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 № 6 від 13.05.26)

РОБОЧА ПРОГРАМА ІСПИТУ

ПРИКЛАДНА КРИПТОЛОГІЯ

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

Київ – 2026

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. 10 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. Первісні корені. Дискретні логарифми (індекси). Задача дискретного логарифмування в скінченному полі.

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, криптосистема Рабіна.

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

Змістовий модуль 5. Тестування на простоту та факторизація цілих чисел

Тема 8 Тестування на простоту та факторизація цілих чисел

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

Змістовий модуль 6. Застосування криптографічних алгоритмів та протоколів для захисту інформації

Тема 9. Криптографічні хеш-функції. Аутентифікація повідомлень. Електронний цифровий підпис.

Задача аутентифікації інформації. Методи контролю цілісності даних. Криптографічні хеш-функції. Типи криптографічних хеш-функцій. . Застосування хеш-функцій у криптографії. Стандартизовані хеш-функції. Державний стандарт України ДСТУ 7564:2014. Хеш-функції, побудовані на однокрокових стискуючих функціях. Хеш-функції на основі блокових шифрів. *MAC*-коди.

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.

Тема 10. Елементи еліптичної криптографії

Еліптичні криві та їх властивості. Групова операція на множині точок еліптичної кривої. Еліптичні криві над скінченним полем. Методи обчислення скалярного добутку на еліптичній кривій. Криптографічні перетворення в групах точок еліптичних кривих. Обмін ключами з використанням еліптичних кривих; шифрування з використанням еліптичних

кривих; електронний цифровий підпис на еліптичних кривих. Державний стандарт України ДСТУ 4145-2002.

Тема 11. Протоколи аутентифікації

Поняття криптографічного протоколу. Протоколи аутентифікації абонентів в інформаційних системах. Парольна аутентифікація. Протоколи аутентифікації з одноразовими паролями. Протоколи аутентифікації "запит-відповідь". Протоколи аутентифікації на основі асиметричних криптосистем. Основні атаки на протоколи аутентифікації.

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