Криптографічні методи захисту інформації

Криптографія (від грецького κρυπτός — прихований і gráphein — писати) — наука про методи безпечного спілкування в присутності третіх осіб. Вона також використовується для встановлення безпечного з'єднання між двома системами. Криптографія використовує математику (перш за все арифметику та теорію чисел) для забезпечення конфіденційності, цілісності та автентичності повідомлень за певних умов. Криптографія включає в себе конфіденційність, гарантуючи, що інформацію неможливо прочитати або підробити під час передачі.

Тривалий час під криптографією розумілось лише шифрування — процес перетворення звичайної інформації (відкритого тексту) в незрозуміле «сміття» (тобто, шифротекст). Дешифрування — зворотний процес відтворення інформації із шифротексту. Шифром називається пара алгоритмів шифрування/розшифрування. Дія шифру керується як алгоритмами, та, в кожному випадку, ключем. Ключ — секретний параметр (в ідеалі, відомий лише двом сторонам) для окремого контексту під час передачі повідомлення. Ключі мають велику важливість, оскільки без змінних ключів алгоритми шифрування легко зламуються і непридатні для використання в більшості випадків. Історично склалось так, що шифри часто використовуються для шифрування та дешифрування, без виконання додаткових процедур, таких як аутентифікація або перевірка цілісності.

Алгоритми шифрування

Алгоритм криптографії — це метод шифрування та дешифрування, який використовує математичну формулу для перетворення звичайного тексту в зашифрований текст і навпаки. **Алгоритм криптографічного шифрування** — це тип шифру, який використовується для забезпечення конфіденційності та цілісності даних у комп'ютерній системі. Він використовує ключ шифрування для перетворення відкритого тексту в зашифрований текст, який потім надсилається через мережу, наприклад Інтернет, до місця призначення, де одержувач розшифрує його.

Алгоритми криптографічного шифрування зазвичай використовуються в комерційній електронній торгівлі, онлайн-банкінгу та інших програмах, де конфіденційність є важливою. Ці алгоритми шифрування включають **Data Encryption Standard (DES), Triple DES, Blowfish і CAST-256**.

Існує багато типів криптографічних алгоритмів. Вони відрізняються за складністю та захищеністю залежно від типу зв'язку та конфіденційності інформації, якою обмінюються.

При цьому можна виділити два основні типи алгоритмів шифрування, які використовуються для захисту інформації: **блоковий шифр** і **потоковий шифр**

Блоковий шифр шифрує дані по блоках фіксованого розміру, зазвичай 64 або 128 біт. Кожен блок шифрується незалежно від інших блоків, використовуючи ключ шифрування. Блокові шифри часто використовуються для шифрування великих обсягів даних, таких як файли або диски.

Потоковий шифр шифрує дані по одному біту або байту за раз. Потокові шифри генерують

псевдовипадковий потік ключів, який використовується для шифрування даних. Потокові шифри часто використовуються для шифрування потоків даних, таких як голосовий або відео зв'язок.

Як працюють різні криптографічні алгоритми?

Криптографічні алгоритми мають базовий алгоритм, який виробляє **ключ**, і кожен з них використовує цей ключ для шифрування та дешифрування інформації. Але є багато способів зробити це.

Одним із способів є використання **блокового шифру**, який бере кілька байтів і перетворює їх у більш розширену послідовність байтів. Цей процес називається шифруванням.

Інший спосіб полягає в тому, щоб взяти блоковий шифр, перетворити його на щось менше, а потім перетворити його назад у початковий розмір блоку. Цей процес називається дешифруванням (або дешифруванням).

Ці алгоритми можуть бути **симетричними** або **асиметричними**, залежно від використовуваного алгоритму.

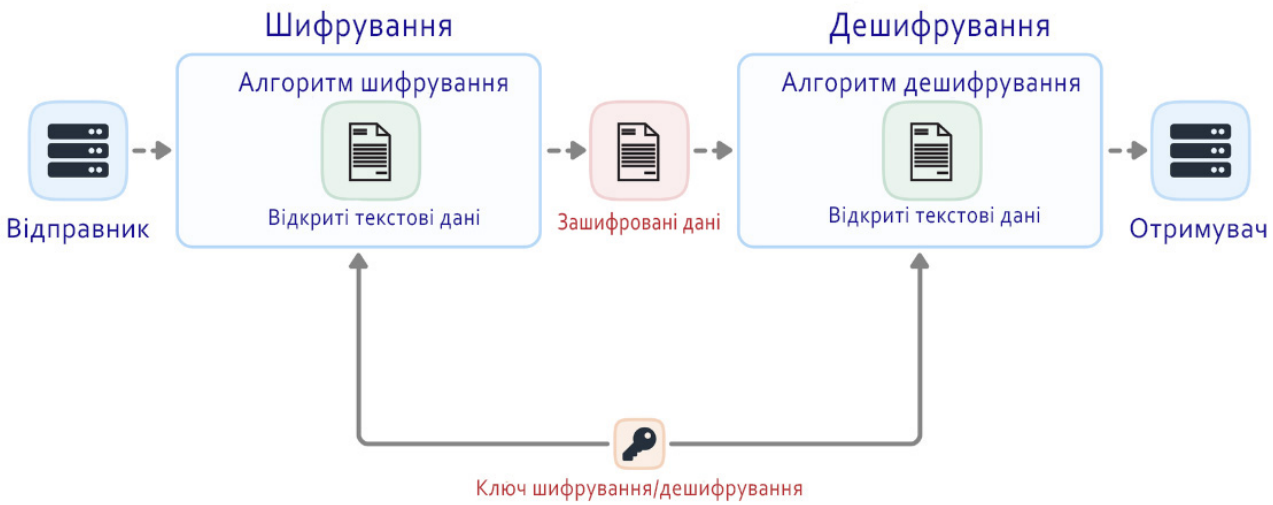
Симетричні алгоритми використовують один і той самий ключ для шифрування та дешифрування даних, тоді як **асиметричні** алгоритми використовують два окремих ключі: один для шифрування та інший для інтерпретації даних.

Алгоритми також використовують код автентифікації повідомлення (MAC), щоб забезпечити цілісність повідомлення.

Криптографія секретного ключа

Симетричне шифрування

Симетричне шифрування, також відоме як шифрування з **секретним ключем**, полягає у використанні одного криптографічного ключа як для шифрування, так і для дешифрування даних. На малюнку нижче показано, як відкритий текст можна перетворити на зашифрований за допомогою шифру та секретного ключа. Той самий ключ використовується, коли шифр працює в режимі дешифрування для отримання відкритого тексту із зашифрованого. **Шифр** — це набір двох алгоритмів: алгоритму шифрування (Encryption) `E(K,m) → c`, який приймає ключ шифрування `K` та повідомлення `m`, яке потрібно зашифрувати, як параметри і повертає зашифрований текст `c`, а також алгоритму дешифрування (Decryption) `D(K,c) → m`, що визначається як операція, зворотна шифруванню та розшифровує повідомлення назад до початкового відкритого тексту.



Симетричне шифрування

Генерація симетричних ключів

Симетричні ключі шифрування використовуються двома сторонами для безпечного шифрування та дешифрування даних. Генерація та обмін згенерованими ключами повинні здійснюватися безпечним способом.

Симетричні ключі забезпечують такий же рівень безпеки, як і їхня кількість бітів, тобто 128-бітний ключ забезпечує 128-бітний захист (відносно атаки грубої сили) і може бути згенерований за допомогою криптографічного генератора псевдовипадкових чисел. Така бібліотека, як **OpenSSL**, надає набір інструментів для генерації випадкового симетричного ключа.

> Метод «грубої сили» (від англ. brute force; або повний перебір) — метод рішення криптографічної задачі шляхом перебору всіх можливих варіантів ключа. Складність повного перебору залежить від кількості всіх можливих рішень задачі. Якщо простір рішень дуже великий, то повний перебір може не дати результатів протягом декількох років або навіть століть.

Розширений стандарт шифрування (AES)

Розширений стандарт шифрування (Advanced Encryption Standard) (AES) - алгоритм шифрування, що характеризується двома елементами, а саме розміром блоку та розміром ключа. Повідомлення відкритого тексту ділиться на блоки b бітів, де b — розмір блоку. Зазначені блоки потім обробляються функцією шифрування всі одночасно, додаючи необов’язкове доповнення в кінці, коли розмір відкритого тексту не є цілим числом, кратним розміру блоку. Більшість шифрів, які сьогодні використовуються для шифрування даних, є блоковими шифрами завдяки своїй практичності та ефективності.

Розширений стандарт шифрування (AES) є найпоширенішим шифром у світі. Він був прийнятий як стандарт шифрування Національним інститутом стандартів і технологій США (NIST) у 2001 році для шифрування електронних даних. Він замінює застарілий стандарт шифрування даних (DES), який був представлений у 1977 році. AES визначає набір алгоритмів із симетричним ключем і існує в різних варіантах, а саме 128, 192 та 256-бітних розмірів ключа. Алгоритм шифрування AES застосовує кілька раундів замін і перестановок до початкового відкритого тексту та виводить зашифрований текст такої ж довжини, що й відкритий текст.

MAC-підпис

MAC (англ. message authentication code — код аутентифікації повідомлення) — спеціальний набір символів, що додається до відповідного повідомлення, логічно поєднаний з цим повідомленням та призначений для забезпечення цілісності повідомлення та аутентифікації джерела даних.

Шифрування, будучи основним застосуванням криптографії, не забезпечує всіх гарантій безпеки, необхідних для захисту даних. Дійсно, дані користувача все ще можуть бути підроблені в їх зашифрованому стані, збережені в базі даних, наприклад, якщо не вжити належних заходів для перевірки цілісності зазначених даних. Коди автентифікації повідомлень (MAC) створюють теги, які застосовуються до повідомлення, щоб гарантувати його автентичність і цілісність. MAC — це функція з ключем `T = MAC(K,m)`, яка дає змогу будь-якій стороні, яка знає ключ MAC, перевірити цілісність повідомлення, обчислюючи тег у повідомленні та перевіряючи, чи він відповідає отриманому тегу. У захищених комунікаціях і зберіганні даних практикується комбінування **шифру** та **MAC**, щоб забезпечити конфіденційність, цілісність і автентичність даних.

Криптографія з відкритим ключем

Асиметричне шифрування

В асиметричному шифруванні є два ключі, один для шифрування, а інший для дешифрування. Асиметричне шифрування забезпечило набагато більшу гнучкість безпечного зв’язку, оскільки ключ шифрування не зберігається в секреті. Наприклад, якщо відправник, Аня, хоче надіслати повідомлення Максиму, то Аня отримує відкритий ключ шифрування Максима, який стає доступним для всіх, хто хоче зашифрувати повідомлення та надіслати його Максиму. Потім вона шифрує повідомлення ключем Максима перед тим, як надіслати йому зашифрований текст. Лише Максим може розшифрувати зашифрований текст за допомогою свого приватного ключа розшифровки, який залишається секретним. В симетричному шифруванню перед початком процесу шифрування у нас виникає проблема встановлення безпечного каналу для обміну секретним ключем шифрування/дешифрування. Це обмеження знято в асиметричному шифруванні.

Асиметричне шифрування

Цифровий підпис

Електро́нний цифровий підпис (ЕЦП) (англ. digital signature) — 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. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Цифровий підпис є еквівалентом відкритого ключа **MAC**. Це дозволяє будь-якій стороні додавати підпис до повідомлення за допомогою приватного ключа. Подібно до традиційних підписів на папері, будь-яка сторона може перевірити автентичність відправника за допомогою публічного алгоритму перевірки та відкритого ключа. Схема цифрового підпису складається з алгоритму підпису `S(SK,m) → s`, який створює підпис `s` із закритого ключа SK у повідомленні `m`, і алгоритму перевірки `V(PK,s)→{0,1 }`, який повертає логічне значення `0` (або `false`), якщо процес перевірки не вдається, або `1` (або `true`), якщо перевірка вдається.

Хеш-функції

Хеш-функція, або геш-функція — функція, що перетворює вхідні дані будь-якого (як правило великого) розміру в дані фіксованого розміру.

Хешування (гешування, англ. hashing) — перетворення вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини. Такі перетворення також називаються хеш-функціями, або функціями згортання, а їхні результати називають хешем, хеш-кодом, хеш-сумою, або дайджестом повідомлення (англ. message digest).

Хеш-функція є надзвичайно корисним інструментом у наборі інструментів криптографа. Вони використовуються в побудові багатьох криптографічних протоколів, включаючи MAC, цифрові підписи, шифрування з відкритим ключем, протоколи узгодження ключів і багато інших. Такі

алгоритми, як **MD5**, **SHA-1**, **SHA-256**, **SHA-3** і **BLAKE2**, є найвідомішими хеш-функціями. Кожного разу, коли ви підключаєтеся до веб-сайту через HTTPS, надсилаєте електронний лист, отримуєте доступ до файлу в системі хмарного сховища або використовуєте SSH для підключення до віддаленого сервера використовується криптографічна хеш-функція.

Автентифіковане шифрування

Автентифіковане шифрування (Authenticated Encryption) (AE) поєднує симетричне шифрування з перевіркою цілісності та автентичності шляхом додавання тегу до зашифрованого тексту. Дійсно, лише шифрування не забезпечує цих вимог безпеки, і більшість безпечних реалізацій криптографії тепер повинні використовувати цю парадигму. Шифр `AE(K,m) → (c,t)` повертає зашифрований текст і короткий рядок як тег. Тег забезпечує цілісність і гарантує, що зашифрований текст ідентичний тому, який надіслав законний відправник. Це також забезпечує автентичність зашифрованого тексту, оскільки лише відправник, який володіє секретним ключем, може створити цю пару **зашифрований текст - тег**. Вимога безпеки передбачає, що жоден зловмисник не зможе вгадати тег без ключа. Процес дешифрування повертає повідомлення відкритого тексту із зашифрованого тексту тоді і тільки тоді, коли тег `t` є дійсним тегом. Вимоги до безпеки для процесу шифрування залишаються такими ж, як і для будь-якого надійного шифру.

Схема **AE** будується шляхом поєднання симетричного шифру з **MAC**. Найбезпечнішим підходом до цієї комбінації є підхід «Зашифрувати-потім—MAC», у якому зашифрований текст спочатку обчислюється з відкритого тексту, а потім для зашифрованого тексту обчислюється тег. У процесі дешифрування одержувач спочатку обчислює MAC для зашифрованого тексту, щоб переконатися, що тег ідентичний отриманому, а потім він розшифровує зашифрований текст після перевірки автентичності.

Автентифіковане шифрування

Джерела

- Криптографія
- Cryptography Techniques: Everything You Need to Know
- Блоковий шифр
- Потоковий шифр
- Метод_«грубої_сили»
- Advanced_Encryption_Standard
- MAC-підпис

- A Primer on Cryptography
- Хеш-функція

From:
https://library.vpuhlukhiv.com.ua/ - **Wiki Глухівського ВПУ**

Permanent link:
https://library.vpuhlukhiv.com.ua/subjects:basic:informatika:infsecurity:crypto_protection?rev=1706655202

Last update: **31.01.2024 00:53**