1. Що таке криптографія та які її основні цілі?   
   **Криптограафія** — наука про математичні методи забезпечення конфіденційності, цілісності і автентичності інформації.   
   Основні цілі:
   1. **Конфіденційність інформації** — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом.
   2. **Цілісність даних** — підтримка та забезпечення точності та цілісності даних протягом всього життєвого циклу, що є критично важливим аспектом при проектуванні, впровадженні та експлуатації систем, які зберігають, обробляють та постачають дані.
   3. **Автентичність інофрмації** — доказ походження інформації,
2. Які властивості інформації захищаються криптографічними засобами?
3. Що називається ключем шифрування?
   1. Ключ — параметр криптографічної системи, який використовується для
      1. шифрування і/або дешифрування повідомлення при шифруванні;
      2. накладення та перевірки коду автентифікації повідомлень або електронного цифрового підпису.
4. Яку архітектуру має криптографічна система?
5. У чому полягає принцип Керкхоффса?
   1. Основне правило криптографії - використовувати відкриті й опубліковані алгоритми та протоколи
   2. Вперше цей головний принцип був сформульований у 1883 році Агустом Керкхгоффсом (A.Kerckhoffs): в криптографічній системі єдиним секретом має залишатися ключ, сам же алгоритм не повинен бути засекречений.
6. Коли у криптографії почали використовуватися наукові підходи?
7. Як класифікуються алгоритми шифрування?
   1. Симетричні - У шифруванні симетричними ключами застосовується єдиний ключ засекречування і для шифрування, і для розшифровки
   2. Асиметричні - По-перше, ми маємо два ключа замість одного: з них один відкритий ключ ( public key ) , інший - індивідуальний або секретний ( private key )
8. Які шифри називаються історичними?
9. Поясніть різницю між симетричним та асиметричним шифруванням. Наведіть приклади кожного типу шифрування.
   1. Симетричні - У шифруванні симетричними ключами застосовується єдиний ключ засекречування і для шифрування, і для розшифровки  
      Приклад – шифр Цезаря
   2. Асиметричні - По-перше, ми маємо два ключа замість одного: з них один відкритий ключ ( public key ) , інший - індивідуальний або секретний ( private key )  
      Приклад – протокол TLS та SSL
10. Що таке криптографічний ключ? Які вимоги до криптографічних ключів?
11. Як працює алгоритм RSA? Опишіть процес створення ключів та процес шифрування/розшифрування повідомлень.
    1. Система ґрунтується на використанні іншої односторонньої функції. В цій системі використовуються наступні факти з теорії чисел:   
       1. Задача перевірки числа на простоту є порівняно простою.   
       2. Задача розкладання числа n=p\*q, де p і q – прості числа, на множники є дуже складною задачею, якщо ми знаємо тільки n, а p і q – великі числа (задача факторизації).   
       В групі абонентів A,B,C,… кожний абонент:   
       1. Вибирає випадково два великих простих числа P і Q і обчислює **N=PQ**  
       2. Обчислює число **f=(P-1)(Q-1)**.  
       3. Вибирає деяке число **d<f**, взаємно просте з f, і за розширеним алгоритмом Евкліда знаходить таке c, що **cd mod f=1**В результаті отримуємо таблицю ключів:

|  |  |  |
| --- | --- | --- |
| Абонент | Секретний ключ | Відкритий ключ |
| A | PA,QA,CA | NA, dA |
| B | PB,QB,CB | NB, dB |
| C | PC,QC,CC | NB, dB |
| … | … | … |

Нехай A хоче передати B повідомлення m< NB. Протокол передачі складається з таких кроків:  
1. Абонент A шифрує повідомлення, використовуючи відкриті параметри абонента B: 𝑒 = 𝑚𝑑𝐵 𝑚𝑜𝑑 𝑁B

2. Абонент B, отримавши зашифроване повідомлення, обчислює 𝑚′ = 𝑒 𝑐𝐵 𝑚𝑜𝑑 𝑁B**Приклад**. Нехай абонент А передає абоненту B повідомлення m=15. Нехай абонент B обрав для себе секретне число PB=3, QB=11, NB=33 і dB=3.За допомогою розширеного алгоритму Евкліда знаходимо сB=7. Тоді e=153 mod 33=9. Це число передається абоненту B. Тільки абонент B знає сB, тому він розшифровує m'=97 mod 33=15.

1. Що таке хеш-функція і які основні властивості вона повинна мати?
2. Поясніть принцип цифрового підпису. Які переваги вона надає у сфері безпеки інформації?
   1. **Електронний цифровий підпис** (ЕЦП) — вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача.  
      Переваги:
      1. Конфіденційність і безпека інформації
      2. Можливість ведення електронного документообігу з державними структурами
      3. Юридична сила електронних документів
3. Які основні принципи протоколів автентифікації та ключового обміну?
4. Що таке блокові та потокові шифри? Які їх основні відмінності та переваги?
   1. Блоковий шифр — різновид симетричного шифру. Особливістю блочного шифру є обробка блоку декількох байт за одну ітерацію (як правило 8 або 16).
   2. Потоковий шифр - група симетричних шифрів, які шифрують кожен символ відкритого тексту незалежно від інших символів.

|  |  |  |
| --- | --- | --- |
| **Основа для порівняння** | **Блоковий шифр** | **Шифр потоку** |
| Основний | Перетворює звичайний текст, приймаючи його блок за один раз. | Перетворює текст, приймаючи один байт звичайного тексту одночасно. |
| Складність | Простий дизайн | Комплекс порівняно |
| Кількість використаних бітів | 64 біта або більше | 8 біт |
| Плутанина і дифузія | Використовує як плутанину, так і дифузію | Покладається тільки на плутанину |
| Використовуються режими алгоритму | ЄЦБ (електронна книга коду) CBC (Cipher Block Chaining) | CFB (Cipher Feedback) OFB (вихідна зворотний зв'язок) |
| Оборотність | Скасування зашифрованого тексту важке. | Він використовує XOR для шифрування, який можна легко змінити на звичайний текст. |
| Реалізація | Feistel Cipher | Vernam Cipher |

1. Які методи симетричного шифрування широко використовуються нині? Обговоріть їх переваги та недоліки.
2. Що таке атака за часом (timing attack) у криптографії? Яких заходів можна вжити для захисту від неї?
   1. Атака по часу (англ. timing attack) — це атака стороннім каналом, в якій нападник загрожує криптосистемі, аналізуючи час потрібний для виконання криптографічних алгоритмів. Кожна логічна дія на комп'ютері вимагає певного часу, і цей час може різнитись залежно від даних на вході; через точне вимірювання тривалості кожної операції, нападник може відновити подані на вхід дані.
   2. Атака по часу — це приклад атаки, що використовує залежні від даних характеристики втілення алгоритму швидше ніж його математичні властивості.
   3. Заходи для захисту:
      1. Перевірка всіх символів до того, як повернемо дані
      2. Перевіряти данні на довжину
3. Поясніть принцип роботи алгоритму шифрування AES (Advanced Encryption Standard). Які його основні характеристики та переваги?
4. Що таке протоколи обміну ключами Діффі-Хеллмана? Поясніть їх принцип роботи та важливість у криптографії.
   1. Протокол Діффі-Геллмана (англ. Diffie–Hellman key exchange — це метод обміну криптографічними ключами. Один з перших практичних прикладів узгодження ключа, що дозволяє двом учасникам, що не мають жодних попередніх даних один про одного, отримати спільний секретний ключ із використанням незахищеного каналу зв'язку. Цей ключ можна використати для шифрування наступних сеансів зв'язку, що використовують шифр з симетричним ключем.

Принцип роботи:  
Аліса і Боб таємно обирають два випадкових цілих числа *sA* та *sB*, в інтервалі [*0,* |*G*| − *1*]. Потім вони таємно обчислють числа *aA* = *gsA* та *aB* = *gsB* відповідно, та обмінюються ними через незахищений канал передачі даних. Нарешті, Аліса та Боб обчислюють *aBA* = *aBsA* = *gsBsA* та *aAB* = *aAsB* = *gsAsB* відповідно. Слід зазначити, що *aAB* = *aBA*, і тому це число може служити спільним таємним ключем *K* Аліси та Боба.

Точніше, тепер Аліса та Боб можуть скористатись відображенням елементів множини *G* у простір іншої криптосистеми. Наприклад, вони можуть використати блок даних необхідного розміру (зокрема, молодші біти) значення *aAB* як ключ звичайної блочної криптосистеми.

Приклад: Візьмемо N = 2147483 659 і G = 2. Тоді маємо:

|  |  |
| --- | --- |
| А | В |
| X = 12 | Y = 34 |
| L=212(mod 2 147 483 659)= 4096 | M=234(mod 2 147 483 659)= 2147483571 |
| Kx = 214748357112(mod 2 147 483 659)= 1082609919 | Ky = 409634 (mod 2 147 483 659)= 1082609919 |

1. Якими є основні етапи процесу цифрового підписування повідомлень? Поясніть, як досягається цілісність і автентичність даних, що підписуються.
2. Що таке криптоаналіз? Які методи криптоаналізу можуть бути використані для злому криптографічних систем?
   1. Криптоаналіз — розділ криптології, що займається математичними методами порушення конфіденційності і цілісності інформації без знання ключа.
   2. Основні методи криптоаналізу:
      1. Атака на основі шифротексту — один з основних способів криптоатак. Передбачається що криптоаналітику відомий тільки набір Шифртекстів, метою є отримання якомога більшої кількості відкритих текстів, відповідних наявним Шифртекстам, або ще краще — ключа, використаного при шифруванні.
      2. Атака на основі відкритих текстів і відповідних шифротекстів
      3. Атака на основі підібраного відкритого тексту (можливість вибрати текст для шифрування)
      4. Атака на основі адаптивно підібраного відкритого тексту
   3. Додаткові методи криптоаналізу:
      1. Атака на основі підібраного шифротексту
      2. Атака на основі підібраного ключа
      3. Бандитський криптоаналіз — метод криптоаналізу, при якому «криптоаналітик» вдається до шантажу, погроз, тортур, здирництва, хабарництва і т. д.
3. Які основні засади протоколів обміну ключами на основі дискретного логарифму? Протокол Діффі-Хеллмана та протокол ElGamal.
4. Поясніть загальну схему симетричного шифрування. Що спільного мають усі методи шифрування із закритим ключем?
5. Дайте визначення шифрів підстановки. Сформулюйте загальні принципи методів шифрування підстановкою.
6. Поясніть сутність шифрів моноалфавітної (одноалфавітної) підстановки.
7. Поясніть суть шифрів багатоалфавітної підстановки.
8. Поясніть сутність адитивного шифру підстановки.
9. Поясніть суть мультиплікативного шифру підстановки.
10. Поясніть сутність афінного шифру підстановки.
11. Поясніть суть шифру Плейфера.
12. Поясніть сутність шифру встановлення Виженера.
13. До якої групи методів шифрування із закритим ключем належить метод із використанням таблиці Віженера? Які алгоритми зашифрування та розшифрування у цьому методі?
14. Поясніть суть шифру Хілла.
15. Поясніть сутність шифрування методом гамування.
16. Поясніть сутність шифрування шляхом розв'язання задачі про укладення рюкзака.
17. Дайте визначення шифру перестановки.
18. Поясніть сутність шифрів перестановки без використання та за допомогою ключа.
19. Поясніть, чому сучасні блокові шифри спроектовані як шифри підстановки замість застосування шифрів транспозиції.
20. Перелічіть компоненти сучасного блокового шифру.
21. Визначте сутність Р-блоків та S-блоків.
22. Поясніть різницю між розсіянням і перемішуванням в блокових алгоритмах.
23. Поясніть різницю між блоковим шифром Фейстеля та не-Фейстеля.
24. Алгоритм DES. Особливості його реалізації.
25. Опишіть відмінності між алгоритмами RSA та DES.
26. Описати алгоритм електронного підпису RSA
27. Назвіть властивості хеш функції
28. Назвіть переваги та недоліки ЕЦП RSA
29. Чим потоковий шифр відрізняється від блокового шифру?
30. Як організується шифрування потоку даних змінної довжини?
31. З якою криптографічною метою можна використовувати генератори справжніх випадкових чисел?
32. Поясніть особливості потокових шифрів.
33. Дайте класифікацію потокових шифрів.
34. Поясніть переваги та недоліки синхронних потокових шифрів.
35. Дайте визначення електронного підпису.
36. Основні функції електронного цифрового підпису.
37. Спільні та відмінні ознаки власноручного та електронного підпису.