|  |  |
| --- | --- |
| Дердавний університет "Житомірська політехніка"  Факультет інформаційно-комп’ютерних технологій  Кафедра комп’ютерної інженерії та кібербезпеки  Спеціальність: 121 "Інженерія програмного забезпечення"  Освітній рівень: "бакалавр" | |
| "ЗАТВЕРДЖУЮ"  Проректор з НПР  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Морозов  «\_\_\_\_» \_\_\_\_\_\_\_\_ 2020 р. | Затверджено на засіданні кафедри  комп’ютерної інженерії та кібербезпеки, протокол № \_\_\_ від \_\_ \_\_\_\_\_\_\_\_\_\_ 2020 р.  Завідувач кафедри  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.А. Єфіменко  "\_\_\_\_" \_\_\_\_\_\_\_\_ 2020 р. |

Питання

**3 НАВЧАЛЬНОЇ ДИСЦІПЛІНИ**

**БЕЗПЕКА ПРОГРАМ ТА ДАНИХ**

| № п/п | Текст завдання |
| --- | --- |
| 1. 1 | Що називається інформацією? |
| 1. 2 | Під інформаційною безпекою розуміють: |
| 1. 3 | Безпека інформації - це: |
| 1. 4 | Захист інформації - це: |
| 1. 5 | Ідентифікація об’єктів і суб’єктів в інформаційної системі - це: |
| 1. 6 | Автентифікація об’єктів і суб’єктів в інформаційної системі - це: |
| 1. 7 | Авторизація об’єктів і суб’єктів в інформаційної системі - це: |
| 1. 8 | Конфіденційність інформації: |
| 1. 9 | Цілісність інформації: |
| 1. 1 | Доступність інформації: |
| 1. 1 | Автентичність інформації (користувача): |
| 1. 1 | Володіння інформацією: |
| 1. 1 | Корисність інформації: |
| 1. 1 | Криптографічні методи захисту інформації призначаються для |
| 1. 1 | Криптографічні методи захисту інформації призначаються для |
|  | Криптографічні методи захисту інформації призначаються для |
| 1. 2 | Зашифрування даних - це: |
| 1. 2 | Ключ шифрування - це: |
| 1. 2 | Розшифрування даних - це: |
| 1. 3 | На які категорії поділяються класичні історичні криптографічні системи (шифри) з симетричним ключем: |
| 1. 3 | На які категорії поділяються класичні історичні криптографічні системи (шифри) з симетричним ключем: |
| 1. 3 | Який загальний вигляд має функція зашифрування в симетричних криптографічних системах? |
| 1. 3 | Який загальний вигляд має функція розшифрування в симетричних криптографічних системах? |
| 1. 3 | Симетричне криптографічне шифрування даних – це: |
| 1. 3 | Симетричне криптографічне шифрування даних поділяють на: |
| 1. 3 | Симетричне криптографічне шифрування даних поділяють на: |
| 1. 3 | Криптографічне шифрування даних системами з відкритими ключами – це: |
| 1. 3 | В докомп’ютерних (історичних) шифрах підстановки: |
| 1. 3 | В докомп’ютерних (історичних) шифрах перестановки: |
| 1. 4 | Шифри гамування в якості ключа шифрування використовують: |
| 1. 4 | Схема якого шифру зображена на рисунку: |
| 1. 4 | Схема якого шифру зображена на рисунку: |
| 1. 4 | Встановіть відповідність між шифром і відповідним виразом для зашифрування адитивним шифром: |
| 1. 4 | Встановіть відповідність між шифром і відповідним виразом для зашифрування афінним шифром: |
| 1. 4 | Встановіть відповідність між шифром і відповідним виразом для зашифрування шифром Вернама: |
|  | Криптографічний алгоритм AES обробляє блоки даних довжиною (в байтах): |
|  | Криптографічний алгоритм AES використовує ключі шифрування довжиною (в байтах): |
|  | Криптографічний алгоритм AES використовує ключі шифрування довжиною (в байтах): |
|  | Криптографічний алгоритм AES використовує ключі шифрування довжиною (в байтах): |
|  | Кількість раундів шифрування криптографічного алгоритму AES при довжині ключа шифрування 128 бітів становитиме: |
|  | Кількість раундів шифрування криптографічного алгоритму AES при довжині ключа шифрування 192 бітів становитиме: |
|  | Кількість раундів шифрування криптографічного алгоритму AES при довжині ключа шифрування 256 бітів становитиме: |
|  | Яка колова функція алгоритму зашифрування даних криптографічного алгоритму AES використовується першої в повному раунді перетворень: |
|  | Яка колова функція криптографічного алгоритму зашифрування даних AES використовується другої в повному раунді перетворень: |
|  | Яка колова функція криптографічного алгоритму зашифрування даних AES використовується третьої в повному раунді перетворень: |
|  | Яка колова функція криптографічного алгоритму зашифрування даних AES використовується четвертої в повному раунді перетворень: |
|  | Яка колова функція криптографічного алгоритму зашифрування даних AES використовується п’ятої в повному раунді перетворень: |
|  | Яка колова функція криптографічного алгоритму зашифрування даних AES не використовується в неповному раунді перетворень: |
|  | Яка колова функція криптографічного алгоритму зашифрування даних AES використовується в нульовому раунді перетворень: |
|  | Раундове перетворення SubBytes (InvSubBytes) криптографічного алгоритму AES відповідає за: |
|  | Раундове перетворення ShiftRows (InvShiftRows) криптографічного алгоритму AES відповідає за: |
|  | Раундове перетворення MixColumns (InvMixColumns) криптографічного алгоритму AES відповідає за: |
|  | Яка колова функція криптографічного алгоритму криптографічного при оберненому (інверсному) розшифруванні даних використовується першої в повному раунді перетворень: |
|  | Яка колова функція криптографічного алгоритму AES при оберненому (інверсному) розшифруванні даних використовується другої в повному раунді перетворень: |
|  | Яка колова функція криптографічного алгоритму AES при оберненому (інверсному) розшифруванні даних використовується третьої в повному раунді перетворень: |
|  | Яка колова функція криптографічного алгоритму AES при оберненому (інверсному) розшифруванні даних використовується четвертої в повному раунді перетворень: |
|  | Яка колова функція криптографічного алгоритму AES при прямому (еквівалентному) розшифруванні даних використовується першої в повному раунді перетворень: |
|  | Яка колова функція криптографічного алгоритму AES при прямому (еквівалентному) розшифруванні даних використовується другої в повному раунді перетворень: |
|  | Яка колова функція криптографічного алгоритму AES при прямому (еквівалентному) розшифруванні даних використовується третьої в повному раунді перетворень: |
|  | Яка колова функція криптографічного алгоритму AES при прямому (еквівалентному) розшифруванні даних використовується четвертої в повному раунді перетворень: |
|  | Скільки слів потрібно сформувати для формування раундових ключів криптографічного алгоритму AES-128: |
|  | Скільки слів потрібно сформувати для формування раундових ключів криптографічного алгоритму AES-192: |
|  | Скільки слів потрібно сформувати для формування раундових ключів криптографічного алгоритму AES-256: |
|  | У константі Rcon (Round Constant) криптографічного алгоритму AES три з чотирьох байтів є завжди нульовими. Які саме? |
|  | Криптографічний блоковий симетричний алгоритм перетворення даних "Калина" обробляє блоки даних довжиною: |
|  | Криптографічний блоковий симетричний алгоритм перетворення даних "Калина" обробляє блоки даних довжиною: |
|  | Криптографічний блоковий симетричний алгоритм перетворення даних "Калина" обробляє блоки даних довжиною: |
|  | Для чого призначена функція Box (Box-1) в криптографічному блоковому симетричному алгоритмі перетворення даних "Калина": |
|  | Для чого призначена функція Rows (Rows-1) в криптографічному блоковому симетричному алгоритмі перетворення даних "Калина": |
|  | Для чого призначена функція Col (Col-1) в криптографічному блоковому симетричному алгоритмі перетворення даних "Калина": |
|  | Загальна схема якого криптографічного алгоритму наведена на рисунку? |
|  | Загальна схема якого криптографічного алгоритму наведена на рисунку? |
|  | Якщо довжина ключа шифрування в криптографічному алгоритмі перетворення даних "Калина 128" 128 бітів, то кількість раундів перетворень буде дорівнювати: |
|  | Якщо довжина ключа шифрування в криптографічному алгоритмі перетворення даних "Калина 256" 128 бітів, то кількість раундів перетворень буде дорівнювати: |
|  | Якщо довжина ключа шифрування в криптографічному алгоритмі перетворення даних "Калина 512" 128 бітів, то кількість раундів перетворень буде дорівнювати: |
|  | Якщо довжина ключа шифрування в криптографічному алгоритмі перетворення даних "Калина 128" 256 бітів, то кількість раундів перетворень буде дорівнювати: |
|  | Якщо довжина ключа шифрування в криптографічному алгоритмі перетворення даних "Калина 256" 256 бітів, то кількість раундів перетворень буде дорівнювати: |
|  | Якщо довжина ключа шифрування в криптографічному алгоритмі перетворення даних "Калина 512" 256 бітів, то кількість раундів перетворень буде дорівнювати: |
|  | Якщо довжина ключа шифрування в криптографічному алгоритмі перетворення даних "Калина 128" 512 бітів, то кількість раундів перетворень буде дорівнювати: |
|  | Якщо довжина ключа шифрування в криптографічному алгоритмі перетворення даних "Калина 256" 512 бітів, то кількість раундів перетворень буде дорівнювати: |
|  | Якщо довжина ключа шифрування в криптографічному алгоритмі перетворення даних "Калина 512" 512 бітів, то кількість раундів перетворень буде дорівнювати: |
|  | Раундовий (цикловий) ключ в криптографічному алгоритмі перетворення даних "Калина" - це: |
|  | Скільки таблиць замін використовується в криптографічному алгоритмі перетворення даних "Калина" при шифруванні даних? |
|  | Які раундові (циклові) ключі в криптографічному алгоритмі перетворення даних "Калина" формуються шляхом використання повної схеми розгортання ключів? |
|  | Які раундові (циклові) ключі в криптографічному алгоритмі перетворення даних "Калина" формуються шляхом зсуву відносно попереднього за номером? |
|  | Яка довжина раундових (циклових) ключів в криптографічному алгоритмі перетворення даних "Калина 128", якщо довжина секретного ключа шифрування даних дорівнює 128 бітів? |
|  | Яка довжина раундових (циклових) ключів в криптографічному алгоритмі перетворення даних "Калина 128", якщо довжина секретного ключа шифрування даних дорівнює 256 бітів? |
|  | Яка довжина раундових (циклових) ключів в криптографічному алгоритмі перетворення даних "Калина 256", якщо довжина секретного ключа шифрування даних дорівнює 256 бітів? |
|  | Яка довжина раундових (циклових) ключів в криптографічному алгоритмі перетворення даних "Калина 512", якщо довжина секретного ключа шифрування даних дорівнює 512 бітів? |
|  | Який розмір буде мати матриця стану в криптографічному алгоритмі перетворення даних "Калина 128", якщо довжина секретного ключа шифрування даних дорівнює 128 бітів? |
|  | Який розмір буде мати матриця стану в криптографічному алгоритмі перетворення даних "Калина 128", якщо довжина секретного ключа шифрування даних дорівнює 256 бітів? |
|  | Який розмір буде мати матриця стану в криптографічному алгоритмі перетворення даних "Калина 256", якщо довжина секретного ключа шифрування даних дорівнює 256 бітів? |
|  | Який розмір буде мати матриця стану в криптографічному алгоритмі перетворення даних "Калина 256", якщо довжина секретного ключа шифрування даних дорівнює 512 бітів? |
|  | Який розмір буде мати матриця стану в криптографічному алгоритмі перетворення даних "Калина 512", якщо довжина секретного ключа шифрування даних дорівнює 512 бітів? |
|  | Визначити назву режиму шифрування даних криптографічним алгоритмом "Калина" ECB: |
|  | Визначити назву режиму шифрування даних криптографічним алгоритмом "Калина" CTR: |
|  | Визначити назву режиму шифрування даних криптографічним алгоритмом "Калина" CBC: |
|  | Визначити назву режиму шифрування даних криптографічним алгоритмом "Калина" OFB: |
|  | Схема якого режиму шифрування криптографічного алгоритму "Калина" зображена на рисунку: |
|  | Схема якого режиму шифрування криптографічного алгоритму "Калина" зображена на рисунку: |
|  | Схема якого режиму шифрування криптографічного алгоритму "Калина" зображена на рисунку: |
|  | Схема якого режиму шифрування криптографічного алгоритму "Калина" зображена на рисунку: |
|  | Схема якого режиму шифрування криптографічного алгоритму "Калина" зображена на рисунку: |
|  | Схема якого режиму шифрування криптографічного алгоритму "Калина" зображена на рисунку: |
|  | Схема якого режиму шифрування криптографічного алгоритму "Калина" зображена на рисунку: |
|  | Схема якого режиму шифрування криптографічного алгоритму "Калина" зображена на рисунку: |
|  | Для чого призначена криптографічна система Діффі-Хеллмана? |
|  | Абонент A для зашифрування та передачі конфіденційного повідомлення абоненту B формує секретний спільний ключ шифрування з використанням виразу (використовується система Діффі-Хеллмана): |
|  | Абонент B для зашифрування та передачі конфіденційного повідомлення абоненту A формує секретний спільний ключ шифрування з використанням виразу (використовується система Діффі-Хеллмана): |
|  | Схема якої криптографічної системи зображена на рисунку: |
|  | Криптографічна система Діффі-Хеллмана забезпечує: |
|  | На чому основується криптостійкість алгоритму шифрування даних RSA? |
|  | Які вимоги повинні виконуватися під час визначення загальних параметрів схеми шифрування даних RSA? |
|  | В схемі шифрування даних RSA приватні ключі отримуються: |
|  | Алгоритм зашифрування даних в схемі RSA при передачі конфіденційного повідомлення від користувача A до користувача B: |
|  | Схема якої криптографічної системи зображена на рисунку? |
|  | Які недоліки присутні в алгоритмі шифрування даних RSA? |
|  | Які недоліки присутні в алгоритмі шифрування даних RSA? |
|  | На чому основується криптостійкість алгоритму шифрування даних Ель-Гамаля? |
|  | Які вимоги повинні виконуватися під час визначення загальних параметрів схеми шифрування даних Ель-Гамаля: |
|  | Алгоритм зашифрування даних в схемі Ель-Гамаля при передачі конфіденційного повідомлення від користувача A до користувача B: |
|  | Алгоритм розшифрування даних в схемі Ель-Гамаля при передачі конфіденційного повідомлення від користувача A до користувача B: |
|  | Для чого в алгоритмі шифрування даних Ель-Гамаля використовується секретне випадкове число k? |
|  | Які недоліки присутні в алгоритмі шифрування даних Ель-Гамаля? |
|  | Схема якої криптографічної системи зображена на рисунку: |
|  | MDC це: |
|  | Яка довжина дайджесту формується криптографічним алгоритмом гешування даних SHA-1? |
|  | Блоки даних якої довжини обробляються криптографічним алгоритмом гешування даних SHA-1? |
|  | Підблоки (регістри) даних якої довжини обробляються функцією стиску криптографічного алгоритму гешування даних SHA-1? |
|  | З якій кількості раундів складається функція стиснення криптографічного алгоритму гешування даних SHA-1? |
|  | З якій кількості кроків складається один раунд функції стиснення криптографічного алгоритму гешування даних SHA-1? |
|  | Скільки констант використовується на одному кроці функції стиснення криптографічного алгоритму гешування даних SHA-1? |
|  | Скільки констант використовується в одному раунді функції стиснення криптографічного алгоритму гешування даних SHA-1? |
|  | Скільки констант використовується функцією стиснення криптографічного алгоритму гешування даних SHA-1? |
|  | В функції стиснення навчального криптографічного алгоритму гешування даних SHA-1 довжина даних, які обробляються дорівнює 4-м бітам. Визначити результат примітивної логічної функції “якщо b, то с інакше d”. Зміст регістрів B = 716, C = 816, D = A16. |
|  | В функції стиску навчального криптографічного алгоритму гешування даних SHA-1 довжина даних, які обробляються дорівнює 4-м бітам. Визначити результат примітивної логічної функції “біт парності”. Зміст регістрів B = E16, C = 716, D = A16. |
|  | В функції стиснення навчального криптографічного алгоритму гешування даних SHA-1 довжина даних, які обробляються дорівнює 4-м бітам. Визначити результат примітивної логічної функції c (b v ), якщо зміст регістрів B = 716, C = 816, D = A16. |
|  | Яка довжина дайджесту формується криптографічним алгоритмом гешування даних SHA-512? |
|  | Блоки даних якої довжини обробляються криптографічним алгоритмом гешування даних SHA-512? |
|  | З якій кількості раундів складається функція стиснення криптографічного алгоритму гешування даних SHA-512? |
|  | Яка кількість різних констант використовується функцією стиснення криптографічного алгоритму гешування даних SHA-512? |
|  | Скільки підблоків даних використовуються функцією стиснення криптографічного алгоритму гешування даних SHA-512? |
|  | В функції стиснення навчального криптографічного алгоритму гешування даних SHA-512 довжина даних, які обробляються дорівнює 4-м бітам. Визначити результат примітивної логічної "мажоритарної" функції". Зміст регістрів E = 716, F = C16, G = B16. |
|  | В функції стиснення навчального криптографічного алгоритму гешування даних SHA-512 довжина даних, які обробляються дорівнює 4-м бітам. Визначити результат примітивної логічної функції "якщо e, то f, інакше g". Зміст регістрів E = 716, F = 816, G = 316. |
|  | Блоки даних якої довжини обробляються криптографічним алгоритмом гешування даних Купина-256? |
|  | Блоки даних якої довжини обробляються криптографічним алгоритмом гешування даних Купина-512? |
|  | Якій розмір має матриця внутрішнього стану криптографічного алгоритму гешування даних Купина-256? |
|  | Якій розмір має матриця внутрішнього стану криптографічного алгоритму гешування даних Купина-512? |
|  | Яку кількість раундів має функція стиснення криптографічного алгоритму гешування даних Купина-256? |
|  | Яку кількість раундів має функція стиснення криптографічного алгоритму гешування даних Купина-512? |
|  | Оберіть злочинну дію, яка відноситься до активного перехоплення: |
|  | Оберіть злочинну дію, яка відноситься до маскараду: |
|  | Оберіть злочинну дію, яка відноситься до ренегатства: |
|  | Оберіть злочинну дію, яка відноситься до підміни: |
|  | Оберіть злочинну дію, яка відноситься до повтору: |
|  | При формування цифрового підпису схемою RSA він визначається за формулою: |
|  | При перевірянні цифрового підпису схемою RSA він визначається за формулою: |
|  | При формування цифрового підпису схемою Ель-Гамаля перше число цифрового підпису визначається за формулою: |
|  | При формування цифрового підпису схемою Ель-Гамаля друге число цифрового підпису визначається за формулою: |
|  | При формування цифрового підпису схемою DSA перше число цифрового підпису визначається за формулою: |
|  | При формування цифрового підпису схемою DSA друге число цифрового підпису визначається за формулою: |
|  | Яка крива використовується в криптографічних системах, стійкість яких заснована на звичайних еліптичних функціях: |
|  | Які основні операції, які виконуються над точками несингулярних еліптичних кривих при використанні них в криптографічних системах: |
|  | Як формується секретний ключ для криптографічної системи цифрового підпису з використанням еліптичних кривих ECDSA? |
|  | Алгоритм формування другого числа (s) криптографічної системи цифрового підпису з використанням еліптичних кривих ECDSA |