ШИФРУВАННЯ ДАНИХ І НОВА МЕТОДИКА ОЦІНКИ КРИПТОГРАФІЧНИХ СИСТЕМ

МОСКАЛЕНКО ПАВЛО СЕРГІЙОВИЧ

- Криптографія – наука про математичні методи забезпечення конфіденційності, цілісності і автентичності інформації.
- Шифрування - перетворення даних, з метою приховання інформації.
- Ключ – інформація, яка використовується для шифрування і дешифрування повідомлення. Він відомий обмеженій кількості людей, або має відкритий доступ в залежності від поставлених задач.
- Метод підбору – метод розшифрування інформації за допомогою підстановки різних ключів.
- Симетричне шифрування - схема шифрування, у якій ключ шифрування, та ключ дешифрування збігаються, або один легко обчислюється з іншого та навпаки.
- Асиметричне шифрування - набір методів криптографічного шифрування, в яких використовують два ключі - таємний(приватний) і відкритий; жоден із ключів не може бути обчислений з іншого.
- Шифр Віженера - поліалфавітний шифр, який у якості ключа використовує слово.
- Шифр Вернама - система симетричного шифрування, в якому ключ є випадковим, збігається за розміром з заданим відкритим текстом та застосовується лише один раз.
- Алгоритм Диффі-Хелмана – алгоритм, що дозволяє двом сторонам отримати однаковий ключ, використовуючи незахищений від прослуховування, але захищений від підміни, канал зв'язку. Цей ключ використовується для шифрування даних за допомогою симетричного шифрування.

Актуальність доповіді полягає в потребі вирішення двох проблем:

- Використання Україною послуг шифрування даних, що розробляються в інших країнах;
- Закупівля технологій шифрування, опираючись на думку чужоземних експертів.

Нова методика оцінки ефективності криптографічних систем

- Простота використання
- Швидкість шифрування інформації
- Стійкість алгоритму до зовнішніх атак
- Ціна
- Кількість використаних математичних операцій
- Перспективність алгоритму

Оцінки різних видів шифрування:

- Шифр Віженера отримав оцінку 4;
- Шифр Вернама отримав оцінку 5;
- Алгоритм Діффі-Хеллмана отримав оцінку 7.

Висновок

Україна вже зараз може отримувати послуги шифрування інших країн з високою продуктивністю, використовуючи дану методику оцінки ефективності криптографічних систем

Дякую за увагу!