УДК 004.91

П. Я. Бондаренко[1]
М. М. Підгорний[1]

ВИЗНАЧЕННЯ ЕФЕКТИВНОСТІ ДВОХ ПОПУЛЯРНИХ МЕТОДІВ ШИФРУВАННЯ

[1]Вінницький національний технічний університет

Анотація

Розглядається питання ефективності асиметричного та симетричного методів шифрування цифрових даних.

Ключові слова: *шифрування даних; асиметричний метод шифрування; симетричний метод шифрування; криптографічний метод.*

Abstract

The efficiency of asymmetric and symmetric methods of digital data encryption is considered.

Keywords: data encryption; asymmetric encryption method; symmetric encryption method; cryptographic method.

Вступ

На даний час стає актуальним пошук та використання більш швидких, безпечних та ресурсозаощаджуючих методів шифрування цифрових даних.

Сучасний рівень безпеки багатьох криптографічних методів базується на складності деяких обчислювальних проблем, таких як розклад цілих чисел, або проблеми з дискретними логарифмами. В багатьох випадках, існують докази безпечності криптографічних методів лише за умови неможливості ефективного розв'язання певної обчислювальної проблеми. За одним суттєвим винятком – схема одноразових блокнотів. Разом із пам'яттю про історію криптографії, розробники криптографічних алгоритмів та систем також мають брати до уваги майбутній поступ технологій в своїх розробках. Наприклад, постійне підвищення обчислювальної потужності комп'ютерів розширило поле для атак грубої сили. Тому, відповідно і оновлюються стандарти в сенсі вибору довжини ключа. Можливі наслідки розвитку квантових комп'ютерів вже враховуються деякими розробниками криптографічних систем; анонсована поява малих реалізацій цих комп'ютерів робить важливою попередню підготовку.

Ефективність методів шифрування

Алгоритм RSA складається з 4 етапів: генерації ключів, шифрування, розшифрування та розповсюдження ключів.

Асиметричне шифрування (англ. – asymmetric coding) – набір методів криптографічного шифрування, в яких використовують два ключі – таємний (приватний) і відкритий; жоден із ключів не може бути обчислений без іншого за прийнятий час.

Метод симетричного шифрування, як і випливає з назви, використовує один криптографічний ключ для шифрування і дешифрування даних. Використання одного ключа для обох операцій робить процес простим.

У симетричному шифруванні можна виділити деякі переваги:

велика пропускна здатність, завдяки спеціальному проектуванню;

ключі мають невеликий розмір;

дані шифри можна застосовувати як основу для будування різноманітних криптографічних механізмів, включаючи з випадковими генераторами чисел, обчислювально-ефективними схемами розпису та тому подібне.

Серед недоліків даного шифрування слід відзначити:

у кожній немаленькій мережі необхідно використовувати значну кількість ключів;

при зв'язку між декількома особами необхідно досить часто змінювати ключі;

коли існує зв'язок між двома особами ключ слід засекречувати на двох кінцях.

Симетричні алгоритми шифрування також можуть використовуватися не самостійно. У новітніх криптосистемах, застосовуються комбінації симетричних та асиметричних алгоритмів, з метою отримання переваг обох схем.

Порівняння двох методів:

Симетричне шифрування	Асиметричне шифрування
Один ключ використовується для шифрування і дешифрування даних.	Пара ключів використовується для шифрування і дешифрування. Ці ключі відомі як "відкритий ключ" і "закритий ключ".
Простий метод шифрування, так як використовується тільки один ключ.	У зв'язку з тим, що використовується пара ключів – процес складний.
Використовується для шифрування великих об'ємів даних.	Забезпечує аутентифікацію.
Забезпечує високу продуктивність і вимагає менше обчислювальної потужності.	Складні процеси протікають повільніше і вимагають більшої обчислювальної потужності.
Для шифрування даних використовується менша довжина ключа (128-256 біт).	Використовуються довші ключі шифрування (1024-4096 біт).
Ідеально підходить для шифрування великої кількості даних.	Використовується при шифруванні невеликого об'єму даних.
Стандартні алгоритми: RC4, AES, DES, 3DES і QUAD.	Стандартні алгоритми: RSA, Diffie-Hellman, ECC, El Gamal і DSA.

Висновки

З точки зору безпеки, асиметричне шифрування, безсумнівно, краще, оскільки воно забезпечує аутентифікацію. Однак продуктивність є аспектом, який не можно ігнорувати, тому симетричне шифрування завжди буде необхідно.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Windows API. URL: https://uk.wikipedia.org/wiki/Windows_API.

2. URL: https://vc.ru/hr/50161-pochemu-c-krut-aktualen-i-bessmerten.

3. Вибір платформи для додатків Windows URL: https://docs.microsoft.com/ru-ru/windows/apps/desktop/choose-your-platform.

4. Литвиненко Н.А. Технологія програмування на С ++. Win32 API-додатки. - СПб .: БХВ-Петербург, 2010. - 288 с .: іл. - (Навчальний посібник).

5. Рисований О.М. Системне програмування [Текст]: підручник для студентів напрямку "Компютерна інженерія" Вищих Навчальних Закладів в 2-х томах. Том 2. – Видання четверте: виправлено та доповнено - Х .: "Слово", 2015. - 378 с.

Бондаренко Павло Якович – викладач кафедри військової підготовки, Вінницький національний технічний університет, м. Вінниця, e-mail: pavlobondarenko1970@gmail.com

Підгорний Максим Максимович, слухач кафедри військової підготовки, навчальна група 06-21, Вінницький національний технічний університет, м. Вінниця, e-mail: maksonpatiphone@gmail.com

Bondarenko Pavlo – Lecturer of the Department of Military Training, Vinnytsia National Technical University, Vinntsia, e-mail: pavlobondarenko1970@gmail.com

Pidgorniy Maksim Maksimovich, student, Department of Military Training, study group 06-21, Vinnytsia National Technical University, Vinnytsia, e-mail: maksonpatiphone@gmail.com