ШИФРУВАННЯ З ВІДКРИТИМ КОДОМ. АЛГОРИТМ RSA

Таранова Д.В., *студентка*; СумДУ, гр. ФЕ-41

Симетричні криптосистеми характеризуються тим, що ключі для шифрування та дешифрування інформації збігаються або ж один можна обчислити при наявності іншого. Головна проблема таких систем – розподіл ключів: одна сторона має створити ключ і секретно передати іншій. Це особливо складно в наш час, коли кількість користувачів криптосистеми може сягати тисяч. Асиметричні системи працюють інакше: для шифрування даних використовується один ключ(відкритий), для розшифрування – інший(секретний). Основна перевага асиметричних криптосистем перед симетричними – не потрібно передавати секретний ключ по захищеному каналу.

Такі алгоритми шифрування використовують необоротні(односторонні) функції, тобто такі, в яких при заданому значенні x досить просто визначити $f(x)$, але знаючи $y=f(x)$ неможливо визначити x. Причому під неможливістю в даному випадку розуміють не теоретичну неможливість, а практичну складність здійснення цієї операції за потрібний інтервал часу.

У своїй роботі я розглянула загальні принципи побудови криптосистеми з відкритим ключем, те, які алгоритми зараз використовуються, та детально вивчила метод RSA, заснований на розкладі великих чисел на прості множники. Розібраний його алгоритм створення відкритих та секретних ключів, те, як проходить шифрування та дешифрування у системі RSA.

Алгоритм RSA використовується в багатьох криптосистемах для захисту програмного забезпечення та в якості електронного підпису. Але через те, що цей алгоритм вимагає великої потужності процесорів та витраченого часу, його частіше застосовують у гібридних криптосистемах, де з його допомогою шифрують лише ключ, а самі повідомлення – симетричним методом.

Асиметричні криптосистеми, зокрема RSA, мають ряд переваг перед симетричними. Такі алгоритми широко застосовують у сучасних програмах.

Керівник: Захарченко Н.М., старший викладач кафедри математичного аналізу і методів оптимізації