2. About CVE [Електронний ресурс] // The MITRE Corporation. – 2021. – Режим доступу до ресурсу: https://cve.mitre.org/about/index.html.

3. Vulnerability Notes Database [Електронний ресурс] // Carnegie Mellon University. – 2021. – Режим доступу до ресурсу: https://www.kb.cert.org/vuls/.

4. Exploit Database [Електронний ресурс] // OffSec Services Limited. – 2021. – Режим доступу до ресурсу: https://www.exploit-db.com/.

Ключові слова: вразливості, інформаційна безпека, бази даних, комп'ютерні системи.

Ключевые слова: уязвимости, информационная безопасность, базы данных, компьютерные системы.

Keywords: vulnerabilities, information security, databases, computer systems.

Плаксін Олександр Андрійович

Національний університет «Одеська юридична академія»,

студент 3-го курсу факультету кібербезпеки та інформаційних технологій

СУЧАСНІ КРИПТОГРАФІЧНІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ

Криптографія – це наука про приховування інформації від несанкціонованих осіб.

Криптографія починає свою історію ще з далеких часів Римської імперії, коли був придуманий один із перших шифрів - Шифр Цезаря. З того часу криптографія просунулась далеко вперед і тепер використовується по всьому світу навіть у звичайнісіньких для нас речах: месенджерах, соціальних мережах, при перегляді ТБ, при серфінгу Інтернету тощо.

Зараз у світі існує безліч способів приховування інформації. Розберемо принцип їхньої дії, їх переваги та недоліки.

1) RSA (абревіатура від прізвищ Rivest, Shamir та Adleman) — один з найвідоміших методів шифрування, більш відомий як метод "ключа та замка". Працює він за таким принципом: Співрозмовник 1 створює свій ключ і замок, співрозмовник 2 робить так само. Далі вони обмінюються "замками". Після цього співрозмовник 1 закриває своє повідомлення замком, який йому дав співрозмовник 2. Так, тепер навіть сам співрозмовник 1 не може відкрити своє повідомлення, але це легко може зробити співрозмовник 2, тому що він має ключ від свого ж замку, яким закрито повідомлення від співрозмовника. 1.Метод працює шляхом створення величезних чисел за рахунок 2х невеликих натуральних чисел. Величезне число, що вийшло внаслідок множення двох натуральних чисел - це і є той самий "замок", тобто публічний ключ. А пара чисел, що дає велике число при перемноженні - це і є приватний ключ. Компрометація приватного ключа може призвести до компрометування всіх зашифрованих даних.

Переваги методу RSA:

1. Діапазон застосування. Даний метод використовується практично в кожній системі шифрування, починаючи від сайтів, закінчуючи різними сервісами обміну повідомлень.

2. Стабільність. Імовірність "неправильного шифрування" при використанні цього методу досить низька за рахунок невеликої кількості факторів, що забезпечують шифрування.

3. Простота використання. Достатньо згенерувати пару ключів, зашифрувати публічним ключем свої дані, а приватний ключ можна перемістити на флешку та носити його із собою. Так, компрометація приватного ключа зводиться нанівець.

Недоліки методу RSA:

1. Не найкраща криптостійкість. Вже є випадки, коли ці два натуральні числа вдалося підібрати через їх слабку генерацію. Це призвело до повної компрометації даних, незважаючи на гарний захист приватного ключа.

2. Кастомізація — не під силу кожному.

Для створення надійної пари ключів зі своїми числами та певною довжиною, необхідно володіти деякими знаннями в галузі математики.

3. Відсутність додаткових захисних механізмів. Незважаючи на те, що приватний ключ можна зашифрувати паролем під час використання, це не виключає ризик підбору цього пароля методом грубої сили.

Незважаючи на це, RSA залишається досить надійним та популярним способом зашифрувати свої дані від третіх осіб.

У руках людини, яка розуміється на математиці та криптографії, цей метод перетворюється вже на щось більше, ніж просто пара ключів і "замків".

2) AES (Advanced Encryption Standard) - сучасний "золотий стандарт" шифрування, ухвалений основним стандартом шифрування урядом США.

Використовує симетричну (на відміну RSA, яка асиметрична) блокову систему шифрування.

Переваги методу AES**:**

1. Широке використання у всьому світі. AES - золотий стандарт, на який всі намагаються дорівнювати. Потужніше шифрування, ніж AES, поки що, не придумали, хіба що багаторазове шифрування цим способом.

2. Висока криптостійкість. Завдяки алгоритму генерації раундових ключів, зміщення рядків та зворотної лінійної трансформації, метод став по-справжньому стійким до різних технік зламів, які ефективні проти інших методів, але не ефективні проти AES.

3. Висока надійність. AES використовує симетричний метод шифрування, тобто ключ, який шифрує - він і розшифровує. Створивши надійний пароль, припустимо, на 32+ символи, на його перебір підуть роки, якщо не століття. Це єдиний спосіб скомпрометувати дані.

Недоліки методу AES:

1. Симетричність. Якщо пароль буде скомпрометовано – всі дані будуть доступні третім особам. Пароль, на сьогоднішній день, не є надійним фактором захисту через нестійкість до перебору.

2. Потрібні деякі навички в галузі криптографії. Існує ймовірність "неправильного шифрування" даних. У такому разі є великий ризик втратити

свої дані для недосвідченого користувача. Перед використанням даного методу краще ознайомитися з інструкцією.

3. Квантова нестійкість. Нещодавні дослідження швейцарських криптографів показали, що алгоритм AES може бути "вскритий" за допомогою квантового суперкомп'ютера протягом кількох років [1].

Тим не менш, на сьогоднішній день, AES залишається одним із найкращих світових стандартів шифрування.

3) GreyNigma(Gigma) - нова розробка в області криптографії, що дозволяє конвертувати текст, що вводиться, в цифри, закриті кривими дужками [2].

Всі цифри, на які замінюються символи - повністю довільні і виставляються користувачем, а також можуть бути згенеровані за допомогою спеціального вбудованого генератора.

Gigma використовує симетричний спосіб шифрування. Усі цифри, на які замінюються символи, зберігаються в спеціальній конфігурації, яку потрібно передати співрозмовнику. Після цього співрозмовник зможе розшифровувати та писати зашифровані повідомлення. Якщо конфігурація не співпадатиме з тією, якою шифрувалося повідомлення - на виході вийде випадковий набір із символів.

Gigma має такі захисні механізми:

- Зміщення літер**.** Всі букви, що вводяться, можуть бути "зсунуті" вліво або вправо, подібно до шифру Цезаря. Зрушення виробляється на певне число, визначене у конфігурації, воно може бути від -26 до 26, оскільки поки що підтримуються лише літери англійського алфавіту, а він має 26 літер.
- Поділ рядків**.** Усього є цілих 3 варіації рядка. Основна їхня відмінність - це те, що у кожного рядка свої значення для кожного символу. У перший рядок можна записати справді важливу інформацію, а в два інші - спотворену чи зовсім непотрібну.
- Випадковий шаблон**.** Кінцеве зашифроване повідомлення може мати абсолютно випадковий порядок рядків, що лише посилює криптостійкість шифру, але ніяк не впливає на розшифровку та кінцевий результат.
- Присолювання**.** Для збільшення потужності шифру, а також штучного збільшення розміру зашифрованого повідомлення, існують спеціальні порожні

рядки, що називаються "солі". Вони виступають як баласт, але при розшифровці правильною конфігурацією вони просто зникають.

- Розворот рядка. Крім того, все повідомлення може бути представлене у зворотному порядку. Ця опція так само визначається конфігурації і повністю регульована. Наприклад, слово "Hello" може перетворитися на "olleH", тим самим лише забезпечуючи ще більший ступор третіх осіб, які можуть намагатися розшифрувати повідомлення.

Конфігурація може бути зашифрована методом RSA за допомогою спеціально розробленого інструменту та безпечно передана співрозмовнику, не переймаючись тим, що може бути перехоплена.

З недоліків можна відзначити тільки те, що все ж таки, цей шифр може бути зламаний шляхом перебору, але враховуючи те, що в сукупності всього існує мінімум 225! (Факториал) варіацій розмістити символи для одного рядка (а їх 3) в конфігурації для одного повідомлення, це може зайняти десятки років, або навіть сторіччя.

Таким чином, у кожного розглянутого метода шифрування є свої недоліки і переваги, що дозволяє використовувати їх безпосередньо за їх призначенням.

Список використаних джерел:

1. Дослідження швейцарських криптографів щодо вразливості AES. URL: https://roskomsvoboda.org/69451 (Дата звернення: 1.11.2021).

2. Grey_Hat_Cybersecurity / GreyNigma. URL: https://notabug.org/Grey_Hat_Cybersecurity/GreyNigma (Дата звернення: 1.11.2021).

Ключові слова: Криптографія, шифрування, RSA, AES, GreyNigma, безпека

Ключевые слова: Криптография, шифрование, RSA, AES, GreyNigma, безопасность

Keywords: Cryptography, encryption, RSA, AES, GreyNigma, security