БІЛЕТИ З КУРСУ МАТЕМАТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 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".

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 2

1. Означення кільця та найпростіші властивості кілець. Яка область називається областю цілісності.

2. Описати основні способи ламання шифрів.

3. Зашифрувати методом біграм слово "YES" за допомогою матриці з рядками $(2, 3)$ і $(7, 8)$.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 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 гомофонічними? Зашифрувати цим шифром повідомлення "ЯТИЯТИ"в кільці лишків Z_{25}.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 4

1. Теореми Ойлера і Ферма. Тестування числа на простоту на основі теореми Ферма.

2. Довести, що кільце лишків Z_m за модулем простого числа m буде полем.

3. Яка група називається повноциклічною? Побудувати повноциклічну групу 6-го порядку за рядком додавання з одиницею 1 3 0 5 2 4.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 5

1. Означення групи та абелевої групи. Поняття нормального дільника групи та його властивості. Теорема Лагранжа.

2. Математичні підстави шифру Шаміра. Зашифрувати повідомлення "ШАМІР" цим шифром.

3. Побудувати поле G_2^2 над полем лишків F_2 за модулем 2.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 6

1. Означення абелевої групи. Прямий добуток груп та його властивості.

2. Назвати основні методи хакерських атак на криптосистеми та коротко охарактеризувати кожний з методів.

3. Метод обміну ключами Діффі-Хеллмана та його основні властивості.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 8

1. Означення протоколу з нульовим розголошенням та методи побудови таких протоколів.

2. Означення односторонньої функції та односторонньої функції з додатковою інформацією.

3. Метод обміну ключами Ель-Гамаля та його основні властивості.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 8

1. Метод криптоаналізу "крок гіганта, крок немовляти" та його математичні підстави.

2. Знайти множину твірних мультиплікативної групи поля F_{13}. Відповідь обгрунтувати.

3. Алгоритм Гаусса розв'язання системи конгруенцій. Розв'язати систему конгруенцій: $x \equiv 4(15), x \equiv 7(20), x \equiv 11(35)$.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 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 властивості еліптичних кривих третього порядку. Навести рівняння еліптичної кривої у формі Веєрштраса.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 10

1. Означення ін'єктивної, сюр'єктивної та бієктивної функцій. Довести, що функція обернена до бієкції теж буде бієкцією.

2. Група підстановок та її властивості. Циклічний розклад підстановки. Парні та непарні підстановки. Теорема Келі.

3. Яка користь від класичних шифрів? Зокрема, яка користь від шифру Вернама?

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 11

1. Криптографічні хеш-функції та їх основні властивості. Навести приклад криптографічної хеш-функції.

2. Протокол обміну ключами Діффі-Хеллмана та його основні властивості.

3. Навести асимптотичні оцінки росту функцій та основні властивості цих оцінок.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 12

1. Класи часової складності алгоритмів. Дати коротку характеристику цих класів і описати зв'зок теорії складності з криптографією.

2. Яке кільце називається областю цілісності. Примарні кільця, теорема Гауса про циклічність мультиплікативної групи кільця.

3. Зашифрувати алгоритмом RSA повідомлення CAR, самостійно підібравши параметри для шифру.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 13

1. Китайська теорема про остачі. Побудова ізоморфізму кільця лишків та прямого добутку абелевих груп.

2. Знайти всі твірні мультиплікативної групи поля F_{11}. Скільки має бути таких твірних?

3. Зашифрувати шифром Віжінера повідомлення $KUKURIKU$ за допомогою ключа $RIKITI$.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 14

1. Теорема про ділення з остачею, теореми про властивості НСД.
2. Кільця та їх властивості. Ідеали кільця, знайти ідеали кільця лишків Z_6.
3. Зашифрувати шифром Шаміра повідомлення $ATTACKINTVELVE$.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 15

1. Означення групи, кільця і поля. Ізоморфізм та гомоморфізм груп.

2. Частотний метод криптоаналізу. Основні засади цього методу.

3. Зашифрувати за допомогою груп підстановок слово "СТУДЕНТ", підібравши самостійно підстановки для двоелементних блоків.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 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 $(7, 8)$.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 17

1. Означення поля. Різновиди скінченних полів. Просте поле та його властивості. Яке поле називається полем характеристики 0?

2. Побудувати ізоморфне відображення кілець Z_6 і кільця, яке задане рядком додавання з одиницею 1 3 0 5 2 4.

3. Навести означення класів складності PSpase і ExpTime.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 18

1. Повні та зведені системи лишків. Порівняння за модулем простого і складеного числа. Властивості цих порівнянь.

2. Довести, що кільце лишків Z_m за модулем простого числа m буде областю цілісності.

3. Зашифрувати шифром Діффі-Хеллмана повідомлення "ШИФР".

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 19

1. Означення групи та абелевої групи. Поняття нормального дільника групи та його властивості. Теорема Лагранжа та її наслідки.

2. Шифр Ель-Гамаля та його математичні підстави.

3. Побудувати поле G_2^2 над полем лишків F_2 за модулем 2.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 20

1. Означення групи. Групи підстановок та їх властивості.

2. Назвати основні методи хакерських атак на криптосистеми та коротко охарактеризувати кожний з методів.

3. Метод обміну ключами Ель-Гамаля та його основні властивості.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 21

1. Означення протоколу з нульовим розголошенням та методи побудови таких протоколів.

2. Коротко охарактеризувати алгоритм Схоуфа для обчислення числа точок на еліптичній кривій.

3. Що собою являє стеганографія і в чому її сенс. Книжковий шифр та його недоліки.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 22

1. Метод криптоаналізу "крок гіганта, крок немовляти" та його математичні підстави.

2. Знайти множину твірних мультиплікативної групи поля F_7. Відповідь обгрунтувати.

3. Алгоритм Гаусса розв'язання системи конгруенцій. Розв'язати систему конгруенцій: $x \equiv 5(15), x \equiv 7(20), x \equiv 8(35)$.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 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 характеру та виробничого характеру?

3. Означення і основні властивості еліптичних кривих третього порядку. Навести рівняння еліптичної кривої у формі Веєрштраса.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 24

1. Означення ін'єктивної, сюр'єктивної та бієктивної функцій. Довести, що функція обернена до бієкції теж буде бієкцією.

2. Група підстановок та її властивості. Циклічний розклад підстановки. Парні та непарні підстановки. Теорема Келі.

3. Розв'язати рівняння $213x + 134y = 1$.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 25

1. Криптографічні хеш-функції та їх основні властивості. Навести приклад криптографічної хеш-функції.

2. Протокол обміну ключами Діффі-Хеллмана та його основні властивості.

3. Обчислити 131^{131} $(mod\ 17)$ двома алгоритмами. Який з двох алгоритмів в даному випадку кращий?

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 26

1. Класи часової складності алгоритмів. Дати коротку характеристику цих класів і описати зв'язок теорії складності з криптографією.

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.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 27

1. Криптосистеми поділу секрета, принципи побудови, застосування.

2. Знайти всі твірні мультиплікативної групи поля F_{17}. Скільки має бути таких твірних?

3. Зашифрувати шифром Віжінера повідомлення $KUKURIKU$ за допомогою ключа $RIKI$.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 28

1. Теорема про ділення з остачею, теореми про властивості функції Ойлера.

2. Метод побудови скінченних полів за допомогою незвідного полінома. Чи довільні два поля однакового скінченного порядку ізоморфні?

3. Зашифрувати шифром Вернама повідомлення $ATTACKINTVELVE$ за допомогою ключа такої самої довжини, що і повідомлення.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 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 самої довжини, що і повідомлення.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 30

1. Функція Мебіуса та її властивості. Теорема Ойлера.

2. Поле та його порядок. Теорема про порядок елемента в полі F_q^*. Область цілісності та її властивості.

3. Лінійні конгруенці з невідомим та метод розв'язання таких конгруенцій. Формула Гауса.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 31

1. Довести примітивну рекурсивність функцій $div(x, y) = 1$ якщо x дільник y; $nd(x)$ – кількість дільників числа x.

2. Нехай розклад підстановки f на цикли має цикли довжини 3, 4, 4. Чому дорівнює f^{12}? Відповідь обгрунтувати.

3. Перерахуйте і дайте характеристику основних криптографічних атак.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 32

1. Цілком таємна криптосистема за Шенноном. Приклад такої системи.

2. Довести, що кільце лишків за модулем числа m буде полем тоді і тільки тоді, коли m просте.

3. Протокол обміну Діффі-Хеллмана. Дати характеристику і довести основні його властивості.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 33

1. Основна теорема арифметики. Найпростіші методи факторизації чисел.

2. Нехай розклад підстановки f на цикли має цикли довжини 3, 4, 4. Чому дорівнює f^{12}? Відповідь обгрунтувати.

3. Перерахуйте і дайте характеристику основних криптографічних атак.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 34

1. Метод побудови великого простого числа. Описати послідовність кроків.

2. Довести, що коли підстановка f має розклад на цикли $s_1 s_2 \cdots s_m$, то підстановка f^k матиме розклад на цикли $s_1^k s_2^k \cdots s_m^k$.

3. Алгоритми тестування чисел на простоту: метод послідовного ділення, решето Ератосфена і критерій Вільсона.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 35

1. Довести, що коли цикл підстановки s має довжину k, то $s^k = \varepsilon$, де ε – тотожна підстановка.

Користуючись цією властивістю, знайти f^{100}, де

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 1 & 7 & 10 & 2 & 6 & 9 & 8 \end{pmatrix}.$$

2. Числа Ферма і Мерсенна та їх властивості.

3. Алгоритм тестування чисел на простоту на основі малої теореми Ферма.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 36

1. Властивості умовної ймовірності. Незалежні події. Ланцюги Маркова та їх властивості.

2. Властивості функцій НСД і НСК. Алгоритми їх обчислення (Евкліда і бінарний).

3. Генератори випадкових чисел. Основні вимоги до таких генераторів та способи їх побудови.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 37

1. Числа Мерсенна і Ферма. Методи тестування цих чисел на простоту.
2. Алгоритми обчислення функції $a^d \ (mod\ m)$ та їх характеристика.
3. Ентропія та інформація. Частотна характеристика природних мов.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 38

1. Довести, що скінченна напівгрупа з одиницею і законом (лівого або правого) скорочення буде групою.
2. Довести, що коли n непарне число, то $n^2 \equiv 1 \ (mod\ 8)$.
3. На чому грунтується впевненість існування односторонніх функцій? Яке поняття припиняє своє існування, якщо $P = NP$?

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 39

1. Основні дискретні розподіли, умовна ймовірність. Властивості. Моделі M_0 і M_1 та їх характеристика.

2. Довести тотожність Гаусса: $\varphi(n) = \sum\limits_{d|n} \varphi(d) = n$.

3. Охарактеризувати основні оцінки асимптотичного порівняння функцій. Навести їх властивості.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 40

1. Довести, що ядро гомоморфізму групи буде нормальним дільником групи, а ядро гомоморфізму кільця буде його ідеалом.

2. Довести формулу обчислення функції Ойлера. Обчислити $\varphi(1600)$.

3. Теорема про основні оцінки асимптотичного порівняння функцій.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 41

1. Еліптичні криві. Вибір параметрів еліптичної кривої.
2. Цифровий підпис та принципи його побудови.
3. Навести приклади односторонніх функцій. На яких властивостях грунтується поняття односторонньої функції?

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 42

1. Електронні гроші та протоколи роботи з ними. На чому грунтується надійність роботи з ними?
2. Протоколи взаємної аутентифікації. Описати кроки.
3. Цілком таємна криптосистема за Шенноном. Приклад такої системи.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 43

1. Криптосистеми поділу секрету. Принципи побудови та властивості.
2. Протоколи взаємної аутентифікації. Описати кроки.
3. Цифровий підпис Ель-Гамаля. Побудова та властивості.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.

Київський національний університет імені Тараса Шевченка
Кафедра інформаційних систем
Математичні основи захисту інформації
4 курс ОКР "бакалавр", 8 семестр
Екзаменаційний білет N 44

1. Цифровий підпис. Умови, яким повинен задовольняти такий підпис.
2. Ентропія та інформація. Ентропія на символ джерела.
3. Цифровий підпис RSA. Побудова та властивості.

Затверджено на засіданні кафедри інформаційних систем 30.03.21 р., протокол N 10
Екзаменатор Кривий С.Л.
Зав. кафедри Провотар О.І.