МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАТИКА, МАТЕМАТИКА, АВТОМАТИКА

IMA :: 2017

МАТЕРІАЛИ
та програма

НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

(Суми, 17–21 квітня 2017 року)

Суми
Сумський державний університет
2017

Програмна реалізація алгоритму шифрування RSA

Романюк О.О.*студент*; Смаглюк М.П. *студент*.
Індустріально-педагогічний технікум КІСумДУ, м. Конотоп

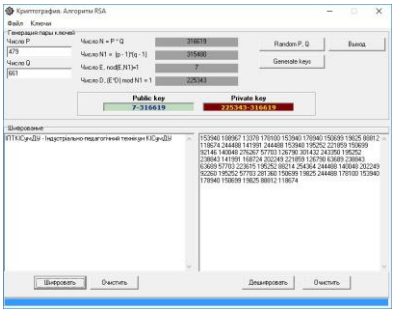
В залежності від структури використовуваних ключів методи шифрування поділяються на:

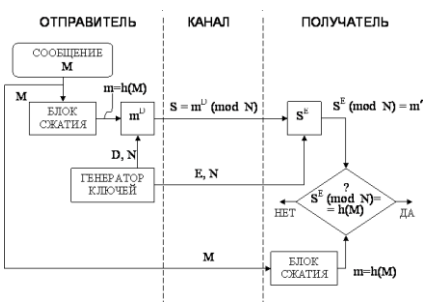
- симетричне шифрування: стороннім особам може бути відомий алгоритм шифрування, але невідома невелика порція секретної інформації – ключа, однакового для відправника і одержувача повідомлення.

- асиметричне шифрування: стороннім особам може бути відомий алгоритм шифрування, і можливо відкритий ключ, але невідомий закритий ключ відомий тільки одержувачу.

Криптографічні системи з відкритим ключем в даний час широко застосовуються в різних мережевих протоколах. Асиметричне шифрування на основі відкритого ключа RSA (розшифровується, як Rivest, Shamir and Aldeman - творці алгоритму) використовує більшість продуктів на ринку інформаційної безпеки. Його криптостійкість ґрунтується на складності розкладання великих чисел на множники.

Алгоритм шифрування RSA був реалізований з допомогою інтегрованого пакета фірми Borland Delphi 7.0.





(а) (б)

Рисунок 1 – Програмна реалізація алгоритму RSA.
(а) Головна формиа прогами, (б) Узагальнена схема формування й перевірки цифрового підпису.

Керівник: Білоус С.О., *викладач*.