ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

8D06101 – ИНФОРМАТИКА БІЛІМ БЕРУ БАҒДАРЛАМАСЫ
БОЙЫНША ҚАБЫЛДАУ ЕМТИХАНЫНЫҢ

БАҒДАРЛАМАСЫ

Қостанай, 2020

Мазмұны

Кіріспе

Арнайы пән бойынша оқуға түсу емтиханының бағдарламасы жоғарғы оқу орнынан кейінгі білім берудің алдыңғы деңгейінің (магистратура) бағдарламасы көлемінде құрастырылған.

Оқуға түсушілердің дайындық деңгейіне қойылатын негізгі талаптар:

Докторантураға оқуға түсуші міндетті:

түсінігі болу керек:

- компьютерлік жүйелерді заманауи бағдарламалық және аппараттық қамтамасыз етуді құру жолдары мен әдістері жайлы;
- бағдарламалау технологиялары мен алгоритмдік тілдері туралы;
- ақпараттық технологиялардың даму тенденциялары мен қолданбалы есептерді шешудің жуық әдістері жайлы;
- өз кәсіби қызметінің саласындағы отандық және шетелдік ғылым мен техниканың жетістіктері жайлы;
- еңбек нарығының қазіргі заман талаптары жайлы.

білуі керек:

- ақпараттық технологиялардың даму тенденциялары мен келешегін;
- есептеу техникасының, коммуникация мен желілердің заманауи құралдарын;
- техникалық құжаттамаларды дайындау құралдарын, әдістері мен ережелерін;
- ғылыми зерттеулер мен өндірісті ұйымдастырудың, экономиканың негіздерін, еңбек заңнамасының және эргономиканың негіздерін;
- заманауи бағдарламалаудың тілдерін;
- бағдарламалаудың қазіргі заман технологияларын, қолданбалы бағдарламалар пакеттерін;
- қолданбалы есептерді шешудің математикалық әдістері мен негізгі алгоритмдерін;
- визуалды бағдарламалауды, файл-менеджерді;
- алгоритмдердің негізгі модельдерін, алгоритм құру әдістерін, алгоритм жұмысының қиындықтарын есептеуді;
- криптографиялық хабарламалардың құрылымын, мәтіндер мен шифрлардың математикалық модельдерін;

игеруі керек:

- ғылыми-зерттеу мен педагогикалық қызмет барысында пайда болатын және тереңдетілген кәсіби білімді талап ететін есептерді тұжырымдау және шешу;
- қажетті зерттеу әдісін тандау, нақты зерттеу есептері нәтижесінде жаңа әдістер құрастыру және бар әдістерді түрлендіру;
- алынған нәтижелерді өңдеу, бар мәліметтерді есепке ала отырып талдау, арнайы әдебиеттер мен ғылыми-техникалық ақпаратпен жұмыс істеу;
- бағдарлама жазу кезінде түрлі модульдер құрастыру; өзіндік компоненттер құру; бағдарламалық құрал-саймандарды пайдаланып компоненттерді рәсімдеу; оқиғаны өңдеуді құру;
- нақты бір есептер үшін алгоритмдер құрастыру; алгоритм жұмысының қиындығын табу;
- негізгі криптографиялық әдістерді, хаттамалар мен алгоритмдерді пайдалану;

дағдылану:

- бағдарлама-аппараттар кешенімен, бағдарламалық қамтамасыз етумен жұмыс;
- қолданбалы есептерді шешу алгоритмін құрастыру;
- бағдарламалау, мәліметтерді шифрлау, мәліметтерді шифрлау үшін таңдалған алгоритмді дәлелдеу;

құзыретті болу:

- заманауи ақпараттық технологиялармен байланысты барлық сұрақтар бойынша: түрлі есептерді шешу үшін компьютерлік жүйені, бағдарламалау тілдерін, бағдарламамен қамтамасыз етуді пайдалану;
- типтік көп кездесетін проблемалар үшін алгоритмнің дұрыстығын дәлелдеу әдісінде;
- көп кездесетін шешілмейтін есептерді дәлелдеу әдісінде;
- шифрлау әдісін таңдауда, ақпаратты шифрлау және шифрды ашу үрдісін оңтайландыру мен керекті математикалық аппаратты пайдалануда;

Бұл бағдарлама 8D06101 – Информатика мамандығы бойынша докторантураға түсушілерге арналған.

Оқуға түсу емтиханы келесі 3 пән бойынша кешенді емтихан түрінде жүргізіледі:

1. Бағдарламалық қамтаманы құру технологиялары
2. Алгоритмдер және олардың қиындықтары
3. Криптология

Негізгі бөлім (пәндердің мазмұны)

1. Бағдарламалық қамтаманы құру технологиялары

Бағдарламалық қамтамасыз етуді құрудың заманауи технологияларына шолу. Бағдарламалық қамтамасыз етуді құру үдерісін ұйымдастыру. Бағдарламалық қамтамасыз етуді құруға қойылатын талаптар. Бағдарламалық құралдарды жобалау. Бағдарламалық құралдарды тестілеу. Бағдарламаларды сүйемелдеу. Интерфейс жасау. Бағдарламалық қамтамасыз етуді ұжымдық әзірлеу. Бағдарламалық өнімдерді әзірлеудің және пайдаланудың экономикалық аспектілері. Объектілі-бағытталған бағдарламалау. Бағдарламалау тілдеріндегі конструктор және деструктор ұғымдары. Бағдарламалау тілдеріндегі инкрементальды жол. Бағдарламалау тілдерінде процедуралар мен функцияларды қолдану. Бағдарламалық қамтамасыз ету сапасын бағалау критерийлері.

2. Алгоритмдер және олардың қиындықтары

Интуитивті деңгейдегі алгоритм ұғымы. Алгоритмдерді талдау. Еркін қатынасуға болатын машиналар (ЕҚМ) және есептелінетін функциялар. Алгоритмдік күрделі проблемалар. Есептеулер күрделілігінің сипаттамалары. Күрделілік кластары, NP және олардың өзара байланысы. NP күрделілік есептері. Рекурсияны пайдаланатын алгоритмдер күрделілігі. Есептеулер тиімділігі. Бағдарламалауда графтық модельдер технологиясын қолдану. Коммивояжер есебі. Есептегіш алгоритмдер. Итерациялық алгоритмдер күрделілігі. Графтық модельдер технологиялары.

3. Криптология

Криптологияның негізгі түсініктері мен міндеттері. Криптографиялық хабарламаларға қойылатын негізгі талаптар. Криптографиялық әдістер. Құпия кілттерді басқару. Құпияларды бөлу. Деректер қорын криптографиялық қорғау. Шифрлардың модельдері. Ашық кілтпен шифрлау жүйелері. Криптографиялық хаттамалар. Сандық қолтаңбалар. Криптографиялық хэш-функциялар. Кілттерді үлестіру хаттамалары. Сандардың псевдокездейсоқ тізбектері. Хаттамаларға арналған арнайы алгоритмдер. Хаттамаларға арналған алгоритмдер.

1 БАҒДАРЛАМАЛЫҚ ҚАМТАМАНЫ ҚҰРУ ТЕХНОЛОГИЯЛАРЫ

1. Бағдарламалық қамтамасыз етуді құрудың заманауи технологияларына шолу. Тарихи аспектідегі бағдарламалау технологиясы. Негізгі ұғымдар мен анықтамалар. Бағдарламалық қамтамасыз етудің жіктелуі. Бағдарламалық өнімді құрудың ерекшеліктері. Бағдарламалық қамтамасыз етуге қойылатын талаптармен жұмыс жасау принциптері. Жобалаудың мәселесі.

2. Бағдарламалық қамтамасыз етуді құру үдерісін ұйымдастыру.
Бағдарламалық өнімді құру ерекшеліктері. Бағдарламалық қамтамасыз етуге қойылатын талаптармен жұмыс жасау принциптері. Жобалаудың мәселесі.

3. Бағдарламалық қамтамасыз етуді құруға қойылатын талаптар.
Бағдарламалық өнімдерге қойылатын талаптарды анықтау. Бағдарламалық қамтамасыз етудің архитектурасын таңдау. Деректер құрылымы және форматы. Статикалық, жартылай статикалық және динамикалық құрылымдар. Модульді бағдарламалау. Құрылымдық жағдайдағы ерекшеліктерді анықтау және талаптарды талдау. Объектілік жағдайдағы ерекшеліктерді анықтау және талаптарды талдау.

4. Бағдарламалық құралдарды жобалау.
Құрылымдық амалдар кезінде бағдарламалық қамтамасыз етуді жобалау. Әзірленетін бағдарламалық қамтамасыз етудің құрылымдық сызбасы. Функционалдық сызба. Алгоритм құрастыру кезінде қадам бойынша талдап тексеру әдісі. Константайнның құрылымдық карталары. Джексонның құрылымдық карталары. CASE-технологиялар. Бағдарламалық қамтамасыз етуді әзірлеуді жылдамдату. RAD әдістемесі. Объектілік тұрғыда бағдарламалық қамтамасыз етуді жобалау. Төтенше бағдарламалау. Бағдарламалаудың мәні. Бағдарламалау және тестілеу.

5. Бағдарламалық құралдарды тестілеу
Терминдер және анықтамалар. «Ақ жәшікті» және «қара жәшікті» тестілеу. Тесті жасау реті. Тестілеуді автоматтандыру. Модульді тестілеу. Интеграциялық тестілеу. Жүйелік тестілеу. Бағдарламаның тиімділігі және оңтайландыру. Бағдарламалау стилі. Бағдарламалық қамтамасыз етудің сенімділігі. Бағдарламаларды дұрыстау.

6. Бағдарламалық жүйелерді тестілеу әдістемесі
Бағдарламалық қамтамасыз етуді тестілеу барысын ұйымдастыру. Бағдарламалық жүйелерді тестілеу әдісі. Элементтерді тестілеу. Интеграцияны тестілеу. Дұрыстықты тестілеу. Жүйелік тестілеу. Дұрыстау өнері.

7. Бағдарламаларды сүйемелдеу.
Бағдарламалық құжаттардың түрлері.Түсіндірме жазба. Қолданушыға арналған нұсқау. Жүйелік бағдарламалаушыға арналған нұсқау.

8. Интерфейс жасау
Бағдарламаны әзірлеудің құрал-жабдықтары. Бағдарламалау технологиялары. Бағдарламалық өнімдерді қорғау. Қолданбалы бағдарламалар пакеті. Бағдарламалық қамтамасыз етуді жасаудың құнын бағалау. Пайдалану кезеңіндегі БҚ тиімділігін бағалау әдісі.

9. Бағдарламалық қамтамасыз етуді ұжымдық әзірлеу
Қолданбалы бағдарлама пакеттері. Microsoft Visual SourceSafe нұсқасын бақылау жүйесі. Subversion нұсқасын бақылау жүйесі.

10. Бағдарламалық өнімдерді әзірлеудің және пайдаланудың экономикалық аспектілері

Бағдарламалық қамтамасыз етуді құрудың құнын бағалау. Сызықтық әдіс. Функционалды нүктелер әдісі. Эмпирикалық деректерді қолданумен бағалау. Пайдалану кезінде БҚ тиімділігін бағалау әдістері.

11. Объектілі-бағытталған бағдарламалау

Бағдарламалау технологиясының дамуы. Объектілі-бағытталған бағдарламалау құралдары. Объектілі-бағытталған бағдарламалау принципі. Бағдарламалаудағы объектілі-бағытталған жолдың маңызы. Объектілі-бағытталған талдауға мысал. Объектілі-бағытталған жобалау. Объектілі-бағытталған жобалау үдерісі. Бағдарламалық бұйымдардың өмірлік циклі түсінігі.

12. Объектілі-бағытталған бағдарламалық жүйелердің метрикалары

Чидамбер-Кемерер метрикаларын пайдалану. Лоренц және Кидд метрикалары. Фернандо Абреу метрикалар жинағы.

13. Бағдарламалау тілдеріндегі конструктор және деструктор ұғымдары

Конструктор және деструктор ұғымдары. Объектілі-бағытталған бағдарламалаудағы мұрагерлік.

14. Бағдарламалау тілдеріндегі инкрементальды жол

Бағдарламалау тілі түсінігі. Инкрементальды бағдарламалау ұғымы. Бағдарламалау тілдеріне инкрементальды көзқарастың маңызды сәттері.

15. Бағдарламалау тілдерінде процедуралар мен функцияларды қолдану

Процедура түсінігі. Функция түсінігі. Функция және процедураны жариялау. Рекурсивті функция. Тура және жанама рекурсия.

16. Бағдарламалау тілдеріндегі модуль ұғымы

Модуль түсінігі. Атаулардың көріну облысы: локальды айнымалы, жаһандық айнымалы. Параметрлерді жіберу: мағынасы бойынша және сілтеме бойынша.

17. Бағдарламалық қамтамасыз ету сапасын бағалау критерийлері

Бағдарламалық қамтамасыз ету түсінігі. Бағдарламалық қамтамасыз ету сапасы. Бағдарламалық қамтамасыз ету сапасын бағалау критерийлері: иілгіштігі, қарапайымдылығы, тиімділігі, шығынның төмендеуі.

Емтихан сұрақтарының тізімі

1. Бағдарламалық қамтамасыз етуді құрудың заманауи технологияларына шолу.
2. Бағдарламалық қамтамасыз етуді құру үдерісін ұйымдастыру.
3. Бағдарламалық қамтамасыз етуді құруға қойылатын талаптар.
4. Бағдарламалық құралдарды жобалау.
5. Бағдарламалық құралдарды тестілеу
6. Бағдарламалық жүйелерді тестілеудің әдістемесі
7. Бағдарламалық құжаттардың түрлері.Түсіндірме жазба. Қолданушыға арналған нұсқау. Жүйелік бағдарламалаушыға арналған нұсқау.
8. Бағдарламаны әзірлеудің құрал-жабдықтары. Бағдарламалық өнімдерді қорғау. Қолданбалы бағдарламалар пакеті.
9. Бағдарламалық қамтамасыз етуді ұжымдық әзірлеу.

10. Бағдарламалық өнімдерді әзірлеудің және пайдаланудың экономикалық аспектілері.
11. Объектілі-бағытталған бағдарламалау. Объектілі-бағытталған бағдарламалаудың құралдары. Объектілі-бағытталған бағдарламалаудың принципі.
12. Объектілі-бағытталған бағдарламалық жүйелердің метрикалары.
13. Бағдарламалау тілдеріндегі конструктор және деструктор ұғымдары
14. Бағдарламалау тілдеріндегі инкрементальды жол
15. Бағдарламалау тілдерінде процедуралар мен функцияларды қолдану
16. Бағдарламалау тілдеріндегі модуль ұғымы
17. Бағдарламалық қамтамасыз ету сапасын бағалау критерийлері

Ұсынылатын әдебиеттер тізімі

1. Гагарина Л. Г., Кокорева Е. В., Виснадул Б. Д. Технология разработки программного обеспечения: учебное пособие / под ред. Л. Г Гагариной. — М: ИД «ФОРУМ»: ИНФРА-М, 2016. — 400 с.: ил. — (Высшее образование).
2. Орлов С.А. Технологии разработки программного обеспечения. СПб.: Питер, 2002. 464 с.
3. Кокарева Е.В., Гагарина Л.Г., Виснадул Б.Д. Технологии разработки программного обеспечения. ИНФРА – М, издательский дом Форум, 2008г.
4. Браудэ Э. Технологии разработки программного обеспечения. СПб.: Питер, 2004. 656 с.
5. Сергушичева А.П. Технологии разработки программного обеспечения: Методические указания к выполнению лабораторной работы №4 «Применение CASE – средств при разработке программного обеспечения». – Вологда: ВоГТУ, 2007. – 31 с.
6. Орлов С.А. Принципы объектно-ориентированного и параллельного программирования на языке Ada 95. Рига: TSI, 2001. 327 с.
7. Ambler, S.W. The Object Primer. 2nd ed. Cambrige University Press, 2001. 541 pp.
8. Beck, K, Fowler, M.Planning Extreme Programming. Addison – Wesley, 2001. 156 pp.
9. Boehm, B.W. etal. Software Cost Estimation with Cocomo II. Prentice Hall, 2011. 502 pp.
10. Fowler, M. The New Methodology http://www.martinfoler.com, 2001
11. Дин Леффингуэлл, Дон Уидриг. Принципы работы с требованиями к программному обеспечению. М.: Вильяме, 2002.
12. Липаев В. В. Проектирование программных средств. М.: Высшая школа, 1990.
13. Майерс Г. Искусство тестирования программ. М.: Финансы и статистика, 1982.
14. Брукс Ф. Мифический человеко-месяц, или Как создаются программные системы. СПб.: Символ-Плюс, 1999.
15. Роберт Дж. Орберг. COM+ технология. Основы и программирование М.: Вильяме, 2000. 478 с.
16. Аджиев В. // Открытые системы. 1998. № 1.
17. Батенко Л. П. // Менеджмент и менеджер. 2003. № 3.
18. Алистэр Коуберн, Лори Вильяме. Парное программирование: преимущества и недостатки.
19. Жоголев Е. А. Введение в технологию программирования (конспект лекций). М.: ДИАЛОГ-МГУ, 1994.
20. Страуструп Б. Язык программирования С++. Киев: ДиаСофт, 1993.
21. Модели и структуры данных / В. Д. Далека, А. С. Деревянко, О. Г. Кравец, Л. Е. Тимановская. Харьков: ХГПУ, 2000.

2 АЛГОРИТМДЕР ЖӘНЕ ОЛАРДЫҢ ҚИЫНДЫҚТАРЫ

1. Интуитивті деңгейдегі алгоритм ұғымы
Интуитивті деңгейдегі алгоритм ұғымы және оның қасиеттері. Алгоритмнің тиімділік шаралары. Алгоритмдер кластары. Полиномиалды және экспоненциалды алгоритмдер.

2. Алгоритмдерді талдау
Алгоритмдерді құру принциптері. Жүзеге асыру және эмпирикалық талдау. Алгоритмдерді талдау. Тьюринг машинасының алгоритмдік моделі. Тьюринг машинасында функцияларды есептеу.

3. Еркін қатынасуға болатын машиналар (ЕҚМ) және есептелінетін функциялар
ЕҚМ алгоритмдік моделі. ЕҚМ-да функцияларды есептеу. Черч тезисі. Дискреттік модельдерді құру принципі. Есепті шешу алгоритмін таңдау. Фон-Нейман бойынша орнықтылықты талдау. Ішінара рекурсивті функциялар үшін Черч тезисі.

4. Алгоритмдік күрделі проблемалар
Теңдеулер жүйесінің үйлесімді шешімін табу алгоритмін құру. Бағдарламалау ерекшеліктері.

5. Есептеулер күрделілігінің сипаттамалары
Теңдеулер жүйесін шешу алгоритмдері. Уақытша және көлемді қиындықтағы функциялар. Тьюринг машинасында уақытша күрделіліктерді төменнен бағалау.

6. Күрделілік кластары, NP және олардың өзара байланысы
Жиындардың жиынтықтары. Генерирлеу. NP – толық есептер. Кук теоремасы.

7. NP күрделілік есептері
Негізгі NP толық есептер. Күшті NP толықтық. Co- NP класы. NP кластар құрылымы және co- NP. NP –толықтық теориясын жуықталған алгоритмдерді құруға қолдану.

8. Рекурсияны пайдаланатын алгоритмдер күрделілігі
Екіөлшемді есептерді шешу алгоритмдерін модельдеу және жүзеге асыру. Матрицаны айналдырудың рекурсивті алгоритмі.

9. Есептеулер тиімділігі
Бірқалыпты емес айырымдық торды қолдануда алгоритмдерді жүзеге асыру. Есептеулер тиімділігі. Есептеуді тиімділендіру тәсілдері.

10. Бағдарламалауда графтық модельдер технологиясын қолдану
Бағдарламалауда графтық модельдер технологиясын қолдану. Есепті шешу алгоритмі моделін графтыққа келтіру.

11. Графтардағы негізгі алгоритмдер
Графта тереңдігінен іздеу. Графта көлденеңінен іздеу. Графтағы ең қысқа жол. Графтағы максималды ағын. Графтың минималды арқау ағашы.

12. Коммивояжер есебі
Коммивояжер есебі үшін дәлдік бағасына кепілдік беретін алгоритмдер. Бұтақтар мен шекаралар әдісі.

13. Есептегіш алгоритмдер

Кесінділердің қиылысуы, көпбұрыштардың бұрыштарын есептеу. Геометрия есептерін шешудің негізгі алгоритмдері.

14. Итерациялық алгоритмдер күрделілігі
Итерациялық алгоритмдерді жасау. Дискретті модельдерді құру принциптері. Есептерді шешу алгоритмін таңдау.

15. Графтық модельдер технологиялары
Лабиринттер, лабиринтте жол іздеу алгоритмі: қайталаумен іздеу, толқынды әдіс.

16. Тиімді алгоритмдер құрастыру
«Бөл де, басқар» әдісі. Динамикалық программалау.

Емтихан сұрақтарының тізімі

1. Интуитивті деңгейдегі алгоритм ұғымы
2. Алгоритмдерді эмпирикалық талдау. Тьюринг машинасының алгоритмдік моделі.
3. Еркін қатынасуға болатын машиналар (ЕҚМ) және есептелінетін функциялар.
4. Алгоритмдік күрделі проблемалар.
5. Есептеулер күрделілігінің сипаттамалары.
6. Күрделілік кластары, NP және олардың өзара байланысы.
7. NP күрделілік есептері.
8. Рекурсияны пайдаланатын алгоритмдер күрделілігі.
9. Есептеуді тиімділендіру тәсілдері. Бірқалыпты емес айырымдық торды қолдануда алгоритмдерді жүзеге асыру.
10. Бағдарламалауда графтық модельдер технологиясын қолдану
11. Графтардағы негізгі алгоритмдер. Графта тереңдігінен іздеу. Графта көлденеңінен іздеу. Графтағы ең қысқа жол.
12. Коммивояжер есебі.
13. Есептегіш алгоритмдер.
14. Комбинаторика. Орналастыру. Орын ауыстыру. Қайталаумен орын ауыстыру. Теру. Теру және Ньютон биномы.
15. Итерациялық алгоритмдер күрделілігі.
16. Графтық модельдер технологиялары.
17. «Бөл де, басқар» әдісімен тиімді алгоритмдер құрастыру

Ұсынылатын әдебиеттер тізімі

1. Алгоритмы. Руководство по разработке», Стивен Скиена,2-е издание, 720 стр., БХВПетербург, 2011
2. Кузюрин, С.А. Фомин. Курс лекций «Сложность алгоритмов» (2013).
3. Sipser M. Introduction to the Theory of Computation. Boston, Mass.: Thomson Course Technology, 2016 (pp. 368–380).
4. Arora S. and Barak B. Computational Complexity: A Modern Approach. Cambridge University Press, 2017 (Chapter 7).
5. Кормен Томас. Алгоритмы: построение и анализ. М.: Вильямс, 2005.
6. M.T. Goodrich, R.Tamassia. Data structures and Algorithms in Java., Prentice Hall. 2005. – 695 p.
7. Р.Сейджвик. Фундаментальные алгоритмы на С.- СПб: ООО «ДиаСофтЮП», 2003. – 1136с.
8. S. Baase. Computer Algorithms. Introduction to Design and Analysis. 2nd edition, Prentice Hall. 2001

9. J.Hastad Notes for the course advanced algorithms
10. Абрамов С.А. Лекции о сложности алгоритмов, - М.: МЦНМОб 2009.
11. Кузюрин Н.Н., Фомин С.А. Эффективные алгоритмы и сложность вычислений, - М.: МФТИ, 2007.
12. Шурыгин В.А. Сложностный метод теории алгоритмов. – М.: ЛИБРОКОМ, 2009.
13. Окулов С.М. Программирование в алгоритмах. - М.:БИНОМ. Лаборатория знаний, 2002. - 341с.
14. Ахо А., Хопкрофт Д., Ульман Д. Структуры данных и алгоритмы.: Пер. с англ.:Учебное пособие. –М.:Издательский дом «Вильямс», 2000. – 384с.
15. Культин Н. Turbo Pascal в задачах и примерах. – СПб.: БХВ-Петербург, 2000. – 256с.
16. Кирюхин В. М., Лапунов А. И., Окулов С. М. Задачи по информатике (международные олимпиады 1989-1996). М.: ABF, 1996.

3 КРИПТОЛОГИЯ

1. Криптологияның негізгі түсініктері мен міндеттері
Симметриялы және асимметриялы шифрожүйелер. Криптографиялық хаттамалар туралы түсінік. Құпия байланысты ұйымдастыру, криптоаналитика есептері.

2. Криптологиядағы ақпараттар теориясының әдістері
Шеннон бойынша ақпараттар саны және оның қасиеттері. Криптожүйелердің Шеннондық модельдері. Симметриялы криптожүйелердің тұрақтылығының теоретикалық-ақпараттық бағасы

3. Криптографиялық хабарламаларға қойылатын негізгі талаптар
Құпиялылық. Бүтіндік. Түпнұсқалылық.

4. Криптографиялық әдістер
Кілттерді алдын-ала тарату. Кілттерді жіберу. Кілттердің ашық таратылуы. Бөлу схемасы.

5. Құпия кілттерді басқару
Кілттермен алмасу. Кілттермен алмасуды және шынайылықты тексеретін хаттамалардың формалды талдауы.

6. Құпияларды бөлу. Құпия кілттерді басқару
Құпияны бөлу. Құпияны бірлесіп пайдалану.

7. Деректер қорын криптографиялық қорғау
Деректер қорын криптографиялық қорғау. Криптографиялық режимдер және алгоритмдер типтері.

8. Шифрлардың модельдері
RSA шифрожүйелері. Диффи Хеллман шифрожүйелері. Эль Гамаль шифрожүйелері.

9. Ашық кілтпен шифрлаудын жүйелері
Мак Элис шифрожүйесі. «Рюкзак мәселесі» алгоритмінің негізіндегі шифрожүйелер.

10. Криптографиялық хаттамалар

Хаттамалар элементтері. Негізгі хаттамалар. Аралық хаттамалар. Дамыған хаттамалар. Эзотерикалық хаттамалар. Нөлдік біліммен дәлелдеу.

11. Сандық қолтаңбалар
Ашық кілттер шифрожүйесі негізіндегі сандық қолтаңбалар. Фиат-Шамир сандық қолтаңбасы. Эль Гамаль сандық қолтаңбасы.

12. Криптографиялық хэш-функциялар
Деректердің бүтіндігі және хэштеу функциялары. Хэштеудің кілттік функциялары. Хэштеудің кілтсіз функциялары.

13. Криптографиялық алгоритмдер
DES деректерін шифрлеу стандарты. Блоктық шифрлер. Блоктық шифрлерді біріктіру. Псевдокездейсоқ тізбектердің генераторлары және ағын шифрлері. Нағыз кездейсоқ тізбектердің генераторлары.

14. Кілттерді үлестіру хаттамалары
Симметриялық шифрлауды пайдаланып кілттерді жіберу. Екі жақты хаттамалар. Үш жақты хаттамалар. Ассиметриялы шифрлауды пайдаланып кілттерді жіберу.

15. Сандардың псевдокездейсоқ тізбектері
Генерацияның қарапайым алгоритмдері. Рекуррентті екілік тізбектер. Максимальды ұзындық тізбектері. Псевдокездейсоқ тізбектерді талдау.

16. Хаттамаларға арналған арнайы алгоритмдер
Бірнеше ашық кілттері бар криптографиялар. Құпияны бөлу алгоритмдері. Ақыл-ойға негізделген арна.

17. Хаттамаларға арналған алгоритмдер
«Шындық монетасын» тастау. Бір бағыттағы сумматорлар. «Бәрі немесе ештеңе» құпияларын ашу. Кванттық криптография.

Емтихан сұрақтарының тізімі

1.Симметриялық және ассимметриялық шифрожүйелер. Криптографиялық хаттамалар туралы түсінік.
2.Шеннон бойынша ақпараттар саны және оның қасиеттері. Криптожүйелердің Шеннон модельдері.
3. Криптографиялық хабарламаларға қойылатын негізгі талаптар.
4. Кілттерді алдын ала бөлу. Кілттерді жіберу. Кілттерді ашық бөлу.
5.Құпия кілттермен алмасу. Кілттермен алмасу және түпнұсқаны тексеру хаттамасының формальды талдауы.
6. Құпия кілттерді басқару. Құпияларды бөлу.
7. Деректер қорын криптографиялық қорғау.
8. Шифрлар модельдері: RSA шифрожүйесі, Диффи Хеллман шифрожүйесі.
9. Ашық кілтпен шифрлау жүйесі.
10. Криптографиялық хаттамалар.
11.Ашық кілттері бар шифрожүйелер негізіндегі сандық қолтаңбалар. Фиат-Шамир сандық қолтаңбасы.
12. Криптографиялық хэш-функциялар
13. DES деректерін шифрлау стандарты. Блоктық шифрлар. Блоктық шифрларды біріктіру.

14. Кілттерді бөлу хаттамалары.
15. Сандардың псевдокездейсоқ тізбектері.
16. Хаттамаларға арналған арнайы алгоритмдер.
17.«Шындық монетасын» лақтыру хаттамасына арналған алгоритм. «Бәрі немесе ештеңе» құпияларын ашу.

Ұсынылатын әдебиеттер тізімі

1. А.В.Черемушкин. Лекции по арифметическим алгоритмам в криптографии. - М.: МЦНМО, 2015.
2. Фомичев В.М. Дискретная математика и криптология. – М.: ДИАЛОГ-МИФИ, 2003.
3. Тилберг К.Х.А. Основы криптологии. Профессиональное руководство. – М.: Мир, 2007.
4. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. М.: Высшая школа, 1999.
5. Шнайер Б. Прикладная криптография. – СПб: Питер, 2005.
6. Казарин О.В. Теория и практика защиты программ. – М.: Высшая школа, 2000.
7. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – Спб.: Питер, 2000.
8. W. Stallings. CryptographyandNetworksecurity. PrinciplesandPractice. SecondEdition. Upper Saddle River, NJ: Prentice Hall, 1999.
9. J. JaworskiandP. Perrone. Java Security Handbook.- SAMS Publishing, 2000.