КРИПТОГРАФІЯ ТА НАЙПРОСТІШІ АЛГОРИТМИ ШИФРУВАННЯ ДАНИХ

Кузьмін Дмитро Юрійович, *СІ-32*
Науковий керівник: ***Литвиненко Ю.О.,*** *старший викладач*

Криптогра́фія (від грецького kryptós – прихований і gráphein – писати) – наука про математичні методи забезпечення конфіденційності (неможливості прочитання інформації стороннім) і автентичності (цілісності і справжності авторства) інформації. Розвинулась з практичної потреби передавати важливі відомості найнадійнішим чином. Для математичного аналізу криптографія використовує інструментарій абстрактної алгебри.

Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, що припускають використання обчислювальних засобів. Відомо більш десятка перевірених алгоритмів шифрування, які, при використанні ключа достатньої довжини і коректної реалізації алгоритму, роблять шифрований текст недоступним для криптоаналізу. Широко використовуються такі алгоритми шифрування як Twofish, IDEA, RC4 та ін.

У багатьох країнах прийняті національні стандарти шифрування. У 2001 році в США прийнятий стандарт симетричного шифрування AES на основі алгоритму Rijndael з довжиною ключа 128, 192 і 256 біт. Алгоритм AES прийшов на зміну колишньому алгоритмові DES, який тепер рекомендовано використовувати тільки в режимі Triple-DES (3DES).

Тривалий час під криптографією розумілось лише шифрування – процес перетворення звичайної інформації (відкритого тексту) в незрозуміле «сміття» (тобто, шифротекст). Дешифрування – це обернений процес відтворення інформації із шифротексту. Шифром називається пара алгоритмів шифрування/дешифрування. Дія шифру керується як алгоритмами, та, в кожному випадку, ключем. Ключ – це секретний параметр (в ідеалі, відомий лише двом сторонам) для окремого контексту під час передачі повідомлення. Ключі мають велику важливість, оскільки без змінних ключей алгоритми шифрування легко зламуються і непридатні для використання в більшості випадків. Історично склалось так, що шифри часто використовуються для шифрування та дешифрування, без виконання додаткових процедур, таких як аутенифікація або перевірка цілісності.

Дослідження характеристик мов, що мають будь-яке відношення до криптології, таких як частоти появи певних літер, комбінацій літер, загальні шаблони, тощо, називається криптолінгвістикою.

До нашого часу, криптографія займалася виключно забезпеченням конфіденційності повідомлень (тобто шифруванням) – перетворенням повідомлень із зрозумілої форми в незрозумілу і зворотнє відновлення на стороні одержувача, роблячи його неможливим для прочитання для того, хто перехопив або підслухав без секретного знання (а саме ключа, необхідного для дешифровки повідомлення). В останні десятиліття сфера застосування криптографії розширилася і включає не лише таємну передачу повідомлень, але і методи перевірки цілісності повідомлень, ідентифікування відправника/одержувача (аутентифікація), цифрові підписи, інтерактивні підтвердження, та технології безпечного спілкування, тощо.

Одним з найпростіших методів шифрування є шифрування зсувом. Суть методу полягає в тому що кожний символ тексту переміщується на певну кількість позицій, що робить його недоступним до перегляду. Саме кількість позицій на яку робиться зсув і є ключовим параметром в алгоритмі. Іншим важливим параметром для роботи алгоритму і програми в цілому є кількість символів у вхідному тексті, що міститься у вхідному текстовому файлі.

Алгоритм даної програми був реалізований на Borland Pascal 7.0, програма має декілька режимів роботи і її алгоритм схематично має такий вигляд.

1. На початку роботи програма пропонує ввести кількість символів тексту з яким вона буде працювати та вибрати режим роботи
2. Незалежно від обраного режиму програма відкриває вхідний та вихідний текстові файли.
3. Відбувається зчитування тексту із вхідного файлу та зсув кожного символу відповідно до обраного режиму роботи шифрування чи дешифрування тексту. При виборі режиму шифрування символ переміщується вправо на вказану кількість позицій при дешифруванні вліво.
4. Після завершення роботи програми у вихідному файлі маємо результат згідно з обраним режимом або зашифрований або розшифрований текст

На базі вище зазначеного алгоритму була створена програма під назвою «Навчальний тест». У своїй роботі ця програма використовує алгоритм шифрування зсувом. Питання до тесту зберігаються у блокноті з яким працює програма у зашифрованому вигляді, при створені форми користувача, програма зчитує питання з блокноту та розшифровує його, після чого відтворює користувачу у звичному для нас вигляді. Особисті данні які користувач вводить перед тим як перейти до тесту у програмі шифруються, як і самі результати тесту користувача, після шифрування дані виводяться у блокноти. Секретний параметр алгоритму, а саме зсув, відомий тільки керівнику проекту. Після завершення тестів керівник проекту може переглянути результати скориставшись тим же алгоритмом з введенням секретного параметру, тобто з введенням кількості позицій на яку був зроблений зсув (перенесення кожного

символу зашифрованого тексту).

Дуже перспективною сферою використання алгоритмів шифрування є локальна мережа. Провівши власні дослідження я дійшов до висновку, що у пірінгових локальних мережах важко щось сховати але і сховатися важко. До такого висновку мене привело вивчення структури локальних мереж: уся локальна мережа розбита на підмережі, у кожній під мережі є комутатор. Така структура локальної мережі призводить до того, що фактично кожний користувач може продивлятися та отримувати трафік усієї підмережі. Частіше всього цей трафік циркулює у незашифрованому відкритому вигляді, що може в свою чергу призвести до втрати або розповсюдженню конфіденційної інформації. Із вищесказаного бачимо, що локальна мережа дійсно є дуже перспективною сферою для масового впровадження та використання алгоритмів шифрування. Таке впровадження покращить інформаційну безпеку користувачів у локальному просторі, так як далеко не всі користувачі можуть забезпечити захист власної конфіденційної інформації у мережі.