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.

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

Джерела

- Криптографія
- Cryptography Techniques: Everything You Need to Know
- Блоковий шифр
- Потоковий шифр