|  |  |
| --- | --- |
| Державний університет "Житомирська політехніка"  Факультет інформаційно-комп’ютерних технологій  Кафедра комп’ютерної інженерії та кібербезпеки  Спеціальність: 123 "Комп’ютерна інженерія"  Спеціальність: 125 "Кібербезпека"  Освітній рівень: "бакалавр" | |
| "ЗАТВЕРДЖУЮ"  Проректор з НПР  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Морозов  «\_\_\_\_» \_\_\_\_\_\_\_\_ 2021 р. | Затверджено на засіданні кафедри  комп’ютерної інженерії та кібербезпеки, протокол № \_ від \_\_ \_\_\_\_\_\_\_\_\_ 2021 р.  Завідувач кафедри  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.А. Єфіменко  "\_\_\_\_" \_\_\_\_\_\_\_\_ 2021р. |

**ТЕСТОВІ ЗАВДАННЯ**

**3 НАВЧАЛЬНОЇ ДИСЦІПЛІНИ**

**ПРИКЛАДНА КРИПТОЛОГІЯ**

| № п/п | Текст завдання |
| --- | --- |
| **Теоретичні основи криптології. Класичні алгоритми шифрування** | |
|  | Конфіденційність інформаційних ресурсів – це… |
|  | Цілісність інформаційних ресурсів – це… |
|  | Доступність інформаційних ресурсів – це… |
|  | Криптологія – це… |
|  | Фундамент криптології як науки у 1949 р. заклала праця «Теорія зв’язку в секретних системах». Який вчений є автором цієї праці? |
|  | Набір математичних правил та процедур, який описує такі види перетворень, як шифрування, формування та перевірка ЦП, обчислення хеш-значень, криптографічних контрольних сум, створення імітовставки тощо називається криптографічний... |
|  | Ключ шифрування – це… |
|  | Початкове повідомлення, що підлягає зашифруванню прийнято називати… |
|  | Процес перетворення відкритого тексту до виду, незрозумілого несанкціонованому користувачеві називається... |
|  | За принципом Керкхофа криптографічна стійкість шифру повинна визначатися тільки... |
|  | Перетворення, при якому літери або якісь інші фрагменти відкритого тексту замінюються відповідними фрагментами шифрованого тексту називається… |
|  | Перетворення, при якому літери або якісь інші фрагменти переставляються місцями безпосередньо у відкритому тексті називається… |
|  | Метод шифрування, який застосовують до блоку відкритого тексту, який має певні розміри називається… |
|  | Метод шифрування, який застосовують до кожного знаку відкритого тексту окремо називається… |
|  | Криптосистема називається симетричною, якщо… |
|  | Криптосистема називається асиметричною, якщо … |
|  | Властивість криптосистеми протидіяти атакам супротивника, спрямованим на отримання секретного ключа або відкритого повідомлення називається... |
|  | Спроба порушення безпеки конкретної реалізації криптосистеми називається... |
|  | Шифр, в якому літера тексту циклічно замінюється на літеру в абетці на *k* позицій вперед (праворуч), де *k* – ключ, називається шифром… |
|  | Який вигляд буде мати повідомлення CAESAR після зашифрування за допомогою шифру Цезаря з ключем 3? |
|  | В якому класичному шифрі, літера, що шифрується, замінюється на її координати в квадраті? |
|  | Шифр, в якому літери повідомлення записуються як степені (їх кількість являється ключем), а потім літери в степенях записуються по рядках зверху донизу – це шифр… |
|  | Який вигляд буде мати повідомлення CRYPTOGRAPHY після зашифрування за допомогою шифру частоколу з ключем 3? |
|  | Криптоаналітик виявив, що у шифротексті LODDOB VKDO DRKX XOFOB найчастіше зустрічається літера О. Також відомо, що відкритий текст був англійською мовою та шифрувався шифром Цезаря. Яке значення найімовірніше буде мати ключ шифрування? |
|  | Відкритий текст APRICOT зашифровано за допомогою шифру Цезаря як FUWNHTY. Яку довжину ключа використано? |
|  | Шифр Цезяря є шифром… |
|  | Шифр Стародавньої Греції, де в якості носія повідомлення застосовувалася вузька та довга стрічка пергаменту (папірусу) – це... |
|  | Що являє собою ключ в криптосистемі Хілла? |
|  | У шифрі Плейфера, для того, щоб зашифрувати повідомлення необхідно спочатку… |
|  | Який шифротекст буде у результаті шифрування слова CAR за допомогою шифру Плейфера із заданою ключовою матрицею? |
|  | Яким буде результат дешифрування шифротексту HKTN за допомогою шифру Плейфера із заданою з ключовою матрицею? |
|  | Якщо слово WISDOM зашифрувати за допомогою шифру Віженера з ключем GREAT, то отримаємо шифротекст… |
|  | Шифр Віженера є шифром… |
|  | У чому полягає основна слабкість шифрів простої моноалфавітної заміни? |
|  | Метод криптоаналізу, що ґрунтується на припущенні про існування залежності між частотою появи символів відкритого тексту та символів шифротексту – це... |
|  | Індекс збігу для текстів англійською мовою становить приблизно... |
|  | Якщо текст являю собою випадкову послідовність символів, то індекс збігу становить приблизно… |
|  | Яка літера найчастіше зустрічається у текстах українською мовою? |
|  | Метод криптоаналізу, що дозволяє обчислювати період поліалфавітної криптосистеми за допомогою виявлення однакових груп символів у шифротексті – це... |
|  | Яку назву мала відома німецька шифрувальна машина, що використовувалася у часи Другої світової війни? |
| **Блокові та потокові симетричні алгоритми шифрування** | |
|  | Який загальний вигляд має функція зашифрування в симетричних криптографічних системах? |
|  | Який загальний вигляд має функція розшифрування в симетричних криптографічних системах? |
|  | Криптоаналітик виявив, що багато шифрованих листів, які фірма-виробник надсилає замовникам, починаються зі слів «У відповідь на ваше прохання…». Це дало йому змогу, перехопивши шифрований текст, відновити ключ шифру та прочитати все повідомлення. Яку атаку здійснив криптоаналітик? |
|  | Який з нижченаведених шифрів має теоретичну (абсолютну) стійкість? |
|  | У шифрі Вернама (одноразового блокноту) виконується операція… |
|  | Відкритий текст виглядає як 10010101. Чому буде дорівнювати шифротекст, якщо ключ одноразового блокноту 01010? |
|  | Відкритий виглядає як 00101010. Чому буде дорівнювати шифротекст, якщо ключ одноразового блокноту 10001010? |
|  | Шифротекст виглядає як 01001110. Чому буде дорівнювати відкритий текст, якщо ключ одноразового блокноту 01101101? |
|  | Мережа Фейстеля – це… |
|  | Довжина початкового ключа DES складає… |
|  | Довжина раундових ключів DES складає… |
|  | Початковий ключ в алгоритмі DES ділиться на 2 половини, які залежно від раунду циклічно зсуваються ліворуч на…. |
|  | Скільки раундів виконується шифрування за алгоритмом DES? |
|  | Який розмір має матриця початкової перестановки IP у алгоритмі DES? |
|  | Яке перетворення у алгоритмі DES зображено на рисунку?  Illustration of a round in a Feistel network | Download Scientific Diagram |
|  | Яке перетворення у алгоритмі DES зображено на рисунку?  Data Encryption Standard (DES) | SpringerLink |
|  | У алгоритмі DES функція Фейстеля розширює 32-бітовий вектор до 48-бітового вектора шляхом… |
|  | За допомогою S-боксів у DES перетворюється… |
|  | Скільки S-боксів у DES? |
|  | Яким буде результат S-перетворення блоку 010100 з використанням сьомого S-боксу DES? |
|  | Для здійснення атаки «грубою силою» на алгоритм DES потрібно перебрати… |
|  | Скільки ключів використовує алгоритм 3DES (Triple DES)? |
|  | У чому найбільша перевага режиму зв’язування блоків (CBC)? |
|  | Вектор ініціалізації у режимі зв’язування блоків (CBC) застосовують... |
|  | Який режим шифрування блокового симетричного алгоритму зображено на рисунку? |
|  | Який режим шифрування блокового симетричного алгоритму зображено на рисунку? |
|  | Який режим шифрування блокового симетричного алгоритму зображено на рисунку? |
|  | Який режим шифрування блокового симетричного алгоритму зображено на рисунку? |
|  | Який режим шифрування блокового симетричного алгоритму зображено на рисунку? |
|  | Як називають властивість шифру, при якій невеликі зміни в початкових даних (чи в ключі) можуть викликати значні зміни в зашифрованих даних? |
|  | Яка властивість притаманна синхронним потоковим шифрам? |
|  | Яка властивість притаманна асинхронним потоковим шифрам (шифрам, що самосинхронізуються)? |
|  | Ключовий потік – це… |
|  | З якою метою використовують генератори псевдовипадкових чисел при потоковому шифруванні? |
|  | Який з нижченаведених шифрів є потоковим? |
|  | Яким буде наступне значення, що генерується за допомогою лінійного конгруентного генератору (LCG) при початкових значеннях , , , ? |
|  | Яким буде ключовий потік, що генерує LFSR, якщо його многочлен зворотного зв’язку , а початковий стан 1101? |
|  | Яким буде стартове значення , що генерується за допомогою генератора BBS при початкових значеннях , , ? |
|  | Матриця стану алгоритму RC4 має розмір… |
|  | На рисунку подана схема роботи генератора ключового потоку шифру… |
| **Сучасні стандарти шифрування** | |
|  | В основі стандарту шифрування AES лежить алгоритм… |
|  | AES використовує \_\_\_\_\_\_\_\_\_\_ бітовий розмір блоку та розмір ключа \_\_\_\_\_\_\_\_\_\_ біт |
|  | Скільки раундів шифрування у криптографічному алгоритмі AES при довжині ключа шифрування 128 бітів? |
|  | Скільки раундів шифрування у криптографічному алгоритмі AES при довжині ключа шифрування 192 біти? |
|  | Скільки раундів шифрування у криптографічному алгоритмі AES при довжині ключа шифрування 256 бітів? |
|  | Як називають матрицю проміжного результату при шифруванні за допомогою алгоритму AES? |
|  | Який розмір має матриця стану у алгоритмі AES? |
|  | Многочлен у полі GF(28) відповідає 8-бітовому слову... |
|  | Який многочлен у полі GF(28) відповідає байту **F8** у 16-вій системі числення? |
|  | У алгоритмі AES множення елементів поля GF(28) зводиться до множення многочленів за модулем нерозкладного многочлену... |
|  | Яку кількість слів містить розширений ключ AES-128? |
|  | Яку кількість слів містить розширений ключ AES-192? |
|  | Яку кількість слів містить розширений ключ AES-256? |
|  | Яким буде результат операції додавання за модулем 2 (у 16-вій системі числення) байтів **54⊕FD** у алгоритмі AES? |
|  | Наведіть наступні чотири дії в порядку, за яким відбувається шифрування за алгоритмом AES:  1 – Зсув рядків (ShiftRows);  2 – Підстановка байтів (SubBytes);  3 – Додавання раундового ключа (AddRoundKey);  4 – Перемішування стовпців (MixColumns) |
|  | Наведіть наступні чотири дії в порядку, за яким відбувається дешифрування за алгоритмом AES:  4 – Операція, обернена до перемішування стовпців (InvMixColumns);  1 – Зсув рядків в зворотному порядку (InvShiftRows);  3 – Додавання раундового ключа (AddRoundKey);  2 – Обернена операція до підстановки байтів (InvSubBytes) |
|  | Чим відрізняється шифрування в останньому раунді алгоритму AES від шифрування у попередніх раундах? |
|  | На який байт перетвориться байт **B3** в алгоритмі AES у результаті операції Підстановка байтів (SubBytes)? |
|  | Яка операція алгоритму AES зображена на рисунку? |
|  | Яким буде результат операції Зсув рядків (ShiftRows) для заданої матриці стану в алгоритмі AES? |
|  | Масив раундових констант Rcon алгоритму AES, зображених на рисунку, використовується у процесі… |
|  | Криптографічний блоковий симетричний алгоритм перетворення даних «Калина» визначається стандартом... |
|  | Скільки таблиць замін використовується в криптографічному алгоритмі перетворення даних «Калина»? |
|  | Якщо у алгоритмі «Калина 128/256» довжина ключа шифрування 256 біт, то кількість раундів перетворень буде дорівнювати... |
|  | Якщо у алгоритмі «Калина 256/256» довжина ключа шифрування 256 біт, то кількість раундів перетворень буде дорівнювати... |
|  | Якщо у алгоритмі «Калина 256/512» довжина ключа шифрування 512 біт, то кількість раундів перетворень буде дорівнювати... |
|  | Скільки рядків має матриця стану у алгоритмі «Калина»? |
|  | Який розмір буде мати матриця стану у алгоритмі «Калина 128/256»? |
|  | Який розмір буде мати матриця стану у алгоритмі «Калина 256/512»? |
|  | Який розмір буде мати матриця стану у алгоритмі «Калина 512/512»? |
|  | У алгоритмі «Калина» множення елементів поля GF(28) зводиться до множення многочленів за модулем нерозкладного многочлену... |
|  | Яке перетворення алгоритму «Калина» зображено на рисунку? |
|  | Яке перетворення алгоритму «Калина» зображено на рисунку? |
|  | Яке перетворення алгоритму «Калина» зображено на рисунку? |
|  | Яке перетворення алгоритму «Калина» зображено на рисунку? |
|  | Яке перетворення алгоритму «Калина» зображено на рисунку? |
|  | Скільки разів виконується операція зашифрування у процесі формування допоміжного ключа? |
|  | Які раундові ключі у алгоритмі шифрування «Калина» формуються на основі ключа K та допоміжного ключа Kt з використанням двох раундів зашифрування? |
|  | Які раундові ключі у алгоритмі шифрування «Калина» формуються шляхом циклічного зсуву відносно попереднього за номером ключа? |
|  | Скільки режимів роботи алгоритму «Калина» визначено в національному стандарті шифрування? |
| **Асиметричні алгоритми шифрування** | |
|  | Ідея криптосистеми з відкритим ключем полягає у використанні… |
|  | Основоположниками криптографії з відкритим ключем є… |
|  | Яка основна перевага асиметричних шифрів над симетричними? |
|  | Як називається функція, для якої по відомому просто знайти значення , а визначити з складно? |
|  | При шифрування повідомлення як розв’язання задачі рюкзака шифротекстом виступає… |
|  | Яка інша назва криптосистеми рюкзака? |
|  | Відкритий текст виглядає як 101001, а маси предметів дорівнюють 2, 5, 8, 17, 33, 70 відповідно. Чому дорівнюватиме вага рюкзака? |
|  | Повна вага рюкзака 23, а маси предметів дорівнюють 1, 2, 4, 9, 20, 38. Чому дорівнюватиме відкритий текст? |
|  | Суперзростаюча послідовність – це послідовність, у якій кожний елемент… |
|  | Яка з наведених нижче послідовностей є суперзростаючою? |
|  | Якою буде нормальна послідовність рюкзака, якщо дано суперзростаючу послідовність 1, 3, 5, 11, 35 та параметри та ? |
|  | Знайдіть шифротекст повідомлення 1001 1101 1011 у криптосистемі рюкзака, використовуючи як відкритий ключ наступну нормальну послідовність 7, 14, 11, 5 |
|  | У криптосистемі рюкзака дешифруйте шифротекст 26, використовуючи як закритий ключ суперзростаючу послідовність 1, 2, 4, 8 та параметри та |
|  | На чому ґрунтується криптостійкість алгоритму шифрування даних RSA? |
|  | В алгоритмі RSA обираються 2 випадкові великі значення та . Якою властивістю мають володіти ці числа? |
|  | Знайдіть – модуль криптосистеми RSA, якщо та ? |
|  | Чому дорівнює в алгоритмі RSA? |
|  | Чому буде дорівнювати в алгоритмі RSA, якщо та ? |
|  | Яким чином у алгоритмі RSA отримуються відкритий та закритий ключі? |
|  | З використанням якого алгоритму можна обчислити закритий ключ у криптосистемі RSA? |
|  | Якою властивістю має володіти відкритий ключ в алгоритмі RSA? |
|  | Якщо користувач криптосистеми RSA вибрав для генерації модуля два числа та , то яку відкриту експоненту він може вибрати? |
|  | Чому буде дорівнювати закритий ключ в алгоритмі RSA, якщо та ? |
|  | Яким буде результат шифрування повідомлення = 4 у криптосистемі RSA, якщо та ? |
|  | Яким буде результат дешифрування шифротексту = 9 у криптосистемі RSA, якщо та ? |
|  | На чому ґрунтується криптостійкість алгоритму шифрування даних Ель-Гамаля? |
|  | В алгоритмі Ель-Гамаля шифротекст… |
|  | Який криптографічний алгоритм лежить в основі криптосистеми Ель-Гамаля? |
|  | Первісний корінь 7 дорівнює… |
|  | Чому буде дорівнювати у криптосистемі Ель-Гамаля відкритий ключ , якщо , , ? |
|  | Яким буде результат шифрування повідомлення = 3 із використанням сесійного ключа у криптосистемі Ель-Гамаля, якщо , , ? |
|  | Яким буде результат дешифрування шифротексту у криптосистемі Ель-Гамаля, якщо , , ? |
|  | Схема якої криптографічної системи зображена на рисунку? |
|  | Яке призначення алгоритму Діффі-Хеллмана? |
|  | На чому ґрунтується криптостійкість алгоритму Діффі-Хеллмана? |
|  | У криптографічній системі Діффі-Хеллмана спільний ключ шифрування конфіденційних повідомлень формується… |
|  | Визначте спільний секретний ключ користувачів *A* та *B*, обчислений абонентами у криптосистемі Діффі-Хеллмана, якщо , , = 4, |
|  | У схемі обміну ключами Діффі-Хеллмана обрані значення , . Які числа та розкриваються користувачами *A* та *B*, якщо їх закриті ключі = 2, відповідно? |
|  | Яким буде результат обчислення ? |
|  | Який із наведених криптографічних алгоритмів є асиметричним? |
| **Алгоритми хешування та ЦП. Криптографічні системи на еліптичних кривих** | |
|  | Хеш-функція – це математична або інша функція, яка виконує… |
|  | Що називають дайджестом повідомлення? |
|  | Колізія – це… |
|  | Блоки даних якої довжини обробляються алгоритмом хешування SHA-256? |
|  | Скільки разів виконується основний цикл хешування за алгоритмом SHA-256? |
|  | При ініціалізація значень хешу у алгоритмі SHA-256 використовуються константи, що представляють собою… |
|  | Скільки констант використовується на одному кроці функції стиснення криптографічного алгоритму SHA-256? |
|  | У алгоритмі SHA-256 фінальний хеш є конкатенацією \_\_\_\_ проміжних хеш-значень |
|  | Блоки даних якої довжини обробляються криптографічним алгоритмом хешування даних «Купина-256»? |
|  | Блоки даних якої довжини обробляються криптографічним алгоритмом хешування даних «Купина-512»? |
|  | Якій розмір має матриця стану криптографічного алгоритму хешування даних «Купина-256»? |
|  | Якій розмір має матриця стану криптографічного алгоритму хешування даних «Купина-512»? |
|  | Яку кількість раундів має функція стиснення криптографічного алгоритму хешування даних «Купина-256»? |
|  | Яку кількість раундів має функція стиснення криптографічного алгоритму хешування даних «Купина-512»? |
|  | Криптографічний алгоритм хешування даних «Купина» визначається стандартом... |
|  | Ітерація якого алгоритму хешування представлена на рисунку?  Difference Between SHA-256 and SHA-1 | Difference Between |
|  | Ітерація якого алгоритму хешування представлена на рисунку? |
|  | Оберіть найбільш повне визначення цифрового підпису серед наведених |
|  | При генерації ЦП повідомлення його дайджест шифрується за допомогою… |
|  | При перевірці ЦП повідомлення його дайджест дешифрується за допомогою… |
|  | Наведіть наступні чотири дії в порядку, за яким підписувач може створити ЦП повідомлення, а отримувач може перевірити справжність ЦП:  1 – шифрування хешу закритим ключем підписувача;  2 – порівняння надісланого хешу із обчисленим хешем повідомлення;  3 – дешифрування підпису відкритим ключем підписувача;  4 – обчислення хешу повідомлення |
|  | Що може надати можливість абонентам мережі упевнитися, що особи або організації, від яких вони отримують шифровані повідомлення, дійсно є тими, за кого вони себе видають? |
|  | У якому алгоритмі цифрового підпису формування та перевірка ЦП визначається наступними формулами: |
|  | У якому алгоритмі цифрового підпису формування та перевірка ЦП визначається наступними формулами: |
|  | У якому алгоритмі цифрового підпису формування ЦП визначається наступними формулами: |
|  | Яким буде ЦП повідомлення = 7, сформований за алгоритмом RSA, якщо та ? |
|  | Яким буде ЦП повідомлення = 4, сформований за алгоритмом Ель-Гамаля, якщо , , , ? |
|  | Стандарт цифрового підпису DSS передбачає використання хеш-алгоритму… |
|  | Який розмір хешу генерує хеш-функція SHA-1? |
|  | Українським стандартом цифрового підпису є… |
|  | Який загальний вигляд має крива, що використовується в криптографічних системах, заснованих на еліптичних кривих? |
|  | Яка точка належить еліптичній кривій ? |
|  | Які основні операції виконуються над точками еліптичних кривих при їх використанні в криптографічних системах? |
|  | Яким буде результат додавання двох точок та еліптичної кривої ? |
|  | Для еліптичної кривої обчисліть , якщо |
|  | Якщо – точка еліптичної кривої , то точка має координати… |
|  | Якщо точки , і еліптичної кривої лежать на одній прямій, заданій рівнянням , то… |
|  | Яка математична проблема забезпечує стійкість криптосистем, побудованих на еліптичних кривих? |
|  | Якщо – точка еліптичної кривої , то найменше натуральне число , при якому , називають… |
|  | Оберіть довжину ключа алгоритму ECDSA, при якому забезпечується рівень захисту, еквівалентний рівню, що дає алгоритм DSA з ключем довжиною 1024 бітів |