НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«Київський політехнічний інститут імені Ігоря Сікорського»

Затверджую

Голова Приймальної комісії
Ректор

_____ Михайло ЗГУРОВСЬКИЙ
підпис

26.04.2024
дата

Навчально-науковий фізико-технічний інститут

повна назва факультету/навчально-наукового інституту

ПРОГРАМА
фахового іспиту
для вступу на освітньо-наукову програму підготовки магістра
«Математичні методи криптографічного захисту інформації»

за спеціальністю 113 Прикладна математика

Програму ухвалено:
Вченою Радою Навчально-наукового
фізико-технічного інституту
Протокол № 5/2024 від 15 квітня 2024 р.
Голова Вченої Ради
_____ Олексій НОВІКОВ

Київ – 2024

ВСТУП

Програма фахового іспиту для вступу на освітньо-наукову програму підготовки магістра «Математичні методи криптографічного захисту інформації» за спеціальністю 113 Прикладна математика складена на основі вимог до опанування даної програми.

Програма фахового іспиту передбачає перевірку набуття вступником компетентностей та результатів навчання, що визначені стандартом вищої освіти за спеціальністю 113 Прикладна математика для першого (бакалаврського) рівня вищої освіти.

Фаховий іспит здійснюється в письмовій формі. Білет містить чотири питання (два теоретичні та два практичні з різних розділів програми), на які екзаменований повинен дати письмову відповідь.

Тривалість фахового іспиту – 2 астрономічні години, перерви немає. Екзаменований вільно розподіляє свій час між всіма завданнями.

ОСНОВНИЙ ЗМІСТ ПРОГРАМИ

Розділ 1.

1.1. Теоретична частина

1. Загальне поняття випадкової події та стохастичного експерименту, випадкової величини та випадкового вектора; функції розподілу; незалежні випадкові величини; дискретні та неперервні випадкові величини та їх характеристики.

2. Послідовності випадкових величин: поняття збіжності послідовності випадкових величин; нерівність Чебишева; закон великих чисел.

3. Граничні теореми теорії ймовірностей: слабка збіжність випадкових величин; характеристичні функції випадкових величин; схема незалежних випробувань Бернуллі, центральна гранична теорема.

4. Основні поняття математичної статистики: вибірка, варіаційний ряд та емпірична функція розподілу; вибіркові характеристики; асимптотичний розподіл вибіркових моментів; порядкові статистики; розподіли деяких функцій від нормальних випадкових величин.

5. Оцінки невідомих параметрів розподілу: класифікація оцінок; незміщені оцінки з мінімальною дисперсією; принцип достатності та оптимальні оцінки; оцінки найбільшої правдоподібності; метод моментів; довірчі інтервали та інтервальне оцінювання.

6. Статистичні гіпотези та статистичні критерії; критерії згоди; перевірка гіпотези про вигляд розподілу, критерій χ^2; параметричні гіпотези; вибір з двох простих гіпотез; критерій Неймана-Пірсона; складні гіпотези; критерій відношення правдоподібності.

1.2. Практична частина

1. Числові характеристики дискретних випадкових величин. Задачі на біноміальний розподіл, геометричний, гіпергеометричний розподіл, розподіл Пуассона.

2. Неперервні випадкові величини та вектори, їх властивості та характеристики.

3. Критерії перевірки гіпотези про вигляд розподілу, про однорідність вибірки та гіпотези про незалежність. Вибір з двох простих гіпотез.

Розділ 2.

2.1. Теоретична частина

1. Основні комбінаторні конфігурації. Розміщення з повторенням/без повторення, вибірки без повернення/з поверненням, перестановки без повторень/з повторенням, розбиття множин. Перелічування основних комбінаторних конфігурацій. Біном Ньютона.

2. Генератриси (твірні функції) послідовностей. Звичайні та експоненційні генератриси. Операції над генератрисами (сума, згортка, похідна, інтеграл). Визначення елементів послідовностей за їх генератрисами.

3. Лінійні рекурентні послідовності. Побудова генератриси лінійної рекурентної послідовності. Формула Біне загального елементу послідовності Фібоначчі. Пошук розв’язків лінійних рекурент через корені характеристичного поліному.

4. Комбінаторні алгоритми. Генерація перестановки за індексом, із мінімальними змінами, у лексикографічному порядку. Генерація підмножин за індексом, у лексикографічному порядку; коди Грея, генерація підмножин із мінімальними змінами. Вибір випадкової перестановки та випадкової підмножини.

2.2. Практична частина

1. Задачі на підрахунок числа комбінаторних конфігурацій, потужності множин.

2. Комбінаторні задачі, пов’язані з застосуванням поліномів і генератрис, доведення комбінаторних тотожностей.

3. Задачі на комбінаторні алгоритми породження перестановок та підмножин в лексикографічному порядку, випадкових перестановок та підмножин.

РОЗДІЛ 3.

3.1. Теоретична частина

1. **Основні поняття прикладної алгебри.** Визначення півгрупи, моноїда, групи, абелевої групи. Порядок групи, порядок елементу групи, циклічні підгрупи. Теорема Лагранжа. Визначення кільця, ідеалу кільця, поля.

2. **Кільце лишків за модулем *n*.** Визначення, операції над лишками. Алгоритм Евкліда та розширений алгоритм Евкліда. Мультиплікативна група кільця лишків, функція Ойлера та її обчислення. Теорема Ойлера, мала теорема Ферма. Розв'язування лінійних порівнянь.

3. **Квадратичні лишки.** Символи Лежандра та Якобі, правила обчислення, критерій Ойлера. Пошук квадратних коренів за простим модулем та за модулем виду $p \cdot q$.

4. **Генерування простих чисел.** Означення простого та псевдопростого числа, псевдопрості Ферма, Ойлера, сильні псевдопрості. Тест Ферма, числа Кармайкла. Тест Соловея-Штрассена. Тест Міллера-Рабіна. Сильні прості числа, числа Блюма.

5. **Скінченні поля характеристики 2.** Способи побудови поля та представлення елементів поля (вектори, поліноми), подання операцій над елементами. Операції у поліноміальному та нормальному базисах (додавання, множення, піднесення до степеня, пошук оберненого елементу, обчислення сліду).

3.2. Практична частина

1. Задачі на пошук обернених елементів за модулем, розв'язування лінійних порівнянь.
2. Знаходження квадратних коренів за простим модулем та за модулем виду $p \cdot q$.
3. Задачі на виконання операцій у скінченному полі характеристики 2.
4. Задачі на перевірку натуральних чисел на простоту заданими тестами.

Розділ 4.

4.1. Теоретична частина

1. Основні поняття криптології. Задачі, напрямки та методи захисту інформації. Криптографічний захист інформації. Основні поняття криптології. Поняття ентропії, властивості ентропії ймовірнісних ансамблів, сумісна та умовна ентропія, взаємна інформація. Моделі джерел відкритого тексту, ентропія на символ джерела. Загальна класифікація класичних і сучасних шифрів.

2. Теорія секретних систем Шеннона. Ієрархія типів атак на криптосистему. Теоретична та практична стійкість. Цілком таємні криптосистеми. Границя Шеннона. Ненадійність ключа і відкритого тексту Відстань однозначності. Принципи Шеннона побудови стійких шифрів.

3. Класичні схеми шифрування. Моноалфавітні підстановки. Методи криптоаналізу. Поліалфавітні підстановки. Шифр Віженера та його криптоаналіз. Інші шифри підстановки. Шифри перестановки: загальне визначення, табличні перестановки, грати Кардано, інші шифри перестановки. Комбіновані шифри.

4. Булеві функції та випадкові послідовності. Булеві функції та способи їх зображення. Криптографічні властивості булевих функцій. Методи генерації випадкових та псевдовипадкових послідовностей. Статистичні методи оцінки якості булевих функцій, випадкових та псевдовипадкових послідовностей.

5. Системи блокового шифрування. Схема Фейстеля та її властивості. Стандарти блокового шифрування DES та 3DES. Алгоритм шифрування ДСТУ ГОСТ 28147:2009.

6. Режими роботи блокових шифрів. Режими ECB, CBC, CFB, OFB та лічильника: основні властивості, поширення помилок при розшифруванні.

7. Системи блокового шифрування. Алгоритм шифрування AES. Алгоритм шифрування ДСТУ 7624:2014 «Калина».

8. Регістри зсуву із лінійним зворотним зв'язком. Подання лінійних регістрів зсуву діаграмою, рекурентною, супроводжуючою матрицею та характеристичним поліномом. Визначення періоду послідовності, яку генерує лінійний регістр зсуву. Циклова структура рекурентної послідовності.

9. Потокові системи шифрування. Способи введення нелінійності у схеми потокового шифрування на регістрах зсуву з лінійним зворотним зв'язком. Схеми з нерівномірним рухом регістрів зсуву. Приклади сучасних потокових шифрів: A5/1, SNOW 2.0.

4.2. Практична частина

1. Задачі математичної теорії інформації та теорії секретних систем Шеннона.
2. Вправи на класичні шифри підстановки та перестановки, їх властивості та методи криптоаналізу.
3. Криптографічні властивості булевих функцій.
4. Визначення властивостей потокових симетричних шифрів.

РОЗДІЛ 5.

5.1. Теоретична частина

1. Теоретичні основи асиметричної криптографії. Математичні моделі алгоритмів. Визначення часової та ємнісної складності алгоритмів, поліноміальної і експоненціальної складності. Розв'язувальні і важкорозв'язувальні задачі, класи P і NP. Поліноміальна звідність. NP-повні задачі. Проблема існування важкоборотних функцій у класичній та постквантовій моделях обчислень.

2. Складність алгоритмів та важкооборотні функції. Важкооборотні функції, важкоборотні функції з секретом. Важкоборотна функція дискретного піднесення до степеня. Схема відкритого розподілу ключів Діффі-Хеллмана. Важкооборотні функції RSA, Рабіна. Оцінки складності обчислення та обернення функцій.

3. Системи шифрування асиметричної криптографії. Загальна концепція асиметричних систем шифрування з відкритими ключами. Системи шифрування Мессі-Омури та Ель-Гамаля. Криптосистеми RSA та Рабіна. Основа стійкості асиметричних систем шифрування.

4. Геш-функції. Криптографічні властивості. Загальні схеми побудови. Характеристики геш-функцій, найбільш уживаних у системах захисту інформації. Колізії геш-функцій. Математичні моделі оцінки ймовірностей колізій та трудомісткості їх побудови. Застосування геш-функцій.

5. Цифровий підпис. Задачі цифрового підпису. Загальна концепція та схема цифрового підпису з геш-функцією в асиметричної криптографії. Цифровий підпис у схемі RSA з використанням геш-функцій, цифрові підписи Ель-Гамаля, Рабіна. Сліпий підпис. Атаки на цифровий підпис.

6. Криптографічні протоколи. Протоколи розподілу секретів, доведення без розголошення, схеми пред'явлення випадкових бітів, протоколи електронної готівки. Криптографічні алгоритми автентифікації: парольна автентифікація, автентифікація з використанням симетричних и асиметричних криптосистем.

7. Криптосистеми на еліптичних кривих. Групи точок еліптичних кривих: основні означення, групова операція. Криптосистеми на еліптичних кривих, основні питання, що виникають при їх реалізації. Стандарт цифрового підпису на еліптичних кривих ДСТУ 4145-2002.

5.2. Практична частина

1. Отримання оцінок складності алгоритмів.
2. Задачі на схему Діффі-Хеллмана розповсюдження ключів по відкритим каналам, алгоритми асиметричного шифрування та цифрового підпису.
3. Задачі на роботу асиметричних криптосистем: генерування ключів, шифрування/розшифрування, постановка/перевіряння цифрового підпису у схемах RSA, Ель-Гамаля, Рабіна.
4. Задачі на побудову колізій геш-функцій та оцінку стійкості від еталонних атак.
5. Задачі на побудову еліптичних кривих.

ПРИКІНЦЕВІ ПОЛОЖЕННЯ

ВИКОРИСТАННЯ ДОПОМІЖНОГО МАТЕРІАЛУ

Під час відповідей на теоретичні питання користуватися будь-якими допоміжними матеріалами та/або додатковою літературою забороняється. Для розв'язання задач дозволяється користуватися звичайним калькулятором.

КРИТЕРІЇ ОЦІНЮВАННЯ

На фаховому іспиті вступник отримує екзаменаційний білет, який включає чотири питання з переліку зазначених вище тем і розділів навчальних дисциплін: два теоретичних та два практичних. Питання розподілені по блоках даної Програми таким чином:

– одне питання: Розділ 1.;
– одне питання: Розділи 2,3.;
– одне питання: Розділ 4.;
– одне питання: Розділ 5..

Відповідь на кожне питання оцінюється у 25 балів.

Відповідь на теоретичне питання фахового іспиту оцінюється за бальною шкалою за таким порядком визначення:

- 24…25 – правильна, вичерпна відповідь, що містить всі визначення, твердження та доведення (обсяг виконання 95-100%);
- 21…23 – повна відповідь із деякими непринциповими неточностями (містить не менше 85% потрібної інформації);
- 19…20 – достатньо повна відповідь із незначними неточностями у визначеннях та/або доведеннях (містить не менше 75% потрібної інформації);
- 17…18 – достатня відповідь, яка однак містить значні неточності у визначеннях та/або доведеннях (містить не менше 65% потрібної інформації);
- 15…16 – неповна, але задовільна відповідь (містить не менше 60% потрібної інформації, окремі суттєві помилки);
- менше 15 – незадовільна відповідь із грубими помилками (містить менше 60% потрібної інформації).

Відповідь на практичне питання (задачу) фахового іспиту оцінюється за бальною шкалою за таким порядком визначення:

- 24…25 – повне, безпомилкове, відмінне розв'язання завдання (обсяг виконання 95-100%);
- 21…23 – повне розв'язання завдання з несуттєвими описками або помилками, які не впливають на основний зміст розв'язку; розв'язання, яке містить не всі необхідні пояснення (містить не менше 85% потрібної інформації);

- 19…20 – розв’язання завдання з невеликими помилками, які несуттєво впливають на основний зміст розв’язку, або без значної частини необхідних пояснень (містить не менше 75% потрібної інформації);
- 17…18 – завдання виконане задовільно, але із помилками, які впливають на зміст розв’язку, або без суттєвої частини необхідних пояснень (містить не менше 65% потрібної інформації);
- 15…16 – завдання виконане задовільно, з помилками або без необхідних теоретичних пояснень (містить не менше 60% потрібної інформації);
- менше 15 – завдання виконано незадовільно, із грубими помилками, без необхідних пояснень, або не виконано взагалі.

Загальна оцінка за фаховий іспит обчислюється як сума балів, отриманих за відповіді на кожне з чотирьох питань білету. Максимальна кількість балів – 100. Мінімальна кількість балів, що дає право продовжувати брати участь у конкурсному відборі — 60.

Одержана оцінка за фаховий іспит за стобальною шкалою перераховується в оцінку за шкалою 100..200 балів за Таблицею відповідності:

Таблиця відповідності оцінок РСО (60…100 балів)
оцінкам 200-бальної шкали (100…200 балів)

шкала РСО	шкала 100…200		шкала РСО	шкала 100…200		шкала РСО	шкала 100…200		шкала РСО	шкала 100…200
60	100		70	140		80	160		90	180
61	105		71	142		81	162		91	182
62	110		72	144		82	164		92	184
63	115		73	146		83	166		93	186
64	120		74	148		84	168		94	188
65	125		75	150		85	170		95	190
66	128		76	152		86	172		96	192
67	131		77	154		87	174		97	194
68	134		78	156		88	176		98	196
69	137		79	158		89	178		99	198
									100	200

Приклад екзаменаційного білету

Білет № 0

1. **Граничні теореми теорії ймовірностей:** слабка збіжність випадкових величин; генератриси та характеристичні функції випадкових величин; схема незалежних випробувань Бернуллі, граничні теореми Пуассона та Муавра-Лапласа; центральна гранична теорема.

2. **Системи блокового шифрування.** Схема Фейстеля та її властивості. Стандарти блокового шифрування DES та 3DES. Алгоритм шифрування ДСТУ ГОСТ 28147:2009.

3. Скільки різних генераторів мультиплікативної групи має поле F_{43}? Чи є елемент 2 генератором групи F_{43}?

4. Сформуйте спільний секретний ключ у схемі Діффі-Хеллмана, якщо $p = 43, \alpha = 3$, $k_A = 5, k_B = 7$. Опишіть покроково дії обох учасників схеми (Аліси та Боба) та результати їх обчислень.

Перелік джерел для самостійної підготовки

1. Гнєденко Б. В. Курс теорії ймовірностей. – К.: ВПЦ Київський університет, 2010. – 464 с.
2. Турчин В. Н. Теорія ймовірностей: Основні поняття, приклади, задачі: Навч. посіб. – К.: Видавництво А.С.К., 2004. – 208 с.
3. Огірко О. І., Галайко Н. В. Теорія ймовірностей та математична статистика: навчальний посібник. – Львів: ЛьвДУВС, 2017. – 292 с.
4. Турчин В. Н. Теорія ймовірностей і математична статистика. Основні поняття, приклади, задачі: Підручник для студентів вищих навчальних закладів. – Дніпропетровськ: ІМА-прес, 2014. – 556 с.
5. Дороговцев А. Я., Сільвестров Д. С., Скороход А. В., Ядренко М. Й. Теорія ймовірностей. Збірник задач. – К.: в-во «Вища школа», 1976. – 384 с.
6. Капітонова Ю. В., Кривий С. Л., Летичевський О. А. і ін. Основи дискретної математики. – Київ: в-во «Наукова думка», 2002. – 580 с.
7. Базилевич Л. Є. Дискретна математика у прикладах і задачах: підручник. – Львів: Видавець І. Е. Чижиков, 2013. – 488 с.
8. Riordan J. An Introduction to Combinatorial Analysis. – New York: John Wiley & Sons, Ins. London. Chapman & Hall, Limited, 1958.
9. Reincold E., Nievergelt J., Deo N. Combinatorial Algorithms. Theory and Practice. – New Jersey: Prentice-Hall, Inc., Englewood Cliffs, 1977.
10. Дискретний аналіз. Курс лекцій для студентів спеціальностей, пов’язаних з інформаційними технологіями та захистом інформації. Частина 1. Множини та відношення/ Укладач Мороховець М. К. – К.: НТУУ «КПІ», 2006. – 68 с.

11. Дискретний аналіз. Курс лекцій для студентів спеціальностей, пов'язаних з інформаційними технологіями та захистом інформації. Частина 4. Елементи загальної алгебри/ Укладач Мороховець М. К. – К.: КПІ ім. Ігоря Сікорського, 2015. – 81с.

12. Бородін О. І. Теорія чисел. – К.: в-во «Радянська школа», 1960. – 244 с.

13. Завадська Л. О. Спеціальні розділи математики. Елементи теорії скінченних полів. – К.: в-во «Політехніка», 2006. – 54с.

14. Ковальчук Л. В., Яремчук Ю. Є. Прикладна алгебра. Частина 1. Основи абстрактної алгебри. – Вінниця: ВНТУ, 2015. – 98 с.

15. Ковальчук Л. В., Яремчук Ю. Є. Прикладна алгебра. Частина 2. Теорія чисел. – Вінниця: ВНТУ, 2017. – 129 с.

16. Koblitz N. A course in number theory and cryptography. – N.Y.: Springer-Verlag, 1987. – P. 312.

17. Математичні методи захисту інформації. Курс лекцій. Ч І. / Укладачі Завадська Л. О., Савчук М. М. – К.: КПІ ім. Ігоря Сікорського, 2008. – 128 с.

18. Кузнецов Г. В., Фомичев В. В., Сушко С. О., Фомичова Л. Я. Математичні основи криптографії. – Дніпропетровськ: Національний гірничій університет, 2004. – Ч.1. – 391 с.

19. Вербіцький О. В. Вступ до криптології. – Львів: Науково-технічна література, 1998. – 248 с.

20. Задірака В. К., Олексюк О. С. Комп'ютерна криптологія. – К.: в-во «Вища школа», 2002. – 504 с.

21. Henk C. A. van Tilborg. Fundamentals of Cryptology. – A Professional Reference and Interactive Tutorial. – Kluwer Academic Publishers, 1999, 2000. Second Printing 2001.

22. Mao Wenbo. Modern Cryptography. Theory and Practice. Prentice Hall PTR, Upper Saddle River, New Jersey, 2004.

23. Schneier B. Applied Cryptography: protocols, algorithms and source code in C. John Wiley & Sons, New York, 1996.

Додаткова література

24. Кривий Л. С. Дискретна математика. Вибрані питання: Навч. посіб. для студ. вищ. навч. закл.– К.: Видавничий дім «Києво-Могилянська академія», 2007. – 572 с.

25. Богатирьова Ю. О. Обчислюваність на скінченних множинах та мультимножинах // Вісник Київського національного університету імені Тараса Шевченка. Сер.: фіз.-мат. науки. – 2010. – №4. – С. 88–96.

26. Клесов О. О. Елементарна теорія чисел та елементи криптографії/ підручник. – К.: ТВіМС, 2016. – 412 с.

27. Скороход А.В. Лекції з теорії випадкових процесів: Навч. посібник. – К.: Либідь, 1990. – 168 с.

28. Сушко С. О., Кузнецов В. Г., Фомичова Л. Я., Корабльов А. В. Математичні основи криптоаналізу. – Дніпро: Національний гірничий університет, 2010. – 466 с.

29. Задірака В. К., Олексюк О. С. Методи захисту фінансової інформації. – К.: в-во «Вища школа», 2002. – 457 с.

30. Alasdair McAndrew. Introduction to Cryptography with Open-Souce software. – Boca Raton London New York: CRC Press Taylor & Francis Group, 2011. – 442 p.

31. Katz Jonathan, Lindell Yehuda. Introduction to Modern Cryptography. – Boca Raton London New York: Chapman & Hall /CRC Taylor & Francis Group, 2008. – 534 p.

32. Menezes A., P. van Oorschot, S. Vanstone. Handbook of Applied Cryptography. – CRC Press, 1997. – 780 p.

Додаткові матеріали для самостійної підготовки розміщені на Youtube-каналі кафедри математичних методів захисту інформації:

https://www.youtube.com/MMIS_IPT

а також на ресурсі

https://mmis.ipt.kpi.ua/admissions/admissions-master/

Розробники програми:

_____ Савчук М. М., професор кафедри математичних методів захисту інформації, д. ф.-м. н., чл.-кор. НАНУ

_____ Яковлєв С. В., доцент кафедри математичних методів захисту інформації, к. т. н.

РЕКОМЕНДОВАНО

кафедрою математичних методів захисту інформації
Протокол № 3 від 20 березня 2024 р.

Завідувач кафедри ММЗІ _____ Сергій ЯКОВЛЄВ