Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №1

1. Означення групи, кільця і поля. Ізоморфізм та гомоморфізм груп.
2. Криптосистеми, їх різновиди та характеристика. Що називається криптографічною системою та простором ключів?
3. Зашифрувати шифром Віженера повідомлення "СТУДЕНТ" з ключем "ЗНАННЯСИЛА".

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О. І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №2

1. Означення кільці та найпростіші властивості кілець. Яка область називається областю цілісності? Навести приклади області цілісності та кільця з дільниками нуля.
2. Описати основні злостиві програми інтернету (віруси, бактерії, хробаки) та способи боротьби з ними.
3. Зашифрувати методом біграм слово англійської мови “YES” за допомогою матриці з рядками (2,3) і (7,8).

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.

Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №3

1. Означення поля. Різновиди скінченних полів. Дайте означення характеристики поля. Яке поле називається полем характеристики нуль?
2. Шифр Шаміра, його властивості. Зашифрувати повідомлення 21 цим шифром.
3. Які шифри називаються монадичними? Зашифрувати цим шифром повідомлення "ЯТИЯТИ".

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.

Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №4

1. Означення двознакових шифрів. Зашифрувати цим шифром повідомлення "алгебра", вибравши ключ PAMELI ANDERSOT
2. Довести, що кільце лишків Z_m за модулем простого числа m буде полем.
3. Області цілісності та їх властивості.

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.

Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №5

1. Означення групи та абелевої групи. Поняття нормального дільника групи та його властивості. Групи підстановок. Теорема Келі.
2. Математичні підстави шифру Шаміра. Зашифрувати повідомлення "ШАМІР" цим шифром.
3. Побудувати поле G_2^2 над полем лишків F_2 за модулем 2.

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.

Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №6

1. Означення абелевої групи. Канонічна форма елементів абелевої групи.
2. Назвати основні методи хакерських атак на криптосистеми та коротко охарактеризувати кожен метод.
3. Метод обміну ключами Діффі-Хеллмана та його основні властивості.

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.

Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №7

1. Означення криптографічного протоколу та вимоги до нього. Протоколи обміну ключами.
2. Означення односторонньої функції та односторонньої функції з додатковою інформацією.
3. Метод обміну ключами Ель-Гамаля та його основні властивості.

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №8

1. Метод крипто аналізу "крок гіганта, крок немовляти" та його математичні підстави.
2. Знайти множину твірних мультиплікативної групи поля F_{13}. Відповідь обґрунтувати.
3. Алгоритм Гауса для розв'язування системи конгруенцій. Розв'язати систему конгруенцій: $x \equiv 4(15),\ x \equiv 7(20),\ x \equiv 11(35)$.

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.

Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №9

1. Функція Ойлера та її основні властивості. Математичні підстави шифру RSA.
2. Основні небезпеки для криптографічних систем. В чому полягають небезпеки технічного та людського характеру.
3. Означення і основні різновиди криптографічних систем. Методи ламання таких систем. третього порядку. Зашифрувати шифром Віженера повідомлення «ЕКЗАМЕН», самостійно підібравши ключ.

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №10

1. Означення ін’єктивної, сюр’єктивної та бієктивної функцій. Довести, що функція, обернена до бієкції, також буде бієкцією.
2. Група підстановок та її властивості. Циклічний розклад підстановки. Парні та непарні підстановки. Симетрична група.
3. Яка користь від класичних шифрів? Зокрема, яка користь від шифру Вернама?

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №11

1. Криптографічні хеш-функції та їх основні властивості. Навести приклад криптографічної хеш-функції.
2. Протокол обміну ключами Діффі-Хелмана та його основні властивості.
3. Навести асимптотичні оцінки росту функцій та основні властивості цих оцінок.

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.

Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №12

1. Класи часової складності алгоритмів. Дати коротку характеристику цих класів і описати зв'язок теорії складності з криптографією.
2. Яке кільце називається областю цілісності? Основні властивості областей цілісності.
3. Зашифрувати алгоритмом RSA повідомлення CAR, самостійно підібравши параметри для шифру.

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.

Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №13

1. Проблема дискретного логарифма, часові характеристика складності цієї проблеми та шифр, який побудований на цій проблемі.
2. Знайти всі твірні мультиплікативної групи поля F_{13}. Скільки має бути таких твірних?
3. Зашифрувати шифром Віженера повідомлення *KUKURIKU* за допомогою ключа *RIKITI*.

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №14

1. Теорема про ділення з остачею, теореми про властивості НСД.
2. Кільця та їх властивості. Область цілісності та її властивості.
3. Зашифрувати шифром Вернама повідомлення ATTAKINTVELE за допомогою ключа такої самої довжини, що і повідомлення.

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.

Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №15

1. Означення групи, кільця і поля. Ізоморфізм та гомоморфізм груп.
2. Протокол обміну ключами Діффі-Хеллмана та його обгрунтування.
3. Зашифрувати шифром сталого значення повідомлення "СТУДЕНТ" з функцією $f(i) = i + 3$ і довжиною блока 4.

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №16

1. Означення поля та найпростіші властивості мультиплікативної групи поля.
2. Описати основні способи хакерських атак на шифри.
3. Зашифрувати методом біграм слово англійської мови "ATAS" за допомогою матриці з рядками (2,3) і (7,8).

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.

Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №17

1. Означення поля. Різновиди скінченних полів. Дайте означення характеристики поля. Яке поле називається полем характеристики нуль.
2. Тризнакові шифри. Зашифрувати повідомлення "ORTEGA" таким шифром.
3. Які шифри називаються монадичними? Зашифрувати таким шифром повідомлення "ЯТИЯТИ".

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.

Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №18

1. Означення відношення подільності та його властивості. Класи лишків за модулем простого і складеного числа.
2. Довести, що кільце лишків Z_m за модулем простого числа m буде областю цілісності.
3. Зашифрувати шифром з двома ключами повідомлення "ШИФР".

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.

Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №19

1. Означення групи та абелевої групи. Поняття нормального дільника групи та його властивості. Теорема Лагранжа.
2. Шифр Ель-Гамаля та його математичні підстави.
3. Побудувати поле G_2^2 над полем лишків F_2 за модулем 2.

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №20

1. Означення групи. Групи підстановок та їх властивості.
2. Назвати основні методи хакерських атак та коротко охарактеризувати кожен метод.
3. Метод обміну ключами Ель-Гамаля та його основні властивості.

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.

Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №21

1. Означення протоколу з нульовим розголошенням та методи побудови таких протоколів.
2. Коротко охарактеризувати алгоритм RSA та його математичні підстави.
3. Що являє собою стеганографія і в чому її сенс? Книжковий шифр та його недоліки.

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.

Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №22

1. Метод крипто аналізу "крок гіганта, крок немовляти" та його математичні підстави.
2. Знайти множину твірних мультиплікативної групи F_7. Відповідь обґрунтувати.
3. Алгоритм Гауса розв'язування системи конгруенцій. Розв'язати систему конгруенцій: $x \equiv 5(15),\ x \equiv 7(20),\ x \equiv 8(35)$.

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №23

1. Функція Ойлера та її основні властивості. Математичні підстави шифру RSA. Зашифрувати повідомлення "RSA" цим шифром.
2. Основні небезпеки для криптографічних систем. В чому полягають небезпеки технічного та виробничого характеру?
3. Означення і класи складності алгоритмічних проблем. Охарактеризувати класи PSPACE I NEXPTI

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.

Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №24

1. Означення ін'єктивної, сюр'єктивної та бієктивної функцій. Довести, що функція, обернена до бієкції, також буде бієкцією.
2. Група підстановок та її властивості. Циклічний розклад підстановки. Парні та непарні підстановки. Теорема Келі.
3. Розв'язати рівняння $213x + 134y = 1.$

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.

Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №25

1. Криптографічні хеш-функції та їх основні властивості. Навести приклад криптографічної хеш-функції.
2. Протокол обміну ключами Діффі-Хелмана та його основні властивості.
3. Обчислити $131^{131} (\mathrm{mod}\, 17)$ двома алгоритмами. Який з двох алгоритмів в даному випадку кращий?

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.

Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №26

1. Класи складності алгоритмів. Дати коротку характеристику цих класів і описати зв'язок теорії складності з криптографію.
2. Які переваги і недоліки має лінійний генератор псевдовипадкових чисел? Основні вимоги до таких генераторів.
3. Зашифрувати алгоритмом RSA повідомлення *CAA*, самостійно підібравши параметри для шифру.

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №27

1. Проблема побудови криптографічних систем. Чому проблема $\mathrm{P} \neq \mathrm{NP}$ є лише необхідною умовою стійкості криптографічної системи і не є достатньою?
2. Знайти всі твірні мультиплікативної групи поля F_{17}. Скільки має бути таких твірних?
3. Зашифрувати шифром Віженера повідомлення *KUKURIKU* за допомогою ключа *RIKI*.

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №28

1. Теорема про ділення з остачею, теореми про властивості функції Ойлера.
2. Кільця та їх властивості. Область цілісності та її властивості.
3. Зашифрувати шифром Вернама повідомлення ATTAKINTVELE за допомогою ключа такої самої довжини, що і повідомлення.

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.

Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №29

1. Підстановки. Група підстановок та її властивості. Теорема Келі.
2. Кільця та їх ідеали. Чи буде кільце, порядок якого більший 2 і в якому виконується закон ідемпотентності, областю цілісності?
3. Зашифрувати гомофонічним шифром повідомлення *PLANPILOTA* за допомогою ключа такої ж довжини, що і повідомлення.

Екзаменаційні білети затверджені на засіданні кафедри, протокол №4 від 16.11.2023 р.

Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №30

1. Функція Мебіуса та її властивості. Теорема Ойлера, теорема Ферма.
2. Поле та його порядок. Теорема про порядок елемента в полі F_q^*. Область цілісності та її властивості.
3. Зашифрувати RSA алгоритмом повідомлення *TWELVE*, підібравши потрібні значення параметрів.

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №31

1. Методи факторизації чисел. Побудова великого простого числа. .
2. Кільця та їх властивості. Ізоморфізм та гомоморфізм кільця. Фактор-кільце.
3. Зашифрувати шифром Вернама повідомлення ATTAK IN TWELVE за допомогою ключа такої самої довжини, що і повідомлення.

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №32

1. Підстановки. Група підстановок та її властивості. Теорема Келі.
2. Симетричні криптографічні системи. Приклади моно алфавітних та мультиалфавітних криптосистем.
3. Зашифрувати гомо фонічним шифром повідомлення *PLANPILOTA* за допомогою ключа такої ж довжини, що і повідомлення.

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №33

1. Теорема Ойлера, теорема Ферма. Алгоритм тестування числа на простоту на основі теореми Ферма.
2. Поле та його порядок. Теорема про порядок елемента в полі F_q^*. Область цілісності та її властивості.
3. Зашифрувати RSA алгоритмом повідомлення *ТАРАБАРА*, підібравши потрібні значення параметрів.

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №34

1. Довести, що повно циклічна група є циклічною групою. Навести приклади таких груп..
2. Дільники нуля і одиниці кільця та їх властивості. Показати, що множина дільників нуля є ідеалом кільця.
3. Зашифрувати шифром Віженера повідомлення ATTAKAINTEN за допомогою ключа такої самої довжини, що і повідомлення.

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №35

1. Блокові шифри та групи підстановок. Криптосистеми на основі підстановок. Приклади.
2. Кільця та їх ідеали. Чи буде кільце, порядок якого більший 2 і в якому виконується закон ідемпотентності, областю цілісності?
3. Зашифрувати гомо фонічним шифром повідомлення *PLANPILOTA* за допомогою ключа такої ж довжини, що і повідомлення.

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет № 36

1. Теорема Ойлера, теорема Ферма. Критерій існування розв'язку порівняння $x^2 \equiv a \ (mod\ p)$.
2. Поле та його порядок. Теорема про порядок елемента в полі F_q^*. Мультиплікативна група поля та її властивості..
3. Зашифрувати RSA алгоритмом повідомлення FIELD, підібравши потрібні значення параметрів.

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №37

1. Ентропія та її властивості. Ентропія на символ джерела. Інформаційна Надлишковість природної мови.
2. Кільця та їх властивості. Мультиплікативна група кільця. Хто є її елементами..
3. Зашифрувати шифром триграм повідомлення ATTAKINTVELE за допомогою ключа такої самої довжини, що і повідомлення.

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №38

1. Цифровий підпис на основі алгоритму RSA. Переваги та недоліки його використання.
2. Кільця та їх ідеали. В чому переваги полів над кільцями при використанні в криптографії?
3. Зашифрувати гомо фонічним шифром повідомлення CHEROKI за допомогою ключа такої ж довжини, що і повідомлення.

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет №39

1. Китайська теорема про остачі. Методи розв'язання порівнянь. Складність алгоритмів..
2. Псевдовипадкові послідовності. Генератори таких послідовностей. Різниця між випадковим числом та псевдовипадковим.
3. Зашифрувати шифром Шаміра повідомлення *TWELVE*, підібравши потрібні значення параметрів.

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет № 40

1. Кільця та їх ідеали. В чому переваги полів над кільцями при використанні в криптографії?
2. Псевдовипадкові послідовності. Генератори таких послідовностей. Різниця між випадковим числом та псевдовипадковим.
3. Зашифрувати шифром Шаміра повідомлення СНАО, підібравши потрібні значення параметрів.

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет № 41

1. Групи, абелеві групи, побудова кільця, адитивна група якого повноциклічна.
2. Ентропія та її властивості. Ентропія на символ джерела. Інформаційна Надлишковість природної мови.
3. Зашифрувати шифром Ель-Гамаля повідомлення BACELOR, підібравши потрібні значення параметрів.

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет № 42

1. Означення поля. Різновиди скінченних полів. Дайте означення характеристики поля. Яке поле називається полем характеристики нуль?
2. Шифр Шаміра, його властивості. Зашифрувати повідомлення 21 цим шифром.
3. Шифр Віженера та його варіації. До якого классу шифрів він відноситься та чому? Зашифрувати цим шифром повідомлення "ЯТИЯТИ".

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет № 43

1. Означення поля. Різновиди скінченних полів. Дайте означення характеристики поля. Яке поле називається полем характеристики нуль?
2. Тест Рабіна незвідності полінома над полем. Навести приклади тестування.
3. Шифр Віженера та його варіації. До якого классу шифрів він відноситься та чому? Зашифрувати цим шифром повідомлення "ЯТИЯТИ".

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет № 44

1. Теорема Ойлера, теорема Ферма. Критерій існування розв'язку порівняння $x^2 \equiv a \pmod p$.
2. Поле та його порядок. Теорема про порядок елемента в полі F_q^*. Мультиплікативна група поля та її властивості..
3. Зашифрувати RSA алгоритмом повідомлення FIELD, підібравши потрібні значення параметрів.

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет № 45

1. Криптосистеми, їх різновиди та характеристика. Що називається криптографічною системою та простором ключів?
2. Поле та його порядок. Теорема про порядок елемента в полі F_q^*. Мультиплікативна група поля та її властивості..
3. Зашифрувати RSA алгоритмом повідомлення FIELD, підібравши потрібні значення параметрів.

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет № 46

1. Модель математичного сейфу та її застосування для автентифікації абонентів. Алгоритм автентифікації на основі цієї моделі.
2. Група, абелева група, повноциклічна група. Застосування цих груп в криптографії.
3. Зашифрувати RSA алгоритмом повідомлення 254, підібравши потрібні значення параметрів.

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет № 47

1. Теорема Ойлера, теорема Ферма. Критерій існування розв'язку порівняння $x^2 \equiv a \ (mod\ p)$.
2. Кільце многочленів. Незвідні поліноми над полем та їх застосування до побудови скінченних полів. Тест Рабіна.
3. Зашифрувати алгоритмом Діффі-Хеллмана повідомлення 37, підібравши потрібні значення параметрів.

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет № 48

1. Довести, що повно циклічна група є циклічною групою. Навести приклади таких груп.
2. За яких умов порівняння $x^2 \equiv a \ (mod\ p)$ матиме розв'язок?
3. Зашифрувати шифром Шаміра повідомлення ATTAK IN TEN за допомогою ключа такої самої довжини, що і повідомлення.

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет № 49

1. Довести, що повно циклічна група є циклічною групою. Навести приклади таких груп.
2. За яких умов система лінійних рівнянь в кільці лишків за складеним модулем буде сумісною?
3. Зашифрувати шифром Віженера повідомлення ATTAKAINTEN за допомогою ключа такої самої довжини, що і повідомлення.

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**

Київський університет імені Тараса Шевченка
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр

Екзаменаційний білет № 50

1. Для яких порядків кільця його мультиплікативна група буде циклічною? Навести приклади таких кілець.
2. За яких умов система лінійних рівнянь в полі лишків буде сумісною?
3. Зашифрувати шифром Віженера повідомлення ATTAK IN 8 за допомогою ключа такої самої довжини, що і повідомлення.

Екзаменаційні білети затверджені на засіданні кафедри, протокол № 4 від 16.11.2023 р.
Екзаменатор **Кривий С.Л.**
Завідувач кафедри **Провотар О.І.**