«Әл-Фараби атындағы ҚазҰУ»
КЕАҚ Ғылыми кеңес отырысында
11.06.2024 ж. №11 хаттамамен
БЕКІТІЛДІ

D195 – «Криптология» білім беру бағдарламалары тобына докторантураға түсушілерге арналған емтихан бағдарламасы

I. Жалпы ережелер

1. Бағдарлама «Жоғары және жоғары оқу орнынан кейінгі білімнің білім беру бағдарламаларын іске асыратын білім беру ұйымдарына оқуға қабылдаудың үлгілік қағидаларын бекіту туралы» Қазақстан Республикасы Білім және ғылым министрінің 2018 жылғы 31 қазандағы № 600 бұйрығына (бұдан әрі – үлгілік қағидалар) сәйкес жасалды.

2. Докторантураға түсу емтиханы сұхбаттасудан, эссе жазудан және білім беру бағдарламалары тобының бейіні бойынша емтиханнан тұрады.

Блогы	Балы
1. Сұхбаттасу	30
2. Эссе	20
3. Білім беру бағдарламасы тобының бейіні бойынша емтихан	50
Барлығы/ өту ұпайы	100/75

3. Түсу емтиханының ұзақтығы – 3 сағат 10 минут, осы уақыт ішінде оқуға түсуші эссе жазады, электрондық емтихан билетіне жауап береді. Сұхбаттасу ЖОО қабылдау емтиханының алдында өткізіледі.

II. Түсу емтиханын өткізу тәртібі

1. D195 – «Криптология» білім беру бағдарламалары тобына докторантураға түсушілер проблемалық / тақырыптық эссе жазады. Эссе көлемі – 250 сөзден кем болмауы керек.

Эссе мақсаты – теориялық білімге, әлеуметтік және жеке тәжірибеге негізделген өз аргументациясын құрастыру қабілетінде көрініс табатын аналитикалық және шығармашылық қабілеттер деңгейін анықтау.

Эссенің түрлері:

- зерттеу қызметіне ынталандырушы себептерді ашатын мотивациялық эссе;
- жоспарланған зерттеудің өзектілігі мен әдістемесін негіздейтін ғылыми-аналитикалық эссе;
- пәндік саладағы ғылыми білімнің әртүрлі аспектілерін көрсететін проблемалық/тақырыптық эссе.

2. Электрондық емтихан билеті 3 сұрақтан тұрады.

Білім беру бағдарламасы тобының бейіні бойынша емтиханға дайындалуға арналған тақырыптар

«Ақпараттық қауіпсіздік жүйелерін ұйымдастыру» пәні

Тақырыбы: Криптоанализ

Тақырыпшалар:

1. Классикалық шифрлар және оларды ашу. Ығыстыру және аффиндық шифрлар олардың дешифралу және теру (перебор) әдісімен ашу. Ауыстыру шифрын ашудың жиілікті әдісі. Классикалық шифрлардың кемшіліктері, орыс және қазақ тіліндегі мәтіндердің жиілікті талдауы.
2. Бүтін сандар сақинасы, Евклид алгоритмы және салдарылары. Салыстыру теориясы. Модуль бойынша салыстурылардың қасиеттері. Модуль бойынша түрленетін элементтер.
3. Эйлер функциясы және оның қасиеттері. Жай сандардан Эйлер функциясының мәндері. Эйлер функциясының мультипликативтігі туралы теорема. Эйлер функциясының мәндерін табу формуласы. Эйлер функциясының көмегімен дәрежеге шығару.
4. Ферма-Эйлер теоремасы және RSA шифрдың негізгі теоремасы.
5. RSA-шифр, шифрлеу және оқу процестері, негіздемесі. Берілген мәтіннің ашық кілтімен RSA-шифрлеу. Берілген мәтіннің жабық кілтімен RSA-дешифрлеу.
6. RSA-электрндық қолтаңбасы, мәні және негіздеуі.
7. RSA-электрондық қолтаңба процедурасының жүзеге асырылуы, электрондық қолтаңбамен құжатқа қолтаңба қою бөлігі.
8. RSA-электрондық қолтаңба процедурасының жүзеге асырылуы, қолтаңбаны ашық кілтпен шифрлеу бөлігі.
9. Натурал сандар тізбегінде жай сандардың үлестірілуі және RSA шифрді бағалау.
10. < F2 ; +,* > өрісіндегі көпмүшеліктер сақинасы, Евклид алгоритмі, екі көпмүшеліктің ең үлкен ортақ бөлгішін көрсету. Осы сақинадағы келтірілмейтін көпмүшеліктер. 2,3,4,5 дәрежелі келтірілмейтін көпмүшеліктер.
11. < F2n ; +,* > өрісін келтірілмейтін көпмүшеліктің модуль бойынша қалдықтарынан құралған өріс ретінде қалыптастырылуы. Осы өрістегі қосу және көбейту амалдары. Осы

өрістің нөлдік емес элементтері үшін қосу бойынша және көбейту бойынша кері элементтер. < F16 ; +, * > өрісін құрастыру.

12. Топ ретінің ішкі топ ретіне бөлінуі туралы Лагранж теоремасы. Элементтің реті топтың ретін бөлетіні туралы салдар. Zn тобының ішкі топтарының мысалдары. < F2n ; +,* > өрісіндегі бастапқы элемент туралы теорема. < F16 ; +,* > өрісінің бастапқы элементтері.
13. n-разрядті екілік блоктардан жасалған өрісінің құрылымы. Осы өрісте қосу мен көбейту амалдарын беру. Осы өрістің нөлдік емес элементтері

үшін қосу және көбейту амалдары бойынша кері элементтер. 4-разрядты екілік блоктардан өрісті құру, осы өрістің бастапқы элементтерін көрсету.

14. Дифи-Хеллман есебі. Дифи-Хеллман есебінің «шешілмеушілігіне» сүйеніп, қашықтағы қолданушылар үшін ортақ құпияны құру. Қашықтағы қолданушылар үшін кілттер алмасу мәселесінің шешімі.

15. Эль-Гамаль шифры, кілттермен алмасу, шифрлеу және дешифрлеу процестері. Жүзеге асыру мысалы.

«Компьютерлік ақпаратты қорғаудың әдістері мен құралдары» пәні

Тақырыбы: Ақпаратты шифрлаудың модельдері мен әдістері

Тақырыпшалар:

1. Криптология әдістерінің шығуы мен дамуы туралы қысқаша тарихи ақпарат. Криптография. Құпиялылық. Тұтастық. Аутентификация. Сандық қолтаңба.

2. Белл-Лападула моделі. Кілттердің алдын ала таратылуы. Кілттерді жіберу. Кілттерді ашық тарату. Құпияны бөлісу схемасы. Ашық кілттер инфраструктурасы. Сертификаттар. Сертификациялау орталықтары. Шифрлердің формальді модельдері. Ашық мәтіндер модельдері. Ашық мәтіннің математикалық модельдері. Ашық мәтінді тану критерийлері. Шифрлерді әртүрлі көрсеткіштер бойынша жіктеу. Ауыстыру шифрінің математикалық моделі. Ауыстыру шифрлерін жіктеу.

3. Low-Water-Mark (LWM) моделі. Бағдарлық алмастырулар. Алмастыру шифрлерін криптоталдау элементтері. Ауыстыру шифрлері.

4. J. Goguen, J. Meseguer модельдері. Кестелік гаммалау. Гамма таңбаларының ықти- малдықтарын қалпына келтіру мүмкіндігі туралы. Әртүрлі ықтималдықты гаммамен шифрленген мәтіндерді қалпына келтіру. Гамманы қайталап пайдалану. Виженер шифрін криптоталдау. Шифрлеушінің қателері.

5. Қауіпсіздіктің бұзылуын анықтау моделі. Энтропия және тіл артықтығы. Жалғыздық арақашықтығы. Шифрлердің беріктігі. Шифрлердің теориялық беріктігі. Шифрлердің практикалық беріктігі. Шифрлердің имитациялық беріктігі. Бұрмалауды таратпайтын шифрлер. «Таңбаларды ауыстыру» бұрмалауын таратпайтын шифрлер. «Таңбаларды тастап кету-кірістіру» бұрмалауын таратпайтын шифрлер.

6. Блоктық шифрлеу жүйелері. Блоктық шифрлерді құру принциптері. Блоктық шифрлер мысалдары. DES мәліметтерді шифрлеудің американдық стандарты. ГОСТ 28147-89 мәліметтерді шифрлеу стандарты. Блоктық шифрлерді пайдалану режимдері. Блоктық шифрлеу алгоритмдерін аралас пайдалану. Блоктық шифрлеу алгоритдерін талдау әдістері. Блоктық шифрлеу алгоритмдерін пайдалану бойынша ұсыныстар.

7. Шифрлеудің ағымдық жүйелері. Ағымдық шифржүйелерді синхронизациялау. Ағымдық шифржүйелерді құру принциптері. Ағымдық шифржүйелердің мысалдары. A5 шифржүйесі. Гиффорд шифржүйесі. Сызықтық ығыстыру регистрлері. Берлекемп- Месси алгоритмі. Сызықтық

рекуррентті тізбектердің күрделенуі. Сүзгі генераторлар. Қиыстырушы генераторлар. Сызықтық ығыстыру регистрлерін композициялау. Рекурсия заңы динамикалық өзгеретін сұлбалар. Жады элементтері бар сұлбалар. Ағымдық шифрлерді талдау әдістері.

8. Қауіпсіздікті басқару. Стандарттар, қауіпсіздік аудиты. Сөйлеу сигналдарының ерекшеліктері. Скремблерлеу. Сигналдың жиілікті түрленулері. Сигналдық мерзімдік түрленулері. Мерзімдік алмастырулар жүйелерінің беріктігі. Сандық телефония жүйелері.

9. Ашық кілтті шифрлеу жүйелері. RSA шифржүйесі. Эль-Гамаль шифржүйесі. Мак-Элис шифржүйесі. "Рюкзак мәселесі" негізіндегі шифржүйе.

10. Идентификациялау. Құпия сөздерді құру ережелері. Құпия сөздерді тексеру рәсімдерін күрделендіру. Құпия тіркестер. Тиянақталған құпия сөздерге шабуыл. Құпия сөздерді қайталап пайдалану. Құпия сөздерді толықтай теріп шығу. Сөздік көмегімен шабуылдау. Жеке идентификациялау нөмірлері. Бір реттік құпия сөздер. “Сұрақ-жауап” (күшті идентификациялау). Симметриялық шифрлеу алгоритмдерін пайдаланып “сұрақ-жауапты” жүзеге асыру. Ассимметриялық шифрлеу алгоритмдерін пайдаланып “сұрақ-жауапты” жүзеге асыру. Нөлдік білімі бар хаттамалар. Идентификация хаттамаларына шабуыл.

11. Криптографиялық хеш функциялар. Хэштеу функциялары мен мәліметтер тұтастығы. Кілттік хэштеу функциялары. Кілтсіз хэштеу функциялары. Мәліметтердің тұтастығы және хабарлардың аутентификациясы. Хэштеу функцияларына ықтимал шабуылдар.

12. Сандық қолтаңбалар. Жалпы тұжырымдар. Ашық кілтті шифржүйелер негізіндегі сандық қолтаңбалар. Фиат–Шамир сандық қолтаңбасы, Эль-Гамаль сандық қолтаңбасы. Бір реттік сандық қолтаңбалар.

13. Кілттерді тарату хаттамалары. Симметриялық шифрлеуді пайдаланып кілттерді тапсыру. Екіжақты хаттамалар. Үштарапты хаттамалар. Асимметриялық шифрлеуды пайдаланып кілттерді тапсыру. Сандық қолтаңбаны пайдаланбайтын хаттамалар. Сандық қолтаңбаны пайдаланатын хаттамалар. Ашық кілт сертификаттары. Кілттерді ашық тарату. Кілттерді алдын ала тарату. Байланыс желісінде кілттерді алдын ала тарату схемалары. Құпия бөлісу схемалары. Конференцбайланысқа арналған кілттерді белгілеу әдістері. Кілттерді тарату хаттамаларына ықтимал шабуылдар.

14. Кілттерді басқару. Кілттердің өмірлік циклі. Сенімді үшінші тарап ұсынатын қызметтер. Уақыт белгілерін орнату. Сандық қолтаңбаларды нотаризациялау.

15. Шифржүйелерді пайдаланудың кейбір практикалық аспектілері. Хабарламалар ағымын талдау. Операторлар қателері. Шифржүйелерді пайдалану кезіндегі физикалық және ұйымдастырушылық іс-шаралар. Кілттерді ашық таратудың кванттық криптографиялық хаттамасы. Кванттық арна және оның қасиеттері. Кілттерді ашық тарату хаттамасы.

«Ақпаратты қорғау құралдарының элементтері» пәні

Тақырыбы: Компьютерлік жүйелер туралы ақпаратты қорғау

Тақырыпшалар:

1. Компьютерлік жүйе (КЖ). Негізгі түсініктер. Электрондық құжат (ЭҚ). КЖ-гі ақпарат түрлері.

2. Компьютерлік жүйелердің осалдығы. Қол жеткізу, қол жеткізу субъектісі мен объектісі түсініктері. Рұқсатсыз қол жеткізу (РсҚЖ) туралы түсінік. РсҚЖ кластары және түрлері.

3. Компьютерлік жүйелердегі қауіпсіздік саясаты. Қауіпсіздік саясаты ұғымы және оның негізгі тұжырымдамасы. Қауіпсіздікті бағалау.

4. Мәліметтерге қол жеткізудің КЖ-субъектілерін қолданушыларды идентификациялау. Қолданушыны идентификациялау мәселесі. Идентификация хаттамасы ұғымы. Идентификациялаушы ақпарат ұғымы.

5. Файлдарға қолжетімділікті шектеу құралдары мен әдістері. РсҚЖ-ден мәліметтерді қорғаудың негізгі тәсілдері. Қол жеткізу фактілерін белгілеу әдістері. Қол жеткізу журналдары.

6. Процесс тарапынан мәліметтерге қатынасу. Мәліметтерді өзгертуден қорғау ерекшеліктері. Қол жеткізуді шектеу жүйелерінің сенімділігі. Хеш функцияны құруға негізделген әдіс, қойылатын талаптар және жүзеге асыру жолдары.

7. Программалық-аппараттық шифрлеу құралдары. Программалық-аппараттық шифрлеу кешендерін құру. Сигналдық процессорлардың негізінде криптотүрлендіру модульдерін жобалау.

8. ЭЕМ компоненттеріне қолжетімділікті шектеудің әдістері мен құралдары. ДЭЕМ компоненттері. ДЭЕМ қорғалатын компоненттерінің жіктелуі: ДЭЕМ-нің шеттетілетін және шеттетілмейтін компоненттері.

9. Программаларды рұқсатсыз көшіруден қорғау. Көшіруден қорғау мәселесіне көзқарас. Программалық жабдықтаманы көшіруден қорғаудың жалғыз құралы ретінде ПЖ-ны аппараттық ортаға және физикалық тасымалдаушыларға тәуелдендіруді пайдалану.

10. Маңызды ақпаратты сақтау. Құпия сөздер мен кілттер. Қатынасуды бақылау мақсатында қолданылатын құпия ақпарат: кілттер мен құпия сөздер.

11. Криптографиялық кілттерді басқару. Кілттерді генерациялау. Кілттерді тарату.

12. Симметриялық криптожүйелер үшін кілттерді таратуды аутентификациялау хаттамасы. Негізгі түсініктер мен анықтамалар, криптографиялық хаттамалардың типтері, мысалдар.

13. Асимметриялық криптожүйелерге арналған ашық кілттер сертификаттарын пайдаланатын хаттама.

14. Кілттерді сақтауды ұйымдастыру (жүзеге асыру мысалдары). Тікелей қолжетімді магниттік дискілер. TouchMemory құралы.

15. Программаларды оқып үйренуден қорғау. Программалық жабдықтаманы оқып үйрену және кері жобалау. ПЖ жұмысын зерделеудің мақсаты мен міндеттері. ПЖ зерделеу тәсілдері: статикалық және динамикалық зерделеу.

III. Пайдаланылған әдебиеттер тізімі

Негізгі:

1. Дискретная математика для программистов Хаггарти Р. Изд. Техносфера. М: 2012, 400с.

2. CryptoSchool. Joachim von zur Gathen. Springer; 1st ed. 2015 edition.888 pages;

3. Goutam Paul , Subhamoy Maitra. Publisher.RC4 Stream Cipher and Its Variants (Discrete Mathematics and Its Applications). : CRC Press; 1st edition 2019. 311 pages.

4. С.А.Абрамов Элементы компьютерной алгебры линейных обыкновенных дифференциальных, разностных и q-разностных операторов М: МЦМНО 2012 126с.

5. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2002. 2-е изд.

6. Кнут Д. Искусство программирования. Т. 2. Получисленные алгоритмы. Вильямс: М. – СПб. – Киев, 2000. 3-е издание.

7. Michael E. Whitman, Herbert J. Mattord. Principles of Information Security. Cengage Learning; 6th edition, 2017, 656 pages

8. Richard E. Smith Elementary Information Security. Jones & Bartlett Learning; 3rd edition, 2019. 708 pages

9. David Kim (Author), Michael G. Solomon. Fundamentals of Information Systems Security. Jones & Bartlett Learning; 3rd edition,2016. 548 pages

10. Е. В. Вострецова, Основы информационной безопасности, Екатеринбург, 2019 г., 208с.

11 Ш.Парасрам, А.Замм, Т.Хериянто, Ш.Али, "Kali Linux. Тестирование на проникновение и безопасность", Питер, 2020 г., 448 с.

12. Alan Grid, "Cybersecurity. Learn Information Technology Security: How To Protect Your Electronic Data From Hacker Attacks While You Are Browsing The Internet With Your Smart Devices, Pc Or Television", Via Etenea LTD, 2020, 126 p.

13. Яворски Питер, «Ловушка для багов. Полевое руководство по веб-хакингу», Питер, 2020 г., 272 с.

14. Шелухин О.И., Сакалема Д.Ж., Филинова А.С., "Обнаружение вторжений в компьютерные сети (сетевые аномалии)", 2018 г., 220 с.

15. В. Ф. Шаньгин, "Информационная безопасность и защита информации", ДМК Пресс, 2017 г., 702 с.

16. А. А. Бирюков, "Информационная безопасность. Защита и нападение", ДМК Пресс, 2017г., 434с.

Қосымша:

1. Michael E. Whitman, Herbert J. Mattord. Principles of Information Security.Cengage Learning; 6th edition, 2017, 656 pages

2. Richard E. Smith Elementary Information Security. Jones & Bartlett Learning; 3rd edition, 2019. 708 pages

3. Фороузан Б.А. Криптография и безопасность сетей: Учебное пособие / Фороузан Б.А.; перевод с англ. под ред. А.Н. Берлина. – М.: Интернет-

Университет Информационных технологий: БИНОМ. Лаборатория знаний, 2010 – 784 с.

4. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. М.: МИФИ, 1997.

5. Brij Gupta, Gregorio Martinez Perez, Dharma P. Agrawal, Deepak Gupta. Handbook Of Computer Networks And Cyber Security: Principles And Paradigms. Springer, 2020 – p. 957.

6. Aboul Ella Hassanien, Mohamed Elhoseny. Cybersecurity and Secure Information Systems: Challenges and Solutions in Smart Environments. Advanced Sciences and Technologies for Security Applications. Springer International Publishing, 1st ed., 2019 – p. 320.

7. Виноградов И.М. Основы теории чисел. М.: Наука, 1972.

8. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд. – М.: Вильямс, 2001. – 672 с.

9. Kutub Thakur, Al-Sakib Khan Pathan. Cybersecurity Fundamentals: A Real-World Perspective. CRC Press. 2020 – p. 305

10. RC4 Stream Cipher and Its Variants (Discrete Mathematics and Its Applications). Goutam Paul , Subhamoy Maitra. Publisher : CRC Press; 1st edition 2019. 311 pages

11. С.А.Абрамов Элементы компьютерной алгебры линейных обыкновенных ифференциальных, разностных и q-разностных операторов М: МЦМНО 2012 126с.

12. Нечаев В.И. Элементы криптографии (Основы теории защиты информации) / Под ред. В.А. Садовничего. – М.: Высшая школа, 1999. – 109 с.

13. Фороузан Б.А. Криптография и безопасность сетей: Учебное пособие / Фороузан Б.А.; перевод с англ. под ред. А.Н. Берлина. – М.: Интернет-Университет Информационных технологий: БИНОМ. Лаборатория знаний, 2010 – 784 с.