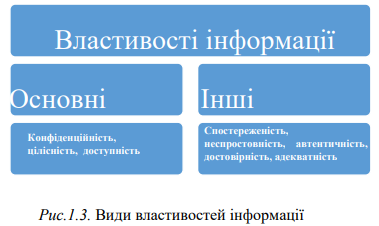
**ТЕОРЕТИЧНІ ПИТАННЯ З КРИПТОГРАФІЇ**

1. **Що таке криптографія та які її основні цілі?**   
   **Криптографія** — 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?**

Захист інформації полягає не лише в захисті засобів обробки інформації, а в організації засобів захисту для підтримки певних властивостей інформації. Виявилося, що такими **основними (фундаментальнимиі) властивостями** є конфіденційність, цілісність та доступність (Рис.1.3), адже захист інформації в більшості випадків пов'язаний з комплексним рішенням трьох завдань:

* забезпеченням конфіденційності інформації.
* забезпеченням цілісності інформації;
* забезпеченням доступності інформації.



Визначення понять конфіденційність, цілісність та доступність дається в Положенні про технічний захист інформації в Україні:

•**«конфіденційність»** - властивість інформації бути захищеною від несанкціонованого ознайомлення»;

• **«цілісність»** - властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення»;

• **«доступність»** - властивість інформації бути захищеною від несанкціонованого блокування».

Порушення кожної з трьох складових призводить до порушення інформаційної безпеки в цілому. Так, порушення доступності призводить до відмови в доступі до інформації, порушення цілісності призводить до фальсифікації інформації і, нарешті, порушення конфіденційності призводить до розкриття інформації.

На додаток до перерахованих вище основних характеристик безпеки можуть розглядатися також і інші характеристики безпеки. Зокрема, до таких характеристик відносяться:

• **Спостережність (accountability)** –- забезпечення ідентифікації суб'єкта доступу та реєстрації його дій.

• **Неспростовність (non-repudiation)** - неможливість відмови від авторства.

• **Автентичність (authenticity)** - гарантує, що суб'єкт або ресурс ідентичні заявленим.

• **Достовірність (reliability)** - властивість відповідності передбаченому поводженню чи результату.

• **Адекватність** – відповідність створюваного з допомогою отриманої інформації образу реальному об'єкту, процесу, явища тощо.

1. **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.
2. **Яку архітектуру має криптографічна система?**
3. **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.
4. **Коли у криптографії почали використовуватися наукові підходи?**

Перші системи шифрування з’явились одночасно з письменністю у V-IV тт. до н.е. Відомо, що вже в той час в Спарті використовувався один з перших шифрувальних пристроїв – Сцитала. Це був жезл циліндричної форми, на який намотувалась стрічка пергаменту. Вздовж осі циліндру записувався текст, призначений для передачі. Після запису стрічка знімалась з жезлу і передавалась адресату, який мав таку саму Сциталу. Цікаво, що був відомий і метод дешифрації такого шифру, винайдення якого приписується Арістотелю. Пропонувалось заточити на конус довгий брус і, обернувши його стрічкою, починати зсувати її по конусу від малого діаметру до найбільшого. Там, де діаметр конусу співпадав з діаметром Сцитали, букви текту утворювали слова. Далі залишалось тільки виготовити циліндр потрібного діаметру.

З часів Цезаря до XIV-XV століть криптографія розвивалась, але практика шифрування зберігалась у глибокій таємниці. Так, в часи хрестових походів шифрувальники Папи Римського після року роботи підлягали фізичному знищенню. Тому про цей період майже нічого невідомо. В епоху Відродження почали розвиватись наукові методи криптографії і крипто аналізу. Зокрема для дешифрування шифрів став використовуватись метод частотного аналізу зустрічаємості букв, для шифрування почали використовуватись шифри багатозначної заміни (омофони), отримали поширення багатоалфавітні шифри (шифр Тритемія, шифр Віженера), в якості засобу шифрування почала використовуватись поворотна решітка. Поворотна решітка представляла собою лист з твердого матеріалу з прорізами. Накладаючи таку решітку на лист паперу, можна записувати у вирізи таємне повідомлення. Після цього, знявши решітку, треба було заповнити вільні місця, що залишились, маскуючим текстом. Подібним стеганографічним методом маскування повідомлень користувались багато історичних осіб, зокрема, кардинал Рішіл’є у Франції.

В історії криптографії XVII-XVIII ст. називають ерою «чорних кабінетів». В цей період в багатьох державах Європи з’явились дешифрувальні підрозділи, які і називались «чорними кабінетами». Перший з них був створений у Франції за ініціативою кардинала Рішіл’є.

В простих нуменклаторах код складався з кількох десятків слів або фраз з двобуквеними кодовими позначеннями. З часом списки слів в номерклаторах збільшились до двох-трьох тисяч. В цілому XVII-XVIII ст. не дали для криптографії нових ідей. Ера «чорних кабінетів» закінчилась в 40их роках XIX ст. Нові ідеї з’явились в середині XIX ст. Цей період пов’язаний з виникненням стійкого способу ускладнення числових кодів – гаміювання. Він полягав у перешифровуванні закодованого повідомлення за допомогою деякого ключового числа, яке називалось гамою. Шифрування за допомогою гами полягало у сумуванні всіх кодованих груп повідомлення з одним і тим самим ключовим числом.

Перша світова війна стала поворотним пунктом в розвитку криптографії в зв’язку зі зростанням обсягів шифропереписки. Криптографія стала широким полем діяльності. Проте нових наукових ідей в цей час не з’явилося. Майже половина XX ст. була пов’язана з використанням колісних шифраторів. Їх різні конструкції були запатентовані майже одночасно в різних країнах (Голандії, Німеччині, Швеції). Найбільш відомою шифромашиною цих часів була «Енігма», яка у довоєнний період і під час другої світової війни використовувалась в германській армії. Принцип її роботи такий. На екрані оператору показувалася буква, якою шифрувалася відповідна літера на клавіатурі. Те, якою буде зашифрована літера, залежало від початкової конфігурації коліс. Суть в тому, що існувало понад сто трильйонів можливих комбінацій коліс, і з часом набору тексту колеса зсувалися самі, так що шифр змінювався протягом усього повідомлення. Все Енігми були ідентичними, так що при однаковому початковому положенні коліс на двох різних машинах і текст виходив однаковий. У німецького командування були Енігми і список положень коліс на кожен день, так що вони могли з легкістю розшифровувати повідомлення один одного, але вороги не повідомляючи положень послання прочитати не могли. У другій половині XX ст. в зв’язку з розвитком елементної бази обчислювальної техніки з’явились електронні шифратори. Сьогодні для шифрування даних найбільш широко застосовують три види шифраторів: апаратні, програмно-апаратні та програмні. Їх основна відмінність полягає не тільки в способі реалізації шифрування і ступеня надійності захисту даних, але і в ціні. Найдешевші пристрої шифрування - програмні, потім йдуть програмно-апаратні засоби і, нарешті, найдорожчі - апаратні. В 70-их роках народилась «нова криптографія» - криптографія з відкритим ключем. Криптографія почала широко використовуватись не тільки у військовій, дипломатичній, державній сферах, а також в комерційній, банківській та інших сферах.

1. **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 )
2. **Які шифри називаються історичними?**

**Історичними (докомпютерними)** називають шифри, що використовувались до 1960 року, тобто в до комп'ютерну епоху. Ці шифри є типовими прикладами симетричних алгоритмів шифрування і залишаються основою багатьох сучасних криптосистем. В класичній криптографії доведено, що в основі криптографічних алгоритмів знаходяться тільки два основних типи перетворень – заміни і перестановки; всі інші є лише їх комбінацією. В перестановочних шрифтах символи відкритого тексту змінюють свої розташування. Наприклад, відкритий текст виписується у вигляді матриці з пронумерованими стовпцями, після чого порядок стовпців змінюється.

1. **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
2. **Що таке криптографічний ключ? Які вимоги до криптографічних ключів?**

**Криптографічний ключ** - це важливий параметр у криптографічних алгоритмах, який використовується для шифрування та розшифрування даних. Ключ визначає спосіб перетворення даних, що забезпечує конфіденційність та безпеку інформації.

Вимог до криптографічних ключів:

* Довжина: Довжина ключа визначає кількість бітів або символів, що використовуються в ключі. Довші ключі зазвичай забезпечують більш надійне шифрування та стійкість до атак грубої сили. Довжина ключа повинна бути достатньою, щоб запобігти швидкому розкриттю ключа за допомогою сучасних обчислювальних ресурсів.
* Випадковість: Криптографічні ключі повинні генеруватися з достатнім рівнем випадковості. Вони повинні бути непередбачуваними і незалежними від будь-яких інших даних. Випадковість важлива, оскільки передбачувані або слабкі ключі можуть стати легкою мішенню для атак.
* Секретність: Ключ повинен зберігатися в таємниці і бути доступним лише авторизованим користувачам або системам. Якщо ключ потрапить до рук зловмисників, це може поставити під загрозу безпеку інформації. Таємність ключа необхідна для збереження конфіденційності та цілісності зашифрованих даних.
* Унікальність: Кожен криптографічний ключ повинен бути унікальним і не використовуватися повторно в різних програмах або протоколах шифрування. Використання одного і того ж ключа для різних цілей або протоколів може призвести до вразливостей і компрометації.
* Розподіл ключів: Безпечний розподіл ключів має вирішальне значення для забезпечення їх конфіденційності. Процес безпечного обміну або розповсюдження ключів серед уповноважених сторін повинен бути ретельно розроблений і впроваджений.
* Управління ключами: Належні практики управління ключами необхідні для генерації, зберігання, резервного копіювання, ротації та відкликання криптографічних ключів. Ефективне управління ключами забезпечує довгострокову безпеку та зручність використання криптографічних систем.
* Сумісність алгоритмів: Криптографічний ключ повинен бути сумісним з алгоритмом, що використовується. Різні алгоритми шифрування можуть мати специфічні вимоги до форматів, розмірів або властивостей ключів.

1. **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?**

**Хеш-функція** - це функція, яка приймає на вхід будь-який вхідний повідомлення будь-якої довжини і обчислює фіксований вихідний результат фіксованої довжини, який називається хешем або хеш-значенням. Головна особливість хеш-функції полягає в тому, що навіть невеликі зміни в початкових даних спричиняють значні зміни в хеш-значенні.

Геш-функція має чотири основні властивості:

* легкість обчислення геш-значення для будь-якого повідомлення
* нездійсненно утворити повідомлення для заданого геш-значення
* нездійсненно змінити повідомлення без зміни геша (лавиновий ефект)
* нездійсненно знайти два різних повідомлення з тим самим гешем

1. **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
2. **Які основні принципи протоколів автентифікації та ключового обміну?**
3. **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?**

Коротше кажучи, AES — це симетричний тип шифрування, оскільки він використовує той самий ключ як для шифрування, так і для дешифрування даних.

Є три довжини ключів шифрування AES. Кожна довжина ключа має різну кількість можливих комбінацій клавіш:

Довжина 128-бітного ключа: 3,4 x 10^38

192-бітна довжина ключа: 6,2 x 10^57

256-бітна довжина ключа: 1,1 x 10^77

Незважаючи на те, що довжина ключа цього методу шифрування змінюється, розмір його блоку – 128 біт (або 16 байт) – залишається незмінним.

Переваги AES

* Крім безпеки, шифрування AES дуже привабливе для тих, хто з ним працює. Оскільки процес шифрування AES відносно простий для розуміння. Це забезпечує просте впровадження , а також дуже швидке шифрування та дешифрування .
* Крім того, AES вимагає менше пам’яті, ніж багато інших типів шифрування (наприклад, DES), що робить його справжнім переможцем, коли справа доходить до вибору бажаного методу шифрування.
* Нарешті, коли для дії потрібен додатковий рівень безпеки, ви можете поєднати AES з різними протоколами безпеки, як-от WPA2, або навіть іншими типами шифрування, як-от SSL.

Як працює шифрування AES?

1. Розбиття даних на блоки

По-перше, ми повинні мати на увазі, що AES є блоковим шифром . На відміну від потокових шифрів, він шифрує дані блоками бітів , а не побітово.

Кожен його блок містить стовпець із 16 байтів у форматі чотири на чотири. Оскільки один байт містить 8 біт, ми отримуємо 128-бітний розмір блоку (16x8=128).

Таким чином, найпершим кроком шифрування AES є поділ відкритого тексту (тексту, який не записаний у коді) на ці блоки.

2. Ключове розширення

Це важливий етап шифрування AES. Він створює нові 128-бітні круглі ключі за допомогою розкладу ключів Rijndael .

3. Додавання круглого ключа

Це найперший раунд шифрування AES. Тут алгоритм додає початковий ключ до нашої фрази, яку раніше перетворили на блок 4x4

4. Заміна байтів

Тепер алгоритм AES замінює кожен байт кодом відповідно до попередньо встановленої таблиці під назвою Rijndael S-box .

5. Зміщення рядів

На цьому кроці алгоритм AES зсуває рядки блоку, отриманого під час процесу заміни байтів.

6. Змішувальні колони

Говорячи математичними термінами, цей крок множить кожен стовпець на заздалегідь визначену матрицю, даючи нам абсолютно новий блок коду.

7. Додавання круглого ключа

Настав час застосувати круглий ключ, який ми отримали в розділі розширення ключів . Додамо його до блоку, який ми отримали в попередньому розділі після процесу змішування колонок

8. Промийте та повторіть

Тепер алгоритм шифрування AES проходитиме ще багато раундів заміни байтів, зміщення рядків, змішування стовпців і додавання круглого ключа.

Кількість ідентичних раундів, через які проходять дані, залежить від довжини ключа AES:

128-бітний ключ: 9 раундів

192-бітний ключ: 11 раундів

256-бітний ключ: 13 раундів

Після згаданих 9, 11 або 13 раундів шифрування є один додатковий раунд. Під час цього додаткового раунду алгоритм проходить лише етапи заміни байтів, зміщення рядків і додавання ключа раунду. Він виключає етап змішування колон.

чому Тому що на даний момент це було б зайвим. Іншими словами, ця дія задіяла б занадто багато процесорної потужності без істотної зміни даних.

Отже, наприкінці процесу шифрування дані пройдуть таку кількість циклів:

128-бітний ключ: 10 раундів

192-бітний ключ: 12 раундів

256-бітний ключ: 14 раундів

1. **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?** 
   1. Шифрування симетричними ключами іноді називають шифруванням c секретним ключем або криптографією з секретним ключем. Наприклад, об'єкт, назвемо його Аліса, може передати повідомлення іншому об'єкту, який називається Боб, по небезпечному каналу, для того, щоб її противник, який називається Єва, не зміг зрозуміти зміст повідомлення, просто підслухавши його по каналу. Аліса зашифрувала повідомлення, використовуючи алгоритм шифрування; Боб розшифровує повідомлення, використовуючи алгоритм розшифровки. У шифруванні симетричними ключами застосовується єдиний ключ засекречування і для шифрування, і для розшифровки
   2. Спільне всіх алгоритмів шифрування з закритим ключем:  
      для дешифрування використовується закритий ключ
5. **Дайте визначення шифрів підстановки. Сформулюйте загальні принципи методів шифрування підстановкою.** 
   1. **Підстановочний шифр** — алгоритм шифрування, який полягає у заміні знаків відкритого тексту іншими знаками за допомогою ключа.
   2. Одноалфавітний шифр підстановки (шифр простої заміни) — шифр, у якому кожен символ відкритого тексту замінюється деякий, фіксований за даному ключі символ тієї самої алфавіту.
   3. Однозвучний шифр підстановки схожий на одноалфавітний крім того, що символ відкритого тексту може бути замінений одним з декількох можливих символів.
   4. Поліграмний шифр підстановки замінює не один символ, а цілу групу. Приклад: Шифр Плейфера.
   5. Поліалфавітний шифр підстановки складається з кількох шифрів простої заміни. Приклади: шифр Віженера, Бофора шифр, одноразовий блокнот.
6. **Поясніть сутність шифрів моноалфавітної (одноалфавітної) підстановки.** 
   1. Одним із важливих підкласів методів заміни є одноалфавітні (або моноалфавітні) підстановки, в яких встановлюється однозначна відповідність між кожним знаком ai вихідного алфавіту повідомлень A та відповідним знаком ei зашифрованого тексту E. Одноалфавітна підстановка іноді називається також простою заміною, оскільки є найпростішим шифром заміни. Приклад одноалфавітної заміни є шифр Цезаря.
7. **Поясніть суть шифрів багатоалфавітної підстановки.**

Багатоалфавітна підстановка послідовно й циклічно змінює використовувані алфавіти.

При *r-алфавітній* підстановці символ *https://studfile.net/html/2706/317/html_zBiLQtzGoT.IDgF/img-SqeWMB.png*вихідного повідомлення замінюється символом https://studfile.net/html/2706/317/html_zBiLQtzGoT.IDgF/img-HGqzkP.pngз алфавітуhttps://studfile.net/html/2706/317/html_zBiLQtzGoT.IDgF/img-F_l98c.png, символhttps://studfile.net/html/2706/317/html_zBiLQtzGoT.IDgF/img-i5LkVp.png– символом https://studfile.net/html/2706/317/html_zBiLQtzGoT.IDgF/img-wpFakx.pngз алфавітуhttps://studfile.net/html/2706/317/html_zBiLQtzGoT.IDgF/img-SeVOqW.pngі т. д., символhttps://studfile.net/html/2706/317/html_zBiLQtzGoT.IDgF/img-LxUg7g.pngзаміняється символомhttps://studfile.net/html/2706/317/html_zBiLQtzGoT.IDgF/img-rwQxcu.pngз алфавітуhttps://studfile.net/html/2706/317/html_zBiLQtzGoT.IDgF/img-Bavt9m.png.

1. **Поясніть сутність адитивного шифру підстановки.**

Якщо в афінному шифрі https://studfile.net/html/2706/360/html_Ro8UuWjNYf.J3tY/img-t6xbl9.png, то існує адитивний однозначно зворотній шифр з правилом шифрування:

https://studfile.net/html/2706/360/html_Ro8UuWjNYf.J3tY/img-ZMv0Qn.png, (2.86)

https://studfile.net/html/2706/360/html_Ro8UuWjNYf.J3tY/img-lTOQ1n.png. (2.85)

доведення здійснюється з урахуванням афінного шифру

https://studfile.net/html/2706/360/html_Ro8UuWjNYf.J3tY/img-IE3QqS.png.

Симетрія шифру міститься в тому, що ключі поліноміально легко зв’язані і один може бути легко визначений при знанні іншого.

1. **Поясніть суть мультиплікативного шифру підстановки.**
2. **Поясніть сутність афінного шифру підстановки.** 
   1. Афінний шифр - це окремий випадок більш загального моноалфавітного шифру підстановки.
   2. В афінному шифрі кожній літері алфавіту розміру m ставиться у відповідність число з діапазону 0.. m-1. Потім за допомогою модульної арифметики для кожного числа, що відповідає літері вихідного алфавіту, обчислюється нове число, яке замінить старе у шифротексті. Функція шифрування для кожної літери:  
      E(x) = (ax + b) mod m  
      де модуль m - розмір алфавіту, а пара a і b - ключ шифру. Значення a має бути обрано таким, що a і m - взаємно прості числа.   
      Функція розшифрування:  
      D(x) = a-1(x - b) mod m  
      де a-1 – зворотне до a число по модулю m, Тобто 1 = aa-1 mod m
3. **Поясніть суть шифру Плейфера.** 
   1. Шифр Плейфера або квадрат Плейфера — ручна симетрична техніка шифрування, в якій вперше використано заміну біграм. Шифр у 1854 році винайшов англійський фізик Чарльз Вітстон, але він отримав ім'я лорда Лайона Плейфера, який просував використання цієї системи у державній службі. Цей метод передбачає шифрування пар символів (біграм) замість одиночних символів, як у шифрі підстановки й у більш складних системах шифрування Віженера. Через це шифр Плейфера стійкіший до злому методом частотного аналізу. Знаходження закономірності розподілу 26 х 26 = 676 можливих біграм потребує суттєво більших зусиль і обсягу зашифрованого тексту, ніж для 26 монограм (літер латинського алфавіту).
4. **Поясніть сутність шифру встановлення Виженера.**

**Шифр Віженера** — [поліалфавітний шифр](https://uk.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D1%96%D0%B0%D0%BB%D1%84%D0%B0%D0%B2%D1%96%D1%82%D0%BD%D0%B8%D0%B9_%D1%88%D0%B8%D1%84%D1%80" \o "Поліалфавітний шифр), який як [ключ](https://uk.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87) використовує слово.

Якщо пронумерувати літери алфавіту від 0 до 32 (а → 0, б → 1, в → 2, …), то шифрування Віженера можна подати формулою:

Ci = (Pi + Kj) mod 33,

де Kj — j-та літера [ключового](https://uk.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87) слова, Pi  — і-а літера вихідного слова.

Ключове слово повторюється, поки не отримано [гаму](https://uk.wikipedia.org/w/index.php?title=%D0%93%D0%B0%D0%BC%D0%B0(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F)&action=edit&redlink=1), рівну довжині повідомлення.

Дешифрування відбувається за наступною формулою:

Ci = (Pi + 33 - Kj) mod 33

1. **До якої групи методів шифрування із закритим ключем належить метод із використанням таблиці Віженера? Які алгоритми зашифрування та розшифрування у цьому методі?** 
   1. Шифр Віженера — поліалфавітний шифр, який як ключ використовує слово.
   2. Використовується перестановка та в разі ключ дорівнює тексту, тоді XOR
2. **Поясніть суть шифру Хілла.** 
   1. Алгебричний метод, який узагальнює афінну систему підставляння Цезаря, формалізований опис якого має такий вигляд:   
        
      був сформульований Лестером С. Хіллом для визначення n-грам. Множина цілих чисел , для якої визначені операції додавання, віднімання та множення за модулем m, є прикладом кільця R, тобто алгебричною системою пар елементів. Ця алгебрична система володіє такими властивостями:
      1. пари елементів кільця R утворюють комутативну групу щодо операції додавання; для неї існують одиничний і зворотний елементи;
      2. операції множення та додавання задовольняють асоціативному і дистрибутивному законам.
3. **Поясніть сутність шифрування методом гамування.** 
   1. Принцип шифрування гамуванням полягає в генерації гами шифру за допомогою датчика псевдовипадкових чисел і накладенні отриманої гами на відкриті дані оборотним чином. Процес дешифрування даних зводиться до повторної генерації гами шифру при відомому ключі і накладенні такої гами на' зашифровані дані. Метод гамування стає ненадійним, якщо зловмиснику стає відомий фрагмент вихідного тексту і відповідна йому шифрограма.
4. **Поясніть сутність шифрування шляхом розв'язання задачі про укладення рюкзака.** 
   1. **Задача пакування рюкзака** — задача комбінаторної оптимізації: для заданої множини предметів, кожен з яких має вагу і цінність, визначити яку кількість кожного з предметів слід взяти, так, щоб сумарна вага не перевищувала задану, а сумарна цінність була максимальною. Задача бере свою назву від доволі відомої ситуації, коли потрібно наповнити рюкзак, що здатен витримати деяку максимальну масу, предметами, кожен з яких має вартість (або корисність) та масу. Необхідно обрати об'єкти в такий спосіб, аби максимізувати сумарну вартість (або користь), але не перевищити максимально припустиму масу.
5. **Дайте визначення шифру перестановки.** 
   1. Перестановочний шифр — алгоритм шифрування, який полягає у перестановці знаків відкритого тексту згідно з певним правилом, яке є ключем.
6. **Поясніть сутність шифрів перестановки без використання та за допомогою ключа.** 
   1. Шифр перестановки — це метод симетричного шифрування, в якому елементи вихідного тексту змінюють місцями. Елементами тексту можуть бути окремі символи (найпоширеніший випадок), пари букв, трійки букв, комбінування цих випадків тощо. Типовими прикладами перестановки є анаграми.
   2. Без ключа - При шифруванні символи відкритого тексту переміщаються з вихідних позицій в один раз.
   3. З ключем - При шифруванні символи відкритого тексту переміщаються з вихідних позицій у кілька разів.
7. **Поясніть, чому сучасні блокові шифри спроектовані як шифри підстановки замість застосування шифрів транспозиції.** 
   1. Бо якщо використовувати шифр транспозиції, тоді для шифрування та дешифрування використовується один й той самий алгоритм, а якщо використовувати шифр підстановки, тоді в процесі шифрування створюється ключ для дешифрування
8. **Перелічіть компоненти сучасного блокового шифру.** 
   1. довжина блоку
   2. кількість раундів
   3. розмір ключа
   4. розмір кожного з підключів
9. **Визначте сутність Р-блоків та S-блоків.** 
   1. S-блок заміщає невеликий блок вхідних біт на інший блок вихідних біт. Ця заміна повинна бути взаємно однозначною, щоб гарантувати оборотність. Призначення S-блоку полягає в нелінійному перетворенні, що перешкоджає проведенню лінійного криптоаналізу.
   2. P-блок (англ. Permutation box or P-box) - отримує на вхід виводи S-блоків, змінює місцями все біти і подає результат S-блокам наступного раунду. Важливою якістю P-блоку є можливість розподілити виводи одного S-блоку між входами якомога більшої кількості S-блоків
10. **Поясніть різницю між розсіянням і перемішуванням в блокових алгоритмах.** 
    1. Розсіювання являє собою поширення впливу одного знака відкритого тексту на багато знаків шифр-текста, що дозволяє приховати статистичні властивості відкритого тексту.
    2. Перемішування полягає в використанні таких перетворень шифрування, які ускладнюють відновлення взаємозв'язку статистичних властивостей відкритого і шифрованого текстів.
11. **Поясніть різницю між блоковим шифром Фейстеля та не-Фейстеля.**
12. **Алгоритм DES. Особливості його реалізації.** 
    1. DES (англ. Data Encryption Standard) — це симетричний алгоритм шифрування певних даних, стандарт шифрування прийнятий урядом США із 1976 до кінця 1990-х, з часом набув міжнародного застосування.
    2. DES – алгоритм блокового шифрування з довжиною блоку 64 біти і симетричним ключем довжиною 56 біт. На практиці ключ має довжину 64 біти,з яких кожний восьмий використовується для контролю парності байту. Головні риси шифру DES визначаються тим, що він ґрунтується на схемі Фейстеля з такими параметрами:
       1. довжина блоку – 64 біти,
       2. кількість раундів – 16,
       3. розмір ключа – 56 бітів,
       4. розмір кожного з підключів k1, k2, …, k16 – 48 бітів.
13. **Опишіть відмінності між алгоритмами RSA та DES.**

Переваги DES:

* - використовується тільки один ключ довжиною 64 (56 біт довжина ключа та 8 контрольних розрядів) біт;
* зашифрувавши повідомлення за допомогою одного пакета програм, для розшифрування можна використовувати будь-який інший пакет програм, що відповідає стандарту DES;
* відносна простота алгоритму забезпечує високу швидкість обробки;
* досить висока стійкість алгоритму.

Переваги RSA:

* Алгоритм RSA може бути реалізований відносно швидко.
* Роздавати відкриті ключі користувачам просто.
* Враховуючи складну математику, зламати алгоритм RSA надзвичайно складно.
* Алгоритм RSA безпечний і надійний для надсилання приватної інформації.
* Для механізмів RSA є надійним і безпечним. Тому над

1. **Описати алгоритм електронного підпису RSA** 
   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. **Назвіть властивості хеш функції**

* легкість обчислення геш-значення для будь-якого повідомлення
* нездійсненно утворити повідомлення для заданого геш-значення
* нездійсненно змінити повідомлення без зміни геша (лавиновий ефект)
* нездійсненно знайти два різних повідомлення з тим самим гешем

1. **Назвіть переваги та недоліки ЕЦП RSA** 
   1. Переваги
      1. забезпечення високої криптостійкості при певній довжині ключа
      2. простота алгоритму
   2. Недоліки
      1. складність обчислення ЕЦП
      2. необхідні великі обчислювальні ресурси
      3. повільність підписання документу
2. **Чим потоковий шифр відрізняється від блокового шифру?**

|  |  |  |
| --- | --- | --- |
| **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. **Як організується шифрування потоку даних змінної довжини?** 
   1. потоковий шифр (stream cipher), який виконує перетворення вхідного повідомлення за одним бітом (або байтом) за операцію. Потоковий алгоритм шифрування усуває необхідність розбивати повідомлення на ціле число блоків досить великої довжини, отже, може працювати у часі. Таким чином, якщо передається потік символів, кожен символ може шифруватись і передаватися відразу.
   2. Потоковий шифр — це симетричний шифр, у якому кожен символ відкритого тексту перетворюється на символ шифрованого тексту залежно як від використання ключа, а й його розташування у потоці відкритого тексту.
2. **З якою криптографічною метою можна використовувати генератори справжніх випадкових чисел?** 
   1. Створення ключів
   2. Генерування сидів
3. **Поясніть особливості потокових шифрів.** 
   1. Висока швидкість шифрування у порівнянні з блочними
   2. Синхронні поточні шифри не мають ефекту розмноження помилок на відміну від блочних
   3. структура потокового ключа може мати вразливі місця
   4. можуть бути атаковані завдяки лінійної алгебри
4. **Дайте класифікацію потокових шифрів.** 
   1. Синхронні потокові шифри(СПШ) – це шифри, в яких потік ключів генерується незалежно від відкритого та зашифрованого повідомлення.  
      Переваги:
      1. відсутність ефекту поширення помилок (тільки перекручений біт буде розшифровано неправильно);
      2. оберігає від будь-яких вставок та видалень зашифрованого повідомлення, оскільки вони призведуть до втрати синхронізації та будуть виявлені
   2. Самосинхронізуються потокові шифри(асинхронні потокові шифри (АПШ)) - це шифри, у яких потік ключів створюється функцією ключа та фіксованого числа знаків зашифрованого повідомлення.  
      Переваги:
      1. Основними перевагами АПШє розмішування статистики відкритого повідомлення
   3. Недоліки:
      1. поширення помилки (кожному неправильному біту зашифрованого повідомлення відповідають n помилок у відкритому повідомленні);
      2. чутливі до розтину повторною передачею.
5. **Поясніть переваги та недоліки синхронних потокових шифрів.** 
   1. Переваги
      1. відсутність ефекту поширення помилок (тільки спотворений біт буде розшифрований невірно);
      2. оберігають від будь-яких вставок і вилучень шифротекста, так як вони приведуть до втрати синхронізації і будуть виявлені.
   2. Недоліки
      1. уразливі до зміни окремих біт зашифрованого тексту. Якщо зловмисникові відомий відкритий текст, він може змінити ці біти так, щоб вони розшифровували, як йому треба.
6. **Дайте визначення електронного підпису.** 
   1. Електронний підпис — це електронні дані, які забезпечують цілісність документів та ідентифікують особу. Електронний підпис може зберігатися у вигляді MobileID, підпису на ID-картці, підпису на “токені” чи захищеному носії інформації. За допомогою електронного підпису можна підписувати електронні документи, користуватися електронними послугами, реєструватися на державних порталах тощо. Документи з цим підписом мають таку саму юридичну силу, як і документи, підписані власноруч.
7. **Основні функції електронного цифрового підпису.** 
   1. можна підписувати електронні документи, користуватися електронними послугами, реєструватися на державних порталах тощо
   2. підтверджує достовірність і цілісність документа
   3. фіксації точного часу підписання документа
8. **Спільні та відмінні ознаки власноручного та електронного підпису.** 
   1. ЕЦП (електронний цифровий підпис) — це електронні дані, які користувач використовує в якості власного підпису, додаючи їх до інших цифрових даних або логічно пов’язуючи їх між собою.
   2. Мають однакову юридичну силу
   3. Електронний підпис важче підробити