- функція розподіл інтервалу часу Δt між сусідніми заявками в найпростішому потоці:

$$P(\Delta t) = P(\tau < \Delta t) = 1 - \lambda e^{-\lambda \Delta t} \quad (4)$$

По-суті, це ймовірність того, що за інтервал Δt надійде один і більше викликів.

- щільність розподілу ймовірності Δt:

$$p\ (\Delta t) = \lambda e\ -\lambda \Delta t \quad (5)$$

Таким чином, розподіл проміжків часу між викликами найпростішого потоку підпорядковується показовому (негативного експоненціальним) законом [4].

Список використаних джерел

1. Алгоритмічні(імітаційні) моделі в економіці та підприємництві: https://cutt.ly/0MwZDwK (дата звернення 7.11.22)

2. Моделювання випадкових подій та величин: https://cutt.ly/kMwZGjR (дата звернення 7.11.22)

3. Імовірнісне моделювання. Моделювання випадкових процесів: https://cutt.ly/uMwZX1Y (дата звернення 7.11.22)

4. Випадкова величина: https://cutt.ly/jMwZNpO (дата звернення 7.11.22)

УДК 681.188:004.056.5

Станіславчук Д. О.,
здобувач 2 курсу спеціальності
125 «Кібербезпека»
Зелінська О.В., доцент кафедри
інформаційних технологій

КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Донецький національний університет імені Василя Стуса, м. Вінниця

На сьогоднішній день одним з найцінніших ресурсів є інформація. З кожним днем її стає все більше, тому збільшується потреба в забезпеченні захисту. В забезпеченні інформаційної безпеки важливу роль відіграє криптографічний захист.

Криптографічний захист - вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо [1].

Ключовим поняттям тут є “Криптографія”.

Криптографія - наука про математичні методи забезпечення конфіденційності, цілісності і автентичності інформації. Її розвиток пов’язаний з потребою передавати таємну інформацію [2].

Найбільше криптографія асоціюється з поняттям шифрування.

Шифрування — це обчислювальний процес, який кодує відкритий текст (незашифровані, зрозумілі людині дані) у зашифрований текст (зашифровані дані), доступ до якого мають лише авторизовані користувачі з правильним криптографічним ключем [3]. Для його виконання використовуються спеціальні криптографічні алгоритми – шифри.

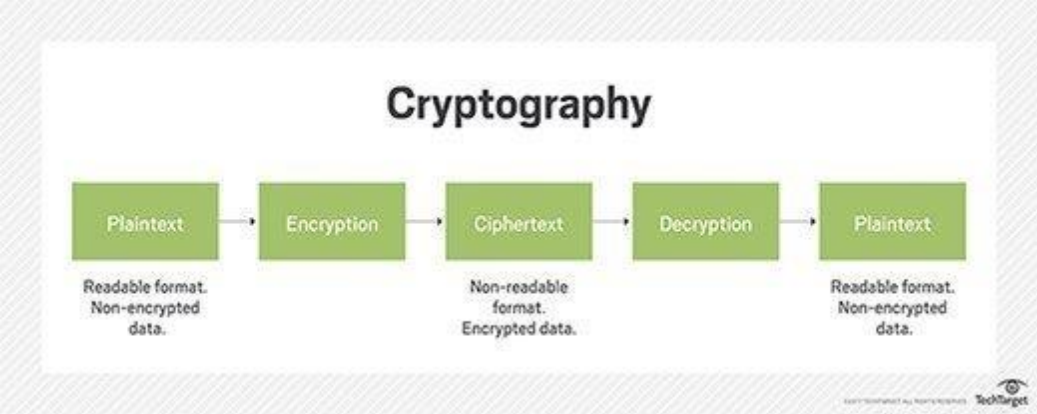

Рис. 1 Алгоритм передачі зашифрованого повідомлення [4].

Відправник передає повідомлення (відкритий текст) шифрувальній машині, яка шифрує його в шифротекст. Це повідомлення передається одержувачу, де повідомлення розшифровується за допомогою ключа, отримуючи вихідний текст. Через те, що повідомлення шифрується до того як відправляється, зловмисник, навіть якщо перехопить повідомлення, отримає лише зашифровану інформацію, яку без ключа буде важко розшифрувати.

На даний момент існує 2 основних методи шифрування – симетричне та асиметричне.

Симетричне шифрування - методи шифрування, в яких відправник, і отримувач повідомлення мають однаковий ключ, або ключі різні, але легко обчислюються. Його перевагами є: простота, швидкість роботи алгоритмів, створення надійного ключа є недорогим, та розмір ключа. Недоліки: потреба в надійному каналі для передавання ключа [5].

Асиметричне шифрування - алгоритм шифрування, включає пару ключів, відому як відкритий ключ і закритий ключ (пара відкритих ключів), які пов’язані з об’єктом, якому необхідно підтвердити свою автентичність в електронному вигляді або підписати або зашифрувати дані. Кожен відкритий ключ публікується, а відповідний закритий ключ зберігається в секреті. Дані, зашифровані відкритим ключем, можна розшифрувати лише відповідним закритим ключем [6]. Переваги: ключ неможливо перехопити, менша кількість ключів. Недоліки: вартість, швидкість алгоритмів, довжина ключів.

Багато хто може помилково подумати що криптографія - це лише про передавання секретних повідомлень між якимись надважливими установами які потребують виключної надійності і тд. Але насправді ми кожен день стикаємось з певними криптографічними засобами захисту. Ось найпопулярніші з них:

- Електронний цифровий підпис – засіб, вид електронного підпису, який дозволяє перевірити користувача (підписувача) та цілісність інформації до якої він прикріплюється.
- Хеш-функція – алгоритм який кодує певну інформацію довільної довжини в бітовий рядок фіксованої довжини. Його особливістю є те, що зміна хоча б одного символу повністю змінить рядок. Цей рядок використовують для перевірки контрольної суми, що гарантує, якщо в процесі передачі інформацію було змінено, контрольна сума не співпаде.
- Цифровий сертифікат - інформація, яка допомагає перевірити чи є ключ до якого він прикріплений вірним.
- Пароль - унікальна послідовність символів, що вводиться як ідентифікаційний код.
- Поділ ключа – це поділ ключової фрази між декількома особами так, що доступ надається лише при наявності встановленої кількості власників ключа

Список використаних джерел

1. *Про Положення про порядок здійснення криптографічного захисту інформації в Україні [Електронний ресурс] реджим доступу: https://zakon.rada.gov.ua/go/505/98 Дата звернення: 02.11.2022*
2. *Криптографія – Вікіпедія [Електронний ресурс] Режим доступу: https://uk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F Дата звернення: 02.11.2022*
3. *What is Encryption and How Does It Work? - Micro Focus [Електронний ресурс] Режим доступу: https://www.microfocus.com/en-us/what-is/encryption Дата звернення: 02.11.2022*
4. *What is Cryptography? Definition from SearchSecurity [Електронний ресурс] Режим доступу: https://www.techtarget.com/searchsecurity/definition/cryptography Дата звернення: 02.11.2022*
5. *Шифрування з симетричними ключами – Вікіпедія [Електронний ресурс] Режим доступу: https://uk.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%B7_%D1%81%D0%B8%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D0%B8%D0%BC%D0%B8_%D0%BA%D0%BB%D1%8E%D1%87%D0%B0%D0%BC%D0%B8 Дата звернення: 02.11.2022*
6. *Public key cryptography – IBM [Електронний ресурс] Режим доступу: https://www.ibm.com/docs/en/ztpf/1.1.0.14?topic=concepts-public-key-cryptography Дата звернення: 02.11.2022*