УДК 004.62

Морозюк А.А., студентка 2 курсу спеціальності 122 «Комп'ютерні науки»
Ніколюк П.К. д.ф.-м.н., професор, професор кафедри комп'ютерних технологій

ШИФРУВАННЯ ДАНИХ

Донецький національний університет імені Василя Стуса, м. Вінниця

У наш час, коли кількість кіберзлочинів постійно зростає, розуміння того, що існує так само багато варіантів захисту від них, наприклад, використання шифрування, тобто перетворення даних із звичного для нас формату в закодований, значно полегшує процеси маніпуляцій з даними. Цей метод захисту є основою безпеки даних, оскільки є найкращим способом гарантії того, що інформація не буде викрадена та прочитана кимось стороннім, хто планує використати її задля власних цілей.

Шифрування інформації виконується із використанням відкритого тексту, тобто даних, які необхідно зашифрувати, ключа та алгоритмів, які загалом є математичними обчисленнями, що працюють із необробленою інформацією. Алгоритм зміни значень: шифрування перетворює відкритий текст у нечитабельний формат, тобто в «зашифрований», далі здійснюється робота з інформацією зі сторони користувача, наприклад, надсилання її одержувачу, після чого інформація буде повернута до початкової форми, тобто відбудеться дешифрування. Для того, щоб мати доступ до закодованої інформації, як відправник, так і одержувач, повинні використовувати ключі шифрування (рядки випадкових символів у певній послідовності) [1].

Процес шифрування можливий завдяки криптографічним ключам та математичним алгоритмам, які відрізняються за індексами безпеки та програмою. Існують наступні методи шифрування даних: симетричне, асиметричне та хешування. Розглянемо кожен з них:

1. Симетричне шифрування – це шифрування, яке містить лише один криптографічний ключ, який використовується як для шифрування відкритого тексту, так і для його дешифрування. Перевагами цього способу є те, що, по-перше, він є досить ефективним, оскільки під час його виконання немає значних часових затримок, майже не впливає на швидкість інтернету та потребує невеликої кількості обчислювальної потужності, по-друге, він забезпечує певний рівень автентифікації, оскільки дані можливо розшифрувати лише одним ключем, який тримається в секреті двома сторонами, то кожен може бути впевнений у безпеці даних. Недоліком цього методу є те, що хтось сторонній може отримати доступ до ключа. В такому випадку, особа, яка володіє несанкціонованим симетричним ключем, матиме доступ до даних та зможе не тільки розшифрувати їх, а й змінити [2].

2. Асиметричне шифрування – це шифрування, яке розшифровує дані за допомогою двох окремих криптографічних ключів. Ці два ключі відомі ще як «відкритий ключ» і «закритий ключ». Перевагою цього методу є те, що він дає змогу довірити відкритий ключ кожному, хто відправляє інформацію, а приватний ключ зберігати при собі. Такий підхід унеможливлює ризик компрометації ключа, а тому підвищує рівень безпеки. Також до переваг асиметричного шифрування можна віднести автентифікацію. Завдяки тому, що дані можуть бути розшифровані тільки за допомогою закритого ключа, є гарантія того, що їх побачить і дешифрує тільки той користувач, який повинен їх отримати [3].
3. Хешування – це процес, під час якого відбувається алгоритм перетворення даних будь-якого розміру в унікальний результат(наприклад, комбінацію цифр разом із буквами), що матиме фіксований розмір. Загалом хешування використовується лише для перевірки даних, тому що інформація, зашифрована за допомогою цього методу, не зможе бути розшифрованою або повернутою до початкового значення. Незважаючи на те, що хешування у комбінації з іншими методами може підвищити безпеку даних, багато експертів не вважають його фактичним способом захисту інформації [2].

На сьогодні, окрім шифрування інформації, що передається, важливим також постає питання безпеки даних, що зберігаються на пристроях, якими ми користуємось, тому що існує ймовірність того, що вони можуть стати зараженими зловмисним програмним забезпеченням, яке шукатиме конфіденційні дані та надсилатиме їх кіберзлочинцю. Для того, щоб унеможливити подібні ситуації, використовується шифрування файлів, яке захищає файлові системи та робить їх доступними тільки для особи, що володіє ключем, яким здійснювався захист та який зазвичай має вигляд пароля або фрази, що дозволяє розшифрувати вміст. Одразу після того, як авторизований одержувач введе правильний пароль або фразу, файл стає читабельним. Підтримка такого методу захисту даних може бути вбудована в операційну систему або файлову систему та працюватиме за рахунок використання складних алгоритмів. Система надійно зберігатиме конфіденційні файли, а ключ дешифрування забезпечуватиме доступ до них. Окрім вбудованих засобів безпеки, може використовуватись додаткове програмне забезпечення, що є, безумовно, найкращим рішенням, оскільки має багато переваг, наприклад, багатошаровий захист даних, збереження цілісності та відповідності, безпечну передачу інформації та надання безпеки декільком пристроям. Також деякі компанії шифрують свої дані в хмарі, але їх меншість, оскільки зберігання зашифрованих файлів у хмарних програмах може бути складнішим [4].

Враховуючи вищенаведену інформацію, можна помітити, що шифрування має досить багато переваг. Перелік переваг:

1. Покращує цілісність даних.
2. Захищає конфіденційність користувачів.
3. Дозволяє безпечно ділитися файлами.

4. Захищає хмарні дані.
5. Підвищує довіру споживачів.
6. Захищає втрачені або ж викрадені пристрої.
7. Забезпечує конкурентну перевагу.
8. Не вимагає значних витрат.

Незважаючи на достатню кількість переваг, шифрування має також і недоліки. Наприклад, втрата значення пароля може призвести до втрати всіх даних, оскільки не буде можливості їх відновити. Також до недоліків можна віднести розвиток хибного відчуття безпеки, тому що з розвитком технологій програмування, розкриття зашифрованих файлів у майбутньому може стати звичною справою, проте необхідно враховувати і те, що методи шифрування також вдосконалюються і цей процес не буде легким [5].

Шифрування даних є доволі важливим процесом та має багато сфер застосування. Важливим воно є, наприклад, через те, що це головна умова роботи компаній. Шифрування допомагає захистити дані від кіберзлочинців та забезпечити можливість спілкування без витоку конфіденційної інформації, тим самим, захистивши корпорацію від зайвих витрат і процесів відновлення даних після порушень безпеки. В інших випадках, якщо дані не стосуються компанії, такий метод захисту інформації допомагає, до прикладу, підвищити безпеку зв'язку між клієнтськими програмами та серверами, захистити приватну інформацію та конфіденційні дані. Особливо важливою є роль шифрування у процесі передачі даних під час фінансових транзакцій. Спектр сфер застосувань досить широкий, прикладом може бути наступний перелік галузей: захист пристроїв, веб-сайтів, повідомлень у різних соціальних мережах, підтвердження автентичності та цілісності інформації за допомогою цифрових підписів, стирання даних, використання у біржових системах, інтернет-трафік.

Отже, шифрування даних – це достатньо складний процес, що вимагає постійного розвитку, пошуку нових способів забезпечення безпеки та вдосконалення існуючих, зобов’язує до ретельного аналізу, планування, чіткої реалізації та професіоналізму на всіх етапах.

Список літературних джерел:

1. *What Is Data Encryption: Types, Algorithms, Techniques and Methods. URL: https://cutt.ly/01DxzfF (дата звернення: 01.12.2022).*
2. *What is encryption? Data encryption defined. URL: https://cutt.ly/51DxDSU (дата звернення: 01.12.2022).*
3. *Шифрування: типи і алгоритми. Що це, чим відрізняються і де використовуються?. URL: https://cutt.ly/S1DcaVu (дата звернення: 02.12.2022).*
4. *What is file encryption?. URL: https://cutt.ly/y1DcLmT (дата звернення: 02.12.2022).*
5. *Advantages of Using Encryption. URL: https://cutt.ly/t1DviQm (дата звернення: 02.12.2022).*