КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

Затверджено на засіданні кафедри
інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
(протокол № 5 від 03.04.24)

РОБОЧА ПРОГРАМА ІСПИТУ

ПРИКЛАДНА КРИПТОЛОГІЯ

галузь знань	12 Інформаційні технології
спеціальність	125 Кібербезпека
освітня програма	125.00.01 Безпека інформаційних і комунікаційних систем

2023 – 2024 навчальний рік

1. Опис екзамену

Освітній рівень	перший (бакалаврський)
Курс	3
Семестр	4
Форма семестрового контролю	екзамен
Форма проведення	тестування в LMS MOODLE в ЕНК дисципліни
Тривалість проведення	1 год. 20 хв.
Максимальна кількість балів:	40
Критерії оцінювання:	30 балів – тестові завдання, 10 балів – задача.

Екзамен проводиться

- в університетській аудиторії у тестовій формі із використанням персональних комп'ютерів, якщо ситуація дозволяє проведення освітнього процесу офлайн;
- онлайн в режимі відеоконференції засобами Google Meet, якщо освітній процес проходить дистанційно.

Студент дає відповіді на запитання та завдання електронного тесту в системі Moodle. Всі завдання передбачають автоматичну (комп'ютерну) перевірку.

Екзамен проводиться із суворим дотриманням принципів академічної доброчесності, що передбачає недопустимість списування, фальсифікацій та обману. При порушенні студент відсторонюється від подальшого проходження екзаменаційного тесту із підсумковою оцінкою *Fx* за дисципліну. При виконанні завдань допускається користування довідковою літературою.

Підсумкова оцінка в балах (максимально 100 балів) за дисципліну є сумою результату поточного контролю за семестр (60 балів) та відповіді на екзамені (40 балів).

Перелік тем, які виносяться на екзамен (будуть представлені у вигляді тестових питань)**:**

Змістовий модуль 4. Асиметричні криптосистеми

Тема 7. Основи асиметричної криптографії

Алгебраїчні конгруенції другого степеня. Квадратичні лишки і нелишки. Критерій Ейлера. Символ Лежандра. Символ Якобі. Добування квадратних коренів за простим модулем. Добування квадратних коренів за модулем складеного числа, що є добутком двох простих чисел. Первісний корінь за модулем p^a. Дискретні логарифми (індекси).

Задачі криптології, які привели до поняття асиметричних шифрів. Поняття про однонапрямлені функції та однонапрямлені функції з лазівками.

Задачі, які приводять до однонапрямлених функцій. Принципи побудови асиметричної криптосистеми. Змішані криптосистеми. Асиметричні системи шифрування: протокол узгодження ключів Діффі-Хеллмана, криптосистема Ель-Гамаля, криптосистема *RSA*.

Змістовий модуль 5. Тестування на простоту і факторизація цілих чисел

Тема 8. Тестування на простоту і факторизація цілих чисел

Тестування на простоту та факторизація чисел. Детерміновані тести: метод пробних ділень, тест Поклінгтона. Числа Кармайкла. Ймовірнісні тести. Тест Ферма та псевдопрості числа. Тест Соловея-Штрассена та ейлерові псевдопрості числа. Тест Міллера–Рабіна та сильні псевдопрості числа. Метод Гордона побудови сильних простих чисел.

Задача і методи факторизації цілих чисел. Огляд сучасних методів факторизації. Загальні вимоги до вибору параметрів криптосистеми RSA. Атаки на криптосистему RSA: методом Ферма, методом безключового читання, повторним шифруванням, атака на основі китайської теореми про остачі.

Змістовий модуль 6. Застосування асиметричних криптосистем

Тема 9. Криптографічні хеш-функції. Аутентифікація. Генератори псевдовипадкових чисел на основі однонапрямлених функцій з лазівкою

Проблема захисту від модифікування даних. Означення та властивості хеш-функцій, побудованих на однокрокових стискуючих функціях. Типи криптографічних хеш-функцій. Хеш-функції на основі блокових шифрів. Застосування хеш-функцій у криптографії. Стандартизовані хеш-функції. Аутентифікація та цілісність повідомлень. *MAC*-коди.

Генератори псевдовипадкових чисел на основі однонапрямлених функцій з лазівкою. Генератор Блюма–Блюм–Шуба (BBS). Застосування генераторів псевдовипадкових послідовностей при ймовірнісному шифруванні. Криптосистема Блюма-Гольдвассер.

Тема 10 Електронний цифровий підпис. Елементи еліптичної криптографії

Поняття про електронний цифровий підпис. Призначення, застосування, властивості і вимоги до електронного цифрового підпису. Загальна схема побудови електронного цифрового підпису. Схеми електронного цифрового підпису: Ель-Гамаля, *DSA*, *RSA*. Стандартизовані схеми ЕЦП. Цифрові сертифікати. Атаки на електронний цифровий підпис.

Арифметика на еліптичних кривих. Використання еліптичних кривих в криптографії: обмін ключами з використанням еліптичних кривих; шифрування з використанням еліптичних кривих; електронний цифровий підпис на еліптичних кривих. Державний стандарт України 4145-2002.

Приклади тестових завдань:

1. Хеш-функція – це
a. перетворення, що дає на виході блок фіксованої довжини;
b. перетворення з секретним ключам, що має на вході та виході блоки фіксованої довжини;
c. перетворення двійкових рядків довільної довжини у двійкові блоки фіксованого розміру;

2. Абонент А хоче передати абоненту В повідомлення $m = 10$, зашифроване за допомогою алгоритму RSA, з параметрами $p = 7$, $q = 11$, і закритою експонентною $d = 47$. Обчисліть значення c зашифрованого повідомлення.
Відповідь:_____

Екзаменатор Юлія ЖДАНОВА

Завідувач кафедри Павло СКЛАДАННИЙ