ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

ЗБІРНИК НАУКОВИХ ПРАЦЬ

XI Всеукраїнської науково-практичної конференції курсантів та студентів

МАТЕМАТИКА, ЩО НАС ОТОЧУЄ: МИНУЛЕ, СУЧАСНЕ, МАЙБУТНЄ

Львів 2024

ОРГАНІЗАТОР ТА ВИДАВЕЦЬ Львівський державний університет безпеки життєдіяльності

АДРЕСА РЕДАКЦІЇ: ЛДУ БЖД, вул. Клепарівська, 35 м. Львів, 79007

контактні телефони: (032)233-24-79 тел/факс 2330088

Математика, що нас оточує: минуле, сучасне, майбутнє: Зб. наук.праць XI Всеукраїнської конф. курсантів та студентів. – Львів: ЛДУ БЖД, 2024 -172с.

Збірник сформовано за матеріалами XI Всеукраїнської конференції курсантів та студентів **«Математика, що нас оточує: минуле, сучасне, майбутнє».**

Збірник містить матеріали таких тематичних секцій:

- Математичні відкриття, що змінили світ
- Прикладні задачі в математиці
- Історія математики
- Математика і сучасність
- Постаті в математиці

Здано в набір 20.05.2024. Підписано до друку 25.05.2024. Формат 60x841/3. Папір офсетний. Ум. друк. арк. 7. Гарнітура Times New Roman. Друк на різографі. Наклад: 100 прим. Друк: ЛДУ БЖД вул. Клепарівська, 35, м. Львів, 79007. ldubzh.lviv@mns.gov.ua

В. Чумак
Львівський державний університет безпеки життєдіяльності
Науковий керівник ***О.О. Карабин,*** *кандидат фізико-математичних наук, доцент кафедри прикладної математики і механіки*

МАТЕМАТИЧНІ АСПЕКТИ ШИФРУВАННЯ ДАНИХ

Основні принципи криптографії:

- Симетричне та асиметричне шифрування:
- Принципи ключів та їх генерація.
- Цілісність та конфіденційність даних.

Симетричне шифрування це метод шифрування, де один і той же ключ використовується як для шифрування, так і для розшифрування повідомлень. Він базується на тому, що відправник і отримувач повинні мати доступ до одного і того ж ключа для обміну даними. Популярними алгоритмами симетричного шифрування є DES (Data Encryption Standard), AES (Advanced Encryption Standard) та IDEA (International Data Encryption Algorithm).

Асиметричне шифрування: це метод, де використовуються два ключі: публічний та приватний. Публічний ключ використовується для шифрування повідомлення, а приватний — для його розшифрування. Цей метод дозволяє створювати безпечні засоби комунікації, оскільки публічний ключ може бути розповсюджений відкрито, тоді як приватний ключ лишається секретним. Популярними алгоритмами асиметричного шифрування є RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography) та ElGamal.

Принципи ключів та їх генерація в криптографії включають наступне.
Ключі мають бути достатньо довгими для забезпечення безпеки шифрування. Зазвичай це означає використання ключів з більшою довжиною бітів, що ускладнює їх перебір.

Випадковість: ключі мають бути випадковими, щоб ускладнити їх вгадування. Генерація ключів повинна здійснюватися за допомогою криптографічно стійких генераторів випадкових чисел.

Секретність: приватний ключ у симетричному шифруванні та асиметричному шифруванні повинен залишатися секретним і не доступним для сторонніх осіб.

Генерація ключа: процес створення ключів повинен бути надійним та безпечним. Для цього застосовуються математичні алгоритми, що генерують ключі, і використовуються криптографічні принципи для забезпечення їх випадковості та безпеки.Генерація ключів важлива для забезпечення безпеки криптографічних систем і виконання криптографічних протоколів.

Цілісність даних: цілісність даних означає забезпечення того, що дані не були змінені або пошкоджені під час передачі або зберігання. Для досягнення цілісності, дані можуть бути захищені від несанкціонованої зміни або порушення за допомогою хеш-функцій або цифрових підписів.

Конфіденційність даних: конфіденційність даних полягає в забезпеченні того, що тільки авторизовані користувачі мають доступ до інформації, інші не можуть

переглядати, копіювати або змінювати дані без дозволу. Конфіденційність забезпечується за допомогою різних методів шифрування, таких як симетричне та асиметричне шифрування, які перешкоджають несанкціонованому доступу до даних.

Математичні алгоритми шифрування

- RSA (алгоритм Рівеста, Шаміра та Адлемана).
- AES (Advanced Encryption Standard).
- DES (Data Encryption Standard).

RSA (алгоритм Рівеста, Шаміра та Адлемана)

RSA (Rivest-Shamir-Adleman) - це асиметричний криптографічний алгоритм, який використовується для шифрування та цифрового підпису повідомлень. Основні принципи RSA такі:

Генерація ключів: користувач створює пару ключів - публічний і приватний. Публічний ключ використовується для шифрування даних, а приватний - для розшифрування.

Шифрування: публічний ключ використовується для зашифрування повідомлення. Кожне повідомлення шифрується за допомогою публічного ключа, що перетворює його у незрозумілий для сторонніх текст.

Розшифрування: розшифрування виконується за допомогою приватного ключа. Лише власник приватного ключа може розшифрувати зашифроване повідомлення, перетворюючи його назад у зрозумілий вигляд.

Цифровий підпис: RSA також використовується для створення цифрових підписів, які дозволяють перевірити автентичність повідомлення та впевнитися, що воно не було змінене під час передачі.

RSA є одним з найбільш поширених алгоритмів шифрування та цифрового підпису і використовується у багатьох системах безпеки та криптографії.

Приклад дії алгоритму RSA

Етап	Опис операції	Результат операції
Генерація ключів	Обрати два простих різних числа	$p = 3557,$ $q = 2579$
	Обчислити добуток	$n = p \cdot q = 3557 \cdot 2579 = 9173503$
	Обчислити функцію Ейлера	$\varphi(n) = (p-1)(q-1) = 9167368$
	Обрати відкриту експоненту	$e = 3$
	Обчислити секретну експоненту	$d = e^{-1} \pmod{\varphi(n)}$ $d = 6111579$
	Опублікувати *відкритий ключ*	$\{e, n\} = \{3, 9173503\}$
	Зберегти *секретний ключ*	$\{d, n\} = \{6111579, 9173503\}$
Шифрування	Обрати текст для шифрування	$m = 111111$
	Обчислити шифротекст	$c = E(m)$ $= m^e \mod n$ $= 111111^3 \mod 9173503$ $= 4051753$
Розшифрування	Обчислити вихідне повідомлення	$m = D(c) =$ $= c^d \mod n$ $= 4051753^{6111579} \mod 9173503$ $= 111111$

AES (Advanced Encryption Standard)

AES (Advanced Encryption Standard) - це симетричний блочний шифр, який використовується для шифрування даних. Основні принципи AES такі:

Розмір блоку: AES працює з блоками даних розміром 128 біт (16 байт).

Довжина ключа: AES підтримує ключі різної довжини - 128, 192 або 256 біт.

Підстановочно-перестановочна мережа: AES використовує комбінацію підстановочних та перестановочних шарів, що робить атаку зворотного тексту надзвичайно складною.

Раунди шифрування: алгоритм AES виконується у кілька раундів, в кожному з яких застосовуються операції підстановки, перестановки та комбінації, що залежать від ключа.

Стійкість до атак: AES є стійким до різних видів криптоаналізу, включаючи атаку методом перебору, диференційний та лінійний криптоаналіз.

AES є одним з найбільш поширених симетричних алгоритмів шифрування і використовується у багатьох сучасних криптографічних застосунках, таких як захист даних у системах зберігання та передачах інформації через Інтернет.

Концепція цифрових підписів

- Використання криптографічних хеш-функцій.
- Застосування приватного ключа для підпису та публічного ключа для перевірки підпису.

Розвиток квантових комп'ютерів відкриває нові можливості для зламування криптографічних шифрів, особливо тих, які базуються на складних математичних проблемах, таких як розкладання на множники великих чисел (як у RSA) або дискретний логарифм (як у криптосистем, що базуються на дифіе-Геллмані).