ЎЗБЕКИСТОН РЕСПУБЛИКАСИ
ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

МИРЗО УЛУҒБЕК НОМИДАГИ
ЎЗБЕКИСТОН МИЛЛИЙ УНИВЕРСИТЕТИ

“ТАСДИҚЛАЙМАН”
(МУМ ректори)
2021 йил “25” август

КРИПТОТАҲЛИЛ ЭЛЕМЕНТЛАРИ

ФАН ДАСТУРИ

Билим соҳаси:	600 000 – Ахборот-коммуникация технологиялари
Таълим соҳаси:	610 000 – Ахборот-коммуникация технологиялари
Таълим йўналиши:	60610300 – Ахборот хавфсизлиги *(соҳалар бўйича)*

Тошкент – 2021

Фан/модуль коди	Ўқув йили	Семестр	ECTS - Кредитлар
KREB407	2024-2025	7	7
Фан/модуль тури	**Таълим тили**		**Ҳафтадаги дарс соатлари**
Мажбурий	Ўзбек		6

	Фаннинг номи	Аудитория машғулотлари (соат)	Мустақил таълим (соат)	Жами юклама (соат)
1.	**Криптотаҳлил элементлари**	90	120	210

2. I. Фаннинг мазмуни

Фанни ўқитишдан мақсад – содда шифрлаш алгоритмлари калитларини аниқлаш ёки уларнинг нозик томонларини топиш ҳамда шифрланган маълумотларни дешифрлаш имкониятларини яратиш малакасини шакллантиришдан иборат.

Фаннинг вазифаси – шифр матнни дешифрлаш масалаларида бирор алгоритмнинг математик модели хусусиятларини ҳисобга олган ҳолда криптотаҳлилни қўллаш кўникмаси ва малакасини ҳосил қилишдан иборат.

II. Асосий назарий қисм (маъруза машғулотлари)

II.I. Фан таркибига қуйидаги мавзулар киради:

1-мавзу. Криптотаҳлил ҳақида дастлабки маълумотлар.

Асосий тушунчалар. Шифрлар классификациялари.

2- мавзу. Шифрларнинг криптобардошлиги ва уларнинг таҳлили.

Шифрларнинг криптобардошлиги. Замонавий ҳамда самарали натижа берадиган криптотаҳлил усуллари.

3-мавзу. Криптотизмларга қўйиладиган талаблар ва бардошлилик.

Криптотизимларга қўйиладиган талаблар. Криптографик тизимларнинг назарий бардошлилиги. Мутлақо махфийлик. Мутлақо махфийликни таъминловчи криптотизимларнинг калитларига қўйиладиган талаблар.

4-мавзу. Ўрнига қўйиш шифрлари.

Ўрнига қўйиш шифрлари. Аддитив шифр бўйича шифрлаш. Мультипликатив шифрлар.

5-мавзу. Бир алифболи ўрнига қўйиш шифри.

Аффин шифрлари. Бир алифболи (моноалифболи) ўрнига қўйиш шифри.

6-мавзу. Кўп алифболи ўрнига қўйиш шифри.

Кўп алифболи ўрнига қўйиш шифри. Автокалитли шифр. Леон Батиста Альберти шифри. Хиллнинг кўп алифболи шифри.

7-мавзу. Виженер шифри.

Виженер шифри бўйича шифрлаш ва дешифрлаш.

8-мавзу. Гаммалаштириш ва ўрин алмаштириш шифрлаш алгоритмлари.

Гаммалаштириш ва ўрин алмаштириш шифрлаш алгоритмлари.

Гаммалаштириш ва ўрин алмаштириш бўйича шифрланган маълумотларни дешифрлаш.

9-мавзу. Оддий ўрнига қўйиш шифрлаш алгоритмларининг криптотаҳлили.

Ўрнига қўйиш шифрлаш алгоритмларининг криптотаҳлили. Частотавий таҳлил усули.

10-мавзу. Оддий ўрнига қўйиш шифрлаш алгоритмларининг криптотаҳлили.

Ўрнига қўйиш шифрлари билан шифрланган ўзбек тилидаги матнларни криптотаҳлили. Очиқ матнда учраши мумкин бўлган эҳтимоллик сўзлардан фойдаланиш усули.

11-мавзу. Кўп алифболи ўрнига қўйиш шифрлари криптотаҳлили.

Калит узунлигини аниқлаш усуллари. Казиски тести. Бир нечта калитга эга бўлган кўп алифболи ўрнига қўйиш шифри.

12-мавзу. Ўрин алмаштириш шифрларининг криптотаҳлили.

Ўрин алмаштириш криптограммалари таҳлили. Устун ва сатрлар бўйича криптотаҳлилни амалга ошириш.

13-мавзу. Очиқ маълумотларни ифодаловчи мавжуд моделлар таҳлили.

Очиқ матннинг математик модели. Очиқ матнларни моделларидан фойдаланиб, шифрматнларни таҳлили.

14-мавзу. RSA криптотизимига нисбатан ҳужумлар ташкил қилиш.

RSA криптотизими ёпиқ шифрлаш калитини билмасдан, шифрланган матндан очиқ матнни тиклаш. Шифрматнни танлашга асосланган ҳужум. RSA криптотизимига Винер ҳужуми. Бир неча фойдаланувчиларга бир хил хабарни жўнатишга асосланган ҳужум.

15-мавзу. RSA рақамли имзосига ҳужумлар ташкил қилиш.

	Нотариус схемаси бўйича RSA рақамли имзосига ҳужум уюштириш. Танланган шифрматн бўйича RSA рақамли имзосига ҳужум уюштириш. RSA криптотизими ва рақамли имзоси хавфсизлигини таъминлаш учун таклиф қилинадиган тавсиялар. **III. Амалий машғулотлари буйича кўрсатма ва тавсиялар** Амалий машғулотлар учун қуйидаги мавзулар тавсия этилади: 1. Шифрларни классификациялаш оид мисоллар. 2. Тарихий шифрларнинг криптобардошлиги ва уларнинг таҳлили. Содда криптографик тизимларга қўйиладиган талаблар ва бардошлилик. 3. Аддитив шифр бўйича шифрлаш. Мультипликатив шифрлар. 4. Бир алифболи ўрнига қўйиш шифрлари. Кўп алифболи ўрнига қўйиш шифри. 5. Автокалитли шифр. Леон Батиста Альберти шифри. 6. Хиллнинг кўп алифболи шифри. 7. Виженер шифри бўйича шифрланган маълумотларни дешифрлаш. 8. Гаммалаштириш ва ўрин алмаштириш бўйича шифрланган маълумотларни дешифрлаш. 9. Ўрнига қўйиш шифрлаш алгоритмларининг криптотаҳлили. Частотавий таҳлил усули. 10. Ўрнига қўйиш шифрлари билан шифрланган ўзбек тилидаги матнларни криптотаҳлили. 11. Очиқ матнда учраши мумкин бўлган эҳтимоллик сўзлардан фойдаланиш усули. Очиқ матннинг математик модели. Очиқ матнларни моделларидан фойдаланиб, шифрматнларни таҳлили 12. Кўп алифболи ўрнига қўйиш шифрларининг калит узунлигини аниқлаш усуллари. Казиски тести. 13. Ўрин алмаштириш шифрларининг криптотаҳлили. 14. RSA криптотизими ёпиқ шифрлаш калитини билмасдан, шифрланган матндан очиқ матнни тиклаш. Шифрматнни танлашга асосланган ҳужум. 15. Танланган шифрматн бўйича RSA рақамли имзосига ҳужум уюштириш. **IV. Лаборатория иши машғулотлари бўйича кўрсатма ва тавсиялар** Лаборатория иши машғулотлари учун қуйидаги мавзулар тавсия этилади:

	1. Частотавий таҳлил усули асосида ўрнига қўйиш шифрлаш алгоритмларининг криптотаҳлили. 2. Калит узунлигини аниқлаш усуллари ва Казиски тестидан фойдаланиб, кўп алифболи ўрнига қўйиш шифрлари криптотаҳлили. 3. Ўрин алмаштириш шифрларининг криптотаҳлили. 4. Очиқ матнларни моделларидан фойдаланиб, шифрматнларни таҳлили. 5. RSA криптотизимига нисбатан ҳужумлар ташкил қилиш. 6. RSA рақамли имзосига ҳужумлар ташкил қилиш. **V. Мустақил таълим ва мустақил ишлар** Мустақил таълим учун тавсия этиладиган мавзулар: 1. Модуляр арифметика ва силжитиш шифрлари. 2. Сонлар назариясидан айрим маълумотлар. 3. Мураккаб алмаштиришли шифрлар. 4. Гамильтон маршрутларига асосланган шифрлаш. 5. Шеннон назарияси. 6. Энтропия ва ундан криптологияда фойдаланиш бўйича қўшимча маълумотлар. 7. Энтропия - аниқмаслик даражасининг ўлчови. Мураккаб ходисалар энтропияси. Шартли энтропия. 8. Тилнинг энтропияси ва тўлалиги. Ягоналик масофаси. 9. Криптотаҳлилда эҳтимоллик назарияси ва статистиканинг қўлланилиши. 10. Очиқ матнларни танлашда энтропиянинг роли. 11. Маъноли очиқ матн энтропиясини аниқлаш усули. 12. Қалбаки калитлар ва ягоналик масофаси. Мустақил ўзлаштириладиган мавзулар бўйича талабалар томонидан рефератлар тайёрлаш ва уни тақдимот қилиш тавсия этилади.
3.	**VI. Фан ўқитилишининг натижалари (шаклланадиган компетенциялар)** Фанни ўзлаштириш натижасида талаба: • ўрнига қўйиш ва ўрин алмаштириш шифрлаш алгоритмларининг криптотаҳлили, шифрлаш алгоритмларининг криптобардошлиги, Виженер шифрининг криптоаҳлили ***ҳақида тасаввурга эга бўлиши;*** • тарихий шифрлаш алгоритмлари, ўрнига қўйиш ва ўрин алмаштириш шифрлаш алгоритмларининг криптотаҳлили, частотавий таҳлил усули, очиқ матнда учраши мумкин бўлган эҳтимоллик сўзлардан фойдаланиш усули, очиқ матнларни аниқлаш критериялари, Виженер шифрининг криптоаҳлилини қўллаш ва амалиётда улардан фойдалана олиш ***кўникмаларига эга бўлиши;*** • шифрматн алифбосини ва шифрматн тилини аниқлаш, очиқ

	матнларни аниқлаш, шифрлаш алгоритмларининг заиф томонларини аниқлаш ва тарихий шифрлаш алгоритмларининг калитларини аниқлаш ***малакаларига эга бўлиши керак.***
4.	**VII. Таълим технологиялари ва методлари:** •маърузалар; •интерфаол кейс-стадилар; •амалий ва лаборатория машғулотлари (мустақил мантиқий фикрлаш, мавзуга оид муаммоларга тезкор ечим топиш); •гуруҳларда ишлаш; •тақдимотларни қилиш; •индивидуал лойиҳалар; •жамоа бўлиб ишлаш ва ҳимоя қилиш учун лойиҳалар.
5.	**VIII. Кредитларни олиш учун талаблар:** Фанга оид назарий ва услубий тушунчаларни тўла ўзлаштириш, таҳлил натижаларини тўғри акс эттира олиш, ўрганилаётган жараёнлар ҳақида мустақил мушохада юритиш ва жорий, оралиқ назорат шаклларида берилган вазифа ва топшириқларни бажариш, якуний назорат бўйича ёзма ишни топшириш.
6.	**Асосий адабиётлар** 1. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши. –Т., Ўзбекистон маркаси. 2009. -432 б. 2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А.В. Основы криптографии: Учебное пособие, 2-е изд. –М.: Гелиос АРВ, 2002.- 480 с. 3. Пилиди В.С. В.С. Криптография. Вводные главы. Электронное учебное пособие. –Ростов-на-Дону, 2009. –110 с. **Қўшимча адабиётлар** 4. Дроботова А.В., Ерохин Е.А., Михайлов А.С. Традиционные симметричные криптосистемы. Лабораторный практикум по курсу «Информационный обмен в сетях». М.: МИФИ, 2002. - 68 с. 5. Жданов О.Н., Куденкова И.А. Криптоанализ классических шифров. –Красноярск, 2008. – 107 с. 6. Шеннон К. Э. Теория связи в секретных системах. В кн.: Шеннон К.Э. Работы по теории информации и кибернетике. М.: ИЛ, 1963, том 1. - С. 333-402. **Ахборот манбаалари** 1. www.intuit.ru 2. www.kripto.ru

	3. www.securityfocus.com 4. www.sans.org 5. www.xforce.iss.net 6. www.packetfactory.net-сайт 7. blacksun.box.sk 8. www.phrack.com 9. www.cerias.purdue.edu
7.	Мирзо Улуғбек номидаги Ўзбекистон Миллий университети томонидан ишлаб чиқилган. ЎзМУ Кенгашининг 2021 йил "25" августдаги 1 -сон баённомаси билан тасдиқланган.
8.	**Фан/модуль учун масъуллар:** Г.У.Жўраев – ЎзМУ, "Ахборот хавфсизлиги" кафедраси мудири физика-математика фанлари доктори; Б.Д.Фармонов – ЎзМУ, "Ахборот хавфсизлиги" кафедраси ўқитувчиси
9.	**Тақризчилар:** Ж.Х. Джуманов – Муҳаммад ал-Хоразмий номидаги Тошкент Ахборот технологиялари университети "Компьютер тизимлари" кафедраси мудири, т.ф.д. А.В.Кабулов – Мирзо Улуғбек номидаги Ўзбекистон Миллий университети "Ахборот хавфсизлиги" кафедраси профессори, т.ф.д.