УДК 004.056.55

СУЧАСНІ АЛГОРИТМИ ШИФРУВАННЯ ІНФОРМАЦІЇ ПРИ РОБОТІ SSL-СЕРТИФІКІВ

Гринчий Н.О., НУЦЗУ
НК – Маляров М.В., к.т.н., доц., НУЦЗУ

Зазвичай при перегляді веб-сторінок, інформація передається у відкритому вигляді. Якщо на шляху передачі трапляться шахраї, вони зможуть перехопити інформацію й використати її в особистих цілях. Щоб уникнути таких ситуацій, потрібен SSL-сертифікат. На сайті з SSL-сертифікатом веб-переглядач використовує безпечне з'єднання. У теперішній час при роботі SSL-сертифіката використовуються два типи шифрування: симетричне й асиметричне.

Метод симетричного шифрування використовує один криптографічний ключ для шифрування та дешифрування даних, що робить процес простим.

Насьогодні у якості симетричного шифрування зазвичай використовуються алгоритм симетричного шифрування AES (advanced encryption system) також відомий як Rijndael. AES – це сімейство блокових шифрів з різною довжиною ключів та різними розмірами блоків.

AES працює методами підстановки та перестановки. Спочатку незашифровані дані перетворюються на блоки, а потім шифрування застосовується з використанням ключа. На сьогоднішній день AES використовується в багатьох програмах, включаючи: бездротову безпеку, безпека процесорів та шифрування файлів, протокол SSL/TLS, безпека Wi-Fi, шифрування мобільних додатків, VPN (virtual private network) тощо.

Асиметричне шифрування, на відміну симетричного, включає кілька ключів для шифрування і дешифрування даних, які математично пов'язані друг з одним. Один із цих ключів відомий як «відкритий ключ», а інший – як «закритий ключ». У теперішній час зазвичай використовується алгоритм асиметричного шифрування RSA

Алгоритм винайшли троє вчених з Массачусетського технологічного інституту у 1977 році. По суті, вибираються два різні випадкові прості числа заданого розміру (наприклад, 1024 біта кожне) і множаться, щоб створити ще одне гігантське число. Завдання у тому, щоб визначити вихідні прості числа з помноженого гігантського. Великою перевагою RSA є його масштабованість. RSA ґрунтується на простому математичному підході, тому його реалізація в інфраструктурі відкритих ключів (PKI) стає легкою. Адаптивність та безпека зробили RSA найбільш використовуваним алгоритмом асиметричного шифрування для різних програм, включаючи сертифікати SSL/TLS, криптовалюти та шифрування електронної пошти.

Більшість сучасних SSL сертифікатів використовують гібридний метод: асиметричне шифрування для автентифікації та симетричне шифрування для конфіденційності.

ЛІТЕРАТУРА

1. Шифрование: типы и алгоритмы. Что это, чем отличаются и где используются? [електронний ресурс] назва з екрану. Режим доступу: https://wiki.hostpro.ua/knowledgebase/shifrovanie-tipy-i-algoritmy/.