Секція «ВИЩА МАТЕМАТИКА»
ШИФРУВАННЯ З ВІДКРИТИМ КЛЮЧЕМ

Автор: ст. гр. П–21 Набока Аліна Костянтинівна
Керівник: к.т.н., доц. Гаєвська В.О.

Довгий час традиційна криптографія використовувала шифрування з таємним або симетричним ключем — один і той же ключ використовувався як для зашифровування, так і для розшифровування даних. Проблема була в тому, що при зміні ключа (шифру) з метою безпеки, його необхідно було доставити одержувачу, який часто перебував далеко і на ворожій території. Передавати шифр відкритими каналами зв'язку було небезпечно. Проблема з ключами була вирішена тільки в 1975 році, коли Уітфілд Діффі та Мартін Хеллман запропонували концепцію шифрування з парою ключів: відкритим (public key), який зашифровує дані, і відповідним йому закритим (private key).

Асиметрична система шифрування отримала назву криптографії з відкритим ключем. Різні ключі використовуються для шифрування і дешифрування. Це властивість відрізняє цю схему від симетричної схеми шифрування. Головною ідеєю при створенні цього класу шифрів є генерація двох ключів. Один відкритий ключ поширюється по відкритих каналах зв’язку й використовується при шифруванні повідомлень. На прийомній стороні за допомогою секретного ключа проводиться розшифрування повідомлення. Основою при створенні таких шифрів, як сказано вище, є задачі з важким розв’язком. У якості таких задач у цей час використовуються задачі факторизації, дискретного логарифмування й методи теорії завадостійкого кодування.

Кожен одержувач володіє унікальним ключем дешифрування, що називається його особистим ключем. Одержувач повинен опублікувати ключ шифрування, що називається відкритим ключем. Як правило, в цій системі залучена довірена третя сторона, яка засвідчує, що певний відкритий ключ належить тільки конкретній людині або об'єкту.

Шифрування з відкритим ключем дозволяє здійснити подвійну перевірку відповідності цифрового ключа й особистості співрозмовника за допомогою так званої «перевірки відбитків». Найкраще таку перевірку здійснювати при

особистій зустрічі. Ваш співрозмовник порівняє кожен символ відбитка відкритого ключа, наданого вами, з відбитком вашого відкритого ключа, що знаходиться у співрозмовника. Якщо ж розкіш особистої зустрічі вам недоступна, ви можете відправити свій відбиток іншим безпечним каналом зв'язку, наприклад за допомогою месенджера, чату або HTTPS-сайту, який використовує наскрізне шифрування.

В цілому, працює система шифрування відкритим ключем так:

• Генерується випадковий секретний (приватний) ключ (це послідовність символів) і за певним алгоритмом підбирається до нього інший – відкритий (публічний) ключ. При цьому, для будь-якого закритого ключа існує тільки один варіант відкритого. Тобто ці ключі (приватний і публічний) завжди працюють в парі (зв'язці).

• Далі отриманий відкритий (публічний) ключ пересилається будь-яким відкритим каналам зв'язку відправнику таємного повідомлення.

• Отримавши відкритий (публічний) ключ, відправник за допомогою нього зашифровує повідомлення і відправляє його одержувачу у якого є відповідний закритий (приватний) ключ.

• Одержувач розшифровує секретне повідомлення, використовуючи свій закритий (приватний) ключ з пари з відкритим (публічним), яким було зашифровано повідомлення.

Слід зазначити, що відкритим (публічним) ключем можна тільки зашифрувати повідомлення, але розшифрувати його вже цим ключем не вийде. Хоча закритий і відкритий ключі пов'язані математично, обчислити закритий ключ з відкритого ключа не представляється можливим. Фактично, інтелектуальна частина будь-якої криптосистеми з відкритим ключем полягає в розробці відносин між двома ключами.