|  |
| --- |
| Державний університет "Житомірська політехніка"Факультет інформаційно-комп’ютерних технологійКафедра комп’ютерної інженерії та кібербезпекиСпеціальність: 121 "Інженерія програмного забезпечення"Освітній рівень: "бакалавр" |
| "ЗАТВЕРДЖУЮ"Проректор з НПР\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Морозов «\_\_\_\_» \_\_\_\_\_\_\_\_ 202\_ р. | Затверджено на засіданні кафедрикомп’ютерної інженерії та кібербезпеки, протокол № \_ від \_\_ \_\_\_\_\_\_\_\_\_ 202\_ р.Завідувач кафедри \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.А. Єфіменко "\_\_\_\_" \_\_\_\_\_\_\_\_ 202\_ р. |

**ТЕСТОВІ ЗАВДАННЯ**

**3 НАВЧАЛЬНОЇ ДИСЦІПЛІНИ**

**БЕЗПЕКА ПРОГРАМ ТА ДАНИХ**

| №п/п | Текст завдання |
| --- | --- |
| **Теоретичні основи безпеки. Класичні алгоритми шифрування** |
|  | Конфіденційність інформаційних ресурсів – це… |
|  | Цілісність інформаційних ресурсів – це… |
|  | Доступність інформаційних ресурсів – це… |
|  | Криптологія – це… |
|  | Наука про принципи, засоби та методи перетворення даних з метою приховування їх змісту, запобігання несанкціонованого використання або підробки – це… |
|  | Наука про методи та способи розкриття (зламу) зашифрованих повідомлень, а також про тактику та стратегію їх застосування – це… |
|  | 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... |
|  | 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… |
|  | 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... |
|  | Який загальний вигляд має функція зашифрування в симетричних криптографічних системах? |
|  | Який загальний вигляд має функція розшифрування в симетричних криптографічних системах? |
| **Симетричні алгоритми шифрування** |
|  | 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? |
|  | Мережа Фейстеля – це… |
|  | Довжина ключа DES складає… |
|  | Скільки раундів виконується шифрування за алгоритмом 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 |
|  | 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? |
|  | 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? |
| **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 $x^{7}+x^{5}+1$ 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 128 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? |
|  | Як називають властивість шифру, при якій невеликі зміни в початкових даних (чи в ключі) можуть викликати значні зміни в зашифрованих даних? |
|  | Який із наведених криптографічних алгоритмів є симетричним? |
| **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 $x$ просто знайти значення $f(x)$, а визначити $x$ з $f(x)$ складно? |
|  | На чому ґрунтується криптостійкість алгоритму шифрування даних RSA? |
|  | В алгоритмі RSA обираються 2 випадкові великі значення $p$ та $q$. Якою властивістю мають володіти ці числа? |
|  | Знайдіть $n$ – модуль криптосистеми RSA, якщо $p=13$ та $q=17$? |
|  | Чому дорівнює $φ(n)$ в алгоритмі RSA? |
|  | Що визначає функція Ейлера $φ(n)$ в алгоритмі RSA? |
|  | Чому буде дорівнювати $φ(n)$ в алгоритмі RSA, якщо $p=7$ та $q=11$? |
|  | 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 $e$ в алгоритмі RSA? |
|  | Якщо користувач криптосистеми RSA вибрав для генерації модуля $n$ два числа $p=7$ та $q=11$, то яку відкриту експоненту $e$ він може вибрати? |
|  | Чому буде дорівнювати закритий ключ $d$ в алгоритмі RSA, якщо $φ(n)=20$ та $e=3$? |
|  | Яким буде результат шифрування повідомлення $M$ = 4 у криптосистемі RSA, якщо $e=3$ та $n=33$? |
|  | Яким буде результат дешифрування шифротексту $C$ = 9 у криптосистемі RSA, якщо $d=3$ та $n=33$? |
|  | 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 $y$, якщо $p=13$, $g=7$, $x=2$? |
|  | Яким буде результат шифрування повідомлення $M$ = 3 із використанням сесійного ключа $k=2$ у криптосистемі Ель-Гамаля, якщо $p=7$, $g=3$, $y=5$? |
|  | Яким буде результат дешифрування шифротексту $(a, b)=(6, 2)$ у криптосистемі Ель-Гамаля, якщо $p=7$, $g=3$, $x=5$? |
|  | 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 $p=11$, $g=2$, $x$ = 4, $y=3$ |
|  | У схемі обміну ключами Діффі-Хеллмана обрані значення $p=19$, $g=10$. Які числа $x\_{A}$ та $y\_{B}$ розкриваються користувачами *A* та *B*, якщо їх закриті ключі $x$ = 2, $y=3$ відповідно? |
|  | Яким буде результат обчислення $5^{-1}(mod 14)$? |
|  | Який із наведених криптографічних алгоритмів є асиметричним? |
| **Хешування та ЦП. Криптографічні системи на еліптичних кривих** |
|  | Хеш-функція – це математична або інша функція, яка виконує… |
|  | Що називають дайджестом повідомлення?  |
|  | Яка основна вимога висувається до криптографічної хеш-функції? |
|  | Колізія – це… |
|  | Оберіть найбільш повне визначення цифрового підпису серед наведених |
|  | Цифровий підпис повідомлення не завжди забезпечує… |
|  | 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:$$S=h(M)^{d}mod n$$$$S^{e}mod n=h(M)$$ |
|  | У якому алгоритмі цифрового підпису формування та перевірка ЦП визначається наступними формулами:$$ r=g^{k}mod p$$$$s=k^{-1}\left(h\left(M\right)-xr\right)mod p-1$$$$g^{h(M)}≡y^{r}r^{s}(mod p)$$ |
|  | У якому алгоритмі цифрового підпису формування ЦП визначається наступними формулами:$$r=\left(g^{k}mod p\right) mod q$$$$s=k^{-1}\left(h\left(M\right)+xr\right)mod q$$ |
|  | Яким буде ЦП повідомлення $h(M)$ = 7, сформований за алгоритмом RSA, якщо $d=3$ та $n=33$? |
|  | Яким буде ЦП повідомлення $h(M)$ = 4, сформований за алгоритмом Ель-Гамаля, якщо $p=7$, $g=3$, $x=4$, $k=5$? |
|  | Стандарт цифрового підпису DSS передбачає використання хеш-алгоритму… |
|  | Який загальний вигляд має крива, що використовується в криптографічних системах, заснованих на еліптичних кривих? |
|  | Яка точка належить еліптичній кривій $y^{2}≡x^{3}+4x+1 (mod 7)$? |
|  | Які основні операції виконуються над точками еліптичних кривих при їх використанні в криптографічних системах? |
|  | Яким буде результат додавання двох точок $P(1, 2)$ та $Q(4, 2)$ еліптичної кривої $E\_{11}=(1, 2)$? |
|  | Для еліптичної кривої $E\_{13}=(1,1)$ обчисліть $2P$, якщо $P(1, 4)$  |
|  | Якщо $P(13, 7)$ – точка еліптичної кривої $E\_{23}=(1, 1)$, то точка $-P$ має координати… |
|  | Якщо точки $P$, $Q$ і $R$ еліптичної кривої лежать на одній прямій, заданій рівнянням $y^{2}≡x^{3}+ax+b (mod p)$, то… |
|  | Яка математична проблема забезпечує стійкість криптосистем, побудованих на еліптичних кривих? |
|  | Якщо $P$ – точка еліптичної кривої $E\_{p}=(a, b)$, то найменше натуральне число $n$, при якому $nP = O$, називають… |
|  | Оберіть довжину ключа алгоритму ECDSA, при якому забезпечується рівень захисту, еквівалентний рівню, що дає алгоритм DSA з ключем довжиною 1024 бітів |