • 5-amaliy ish uchun: 3% • 6-amaliy ish uchun: 3% • 7-amaliy ish uchun: 3% • 8-amaliy ish uchun: 3% • 9-amaliy ish uchun: 3%	25	Semestr davomida
Yozma ish (ma'ruzachi o'qituvchi tomonidan qabul qilinadi)	10	O'quv grafik asosida
Mustaqil ta'lim topshiriqlarining o'z vaqtida va sifatli bajarilishi: • mustaqil ish (2 ta): 8% • prezentatsiya tayyorlash (1marta): 7%	15	Semestr davomida

Yakuniy nazorat		**50**	O‘quv grafik asosida
	Jami:	**100**	
Asosiy adabiyotlar			
1.	Shih F. Y. Digital watermarking and steganography: fundamentals and techniques. – CRC press, 2017.		
2.	Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker. Digital Watermarking and Steganography, the Morgan Kaufmann Series in Multimedia Information and Systems, 2nd Ed., 2007.		
3.	Katzenbeisser S., Petitcolas F. Information hiding. – Artech house, 2016.		
Tavsiya qilinadigan qo‘shimcha adabiyotlar			
1.	Peter Wayner, (2008). Disappearing Cryptography, Second Edition - Information Hiding: Steganography and Watermarking, Morgan Kaufmann.		
2.	Bruce Schneier, (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C, second Edition, John Wiley & Sons.		
3.	Компьютерная стеганография. Г.Ф.Конахович, А.Ю.Пузыренко. «МК-Пресс» Киев, 2006.		
4.	Курс современной стеганографии. Учебник. 3-издание. А.Ю.Пигарев. ООО “Издательство ЮЖЭА”, 2002. -120 ст.		
Internet saytlari			
1.	http://ru-steganography.narod.ru/		
2.	http://learncryptography.com/steganography/		
3.	http://forensicswiki.org/wiki/Steganography/		
4.	https://resources.infosecinstitute.com/topic/steganography-and-tools-to-perform-steganography/		

Fan o‘qituvchisi to‘g‘risida ma’lumot

Dastur mualliflari:	Xamidov Sherzod Jaloldin o‘g‘li
E-mail:	sherzod.hamidov@tuit.uz
Tashkilot:	Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti, “Kriptologiya” kafedrasi.
Taqrizchilar:	Allanov O.M. – Muxammad Al-Xorazmiy nomidagi TATU, “Kiberxavfsizlik va kriminalistika” kafedrasi mudiri, PhD (turdosh OTM). Axmedova O.P. – Fan texnika va marketing tadqiqotlari markazi – “UNICON.UZ” MCHJ Axborot xavfsizligi va kriptologiya Ilmiy-tadqiqot bo‘limi boshlig‘i, t.f.n. (turdosh ITM).

Mazkur Sillabus Universitet Kengashining 20__-yil _____dagi _____-sonli yig‘ilish bayoni bilan tasdiqlangan.

Mazkur Sillabus “Kriptologiya” kafedrasining 2025-yil 11.04 dagi 17-sonli yig‘ilish bayoni bilan ma’qullangan.

O‘quv-uslubiy boshqarma boshlig‘i	A.K. Ergashev
Fakultet dekani	Sh.R. G‘ulomov
Kafedra mudiri	Z.T. Xudoykulov
Tuzuvchi	Sh.J. Xamidov