Філіп'єва М.В., студентка
Гвоздецька К.П., студентка
Харківський національний університет радіоелектроніки, м. Харків
Кафедра Електронних обчислювальних машин

ПОРІВНЯННЯ СИМЕТРИЧНОГО І АСИМЕТРИЧНОГО ШИФРУВАННЯ

Криптографічні системи розділені на дві основні галузі дослідження: симетрична і асиметрична криптографія. Симетричне шифрування часто використовується як синонім симетричною криптографії, а асиметрична криптографія охоплює два основні варіанти використання, це асиметричне шифрування і цифрові підписи.

Алгоритми шифрування діляться на дві категорії, відомі як симетричне і асиметричне шифрування. Принципова відмінність між цими двома методами полягає в тому, що алгоритми симетричного шифрування використовують один ключ, в той час як асиметричні використовують два різних, але пов'язаних між собою ключа [1].

Симетричний алгоритм підходить для передачі великих обсягів шифрованих даних. Асиметричний алгоритм, за інших рівних, буде значно повільніше. Крім того, для організації обміну даними по асиметричному алгоритму або обом сторонам повинні бути відомі відкритий і закритий ключ, або таких пар повинно бути дві (по парі на кожну сторону) [2].

Асиметричне шифрування дозволяє зробити безпечне з'єднання без зусиль з боку користувача, а симетричний алгоритм передбачає, що користувачеві необхідно ще дізнатися пароль [3]. Проте, варто розуміти, що асиметричні алгоритми так само не забезпечують повної безпеки. Наприклад, вони схильні до атак " Man-in-the-middle". Суть останньої полягає в тому, що між вами і сервером встановлюється комп'ютер, який для вас відсилає свій відкритий ключ, а для передачі даних від вас використовує відкритий ключ сервера.

Симетричні алгоритми зазвичай будуються на основі деяких блоків з математичними функціями перетворення [4]. Тому модифікувати такі алгоритми легше. Асиметричні ж алгоритми зазвичай будуються на деяких математичних задачах, наприклад. RSA побудований на завданню зведення в ступінь і взяття по модулю. Тому їх практично неможливо або дуже складно модифікувати.

Як симетричне, так і асиметричне шифрування грає важливу роль в забезпеченні безпеки конфіденційної інформації та комунікації в сучасному цифровому світі [5]. Обидва шифру можуть бути корисні, адже у кожного з них є свої переваги і недоліки, тому вони застосовуються в різних випадках. Оскільки криптографія як наука продовжує розвиватися для захисту від новіших і більш серйозних загроз, симетричні і асиметричні криптографічні системи завжди будуть мати відношення до комп'ютерної безпеки.

Література

1. T. Vitalii, B. Anna, H. Kateryna and D. Hrebeniuk, "Method of Building Dynamic Multi-Hop VPN Chains for Ensuring Security of Terminal Access Systems," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 613-618, doi: 10.1109/PICST51311.2020.9467953.

2. Tkachov V. Principles of Constructing an Overlay Network Based on Cellular Communication Systems for Secure Control of Intelligent Mobile Objects / Vitalii Tkachov, Andriy Kovalenko, Mykhailo Hunko and Kateryna Hvozdetska // Информационные технологии и безопасность. Материалы XIX Международной научно-практической конференции ИТБ-2020. – К.: ООО «Инжиниринг», 2020

3. Tkachov, V., Kovalenko, A., Kuchuk, H., & Ni, I. (2021). Метод забезпечення живучості високомобільної комп'ютерної мережі. Advanced Information Systems-Sučasnì ìnformacìjnì sistemi, 5(2), 159-165.

4. Коваленко А.А. Метод забезпечення живучості комп’ютерної мережі на основі VPN-тунелювання / А.А. Коваленко, Г.А. Кучук, В.М. Ткачов // Системи управління, навігації та зв’язку. Збірник наукових праць. – Полтава: ПНТУ, 2021. – Т. 1 (63). – С. 90-95. – doi:https://doi.org/10.26906/SUNZ.2021.1.090.

5. Kuchuk, N., Kovalenko, A., Tkachov, V., Rosinskiy, D., & Kuchuk, H. (2021). Predicting traffic anomalies in container virtualization. Computer And Information Systems And Technologies.