КИЇВСЬКИЙ 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 № 12 від 01.09.2022)

РОБОЧА ПРОГРАМА ІСПИТУ

КРИПТОМЕХАНІЗМИ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ

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

2022-2023 навчальний рік

Опис програми іспиту

Київський університет імені Бориса Грінченка
Кафедра інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Програма іспиту з дисципліни «Криптомеханізми інформаційної та кібербезпеки»
4 курс – освітній рівень – перший (бакалаврський)
Спеціальність 125 Кібербезпека
Освітня програма: 125.00.01 Безпека інформаційних і комунікаційних систем
Форма проведення: комбінована
Тривалість проведення **1 год. 30 хв.**
Максимальна кількість балів: **40 балів**

Екзамен проводиться в університетській аудиторії у письменної і усної формі із використанням персональних комп'ютерів, якщо ситуація дозволяє проведення освітнього процесу офлайн. Якщо ж освітній процес проходить дистанційно, то екзамен проводиться онлайн в режимі відеоконференції засобами ZOOM.

Студент дає відповіді на питання завдань білету (40 хв) і здає відповіді викладачу. Викладач перевіряє роботи (20 хв) і оцінює їх попередньо. Наступні 30 хв в результаті співбесіди зі студентами виставляється оцінка за іспит в цілому.

Критерії оцінювання завдань відкритого типу (теорії і задач):

1. Теоретичне питання.

9-10 балів: Відмінний рівень знань (умінь), відповідь повна, вичерпна й достатньо обґрунтована з, можливими, незначними недоліками

6-8 балів: Посередній рівень знань (умінь), відповідь містить багато недоліків та / або незначну кількість помилок

3-5 балів: Мінімально допустимий рівень знань (умінь), що характеризується недостатньою обґрунтованістю, фрагментарністю; відповідь неповна, містить недоліки та помилки

2 бали: Незадовільний рівень знань, що виявляється у формальному запам'ятанні деяких понять і фактів, без належного їх розуміння, нездатності застосувати такі знання при розв'язанні задач.

0-1 бал: Незадовільний рівень знань (умінь), що виявляється у неспроможності відтворити означення понять та формулювання теорем, невмінні розв'язувати задачі.

2. Розв'язок задачі

30 балів: Повний розв'язок задачі.

15 балів: Розв'язок задачі з помилками.

0-1 бал: Незадовільний рівень розв'язку, нерозуміння постанови задачі.

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, таблицями значень функції, критеріїв та ін.

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 іспит:

1. Загрози безпеки комп'ютерних мереж і систем.
2. Методи захисту комп'ютерних мереж і систем.
3. Методи захисту від несанкціонованого доступу
4. Задачі технічного захисту інформації
5. Задачі криптографічного захисту інформації
6. Блок-схема симетричної криптосистеми
7. Блок-схема асиметричної криптосистеми
8. Модульна арифметика.
9. Кінцеві структури: групи.
10. Зворотні елементи адитивної групи.
11. Зворотні елементи мультиплікативної групи.
12. Порядок групи і порядок елемента групи.
13. Підгрупи.
14. Генератори групи і підгрупи.
15. Кількість генераторів груп і підгруп.
16. Циклічні і нециклічні групи
17. Кінцеві структури: кільця.
18. Мультиплікативна група кільця.
19. Кінцеві структури: поля.
20. Функція Ейлера.
21. Узагальнена функція Ейлера, що вона визначає.
22. Визначення НОД (a,b) за допомогою алгоритму Евкліда.
23. Мультиплікативна група кільця за модулем N = PQ.
24. Структура МГ кільця за модулем N = PQ.
25. Розподіл ключів по схемі Діффі-Гелмана (над кінцевим полем). Неінтерактивний протокол.
26. Розподіл ключів по схемі Діффі-Гелмана (над кінцевим полем). Інтерактивний протокол.
27. Криптосистема RSA. Функції шифрування-дешифрування. Ключові пари
28. Цифровий підпис RSA.
29. Криптосистема Ель-Гамаля. Напрямкове шифрування.
30. Цифровий підпис Ель-Гамаля.
31. Цифровий підпис DSA
32. Цифровий підпис ГОСТ Р34.310
33. Арифметика еліптичних кривих над полем R. Закони додавання точок.
34. Арифметика еліптичних кривих над полем F_p. . Порядок кривої. Межи Хасе.
35. Арифметика еліптичних кривих над полем F_p. Порядок точки

36.Арифметика еліптичних кривих над полем F_p. Точки 2-го і 3-го порядку, їх визначення.

37.. Безпека асиметричних КС.

38. Безпека симетричних КС. Рівні безпеки.

Приклад екзаменаційного білету:

1.Визначення кільця цілих чисел з модульною арифметикою за модулем *n*. Мультиплікативна група кільця. Порядок групи і порядки елементів. Структура групи

2. Побудувати алгоритми формування і перевірки цифрового підпису згідно DSA, якщо $P = 23$, $Q = 11$, $X_A=6$, $K_A = 5$, $h = 10$. Знайти генератор мультиплікативної підгрупи поля F_P порядку Q

Екзаменатор Анатолій БЕССАЛОВ

Завідувач кафедри Павло СКЛАДАННИЙ