Магістерська кваліфікаційна робота на тему:

“Розробка програмного забезпечення для створення захищеного каналу передачі даних”

Науковий керівник роботи:, к.т.н., доцент Паламарчук Є. А.

Виконав студент гр. 1ПЗ-15м(сп) Харін В.О.

Мета і задачі роботи

Метою роботи є підвищення захисту передачі даних в комп'ютерних мережах за рахунок використання додаткового шифрування.

У відповідності до поставленої мети в роботі вирішуються такі завдання:

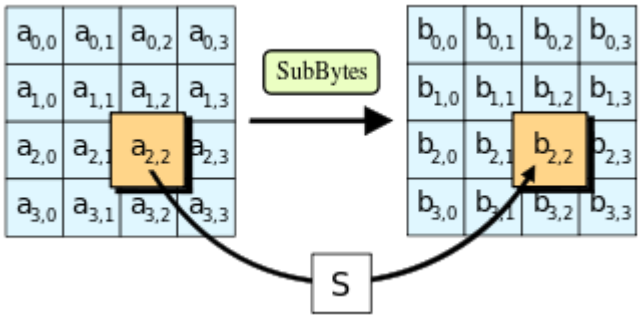
- техніко-економічне обгрунтування доцільності розробки програмного забезпечення;
- вибір програмних засобів для вирішення поставлених завдань;
- розробка алгоритмів та програмних модулів;
- розробка графічного інтерфейсу та тестування програмного продукту;

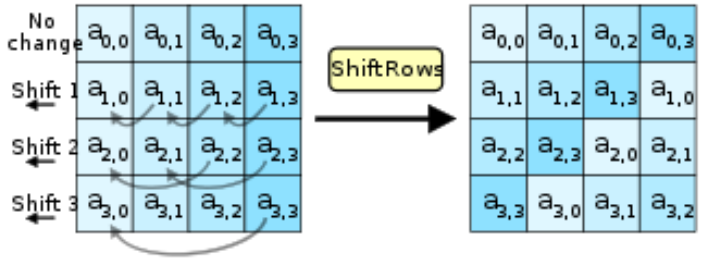
Переваги додатку

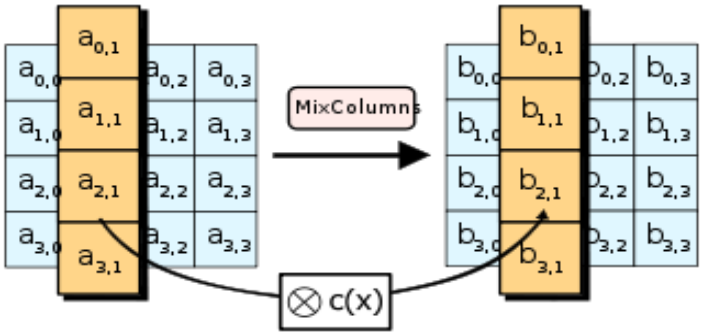
Комбіноване використання систем шифрування :

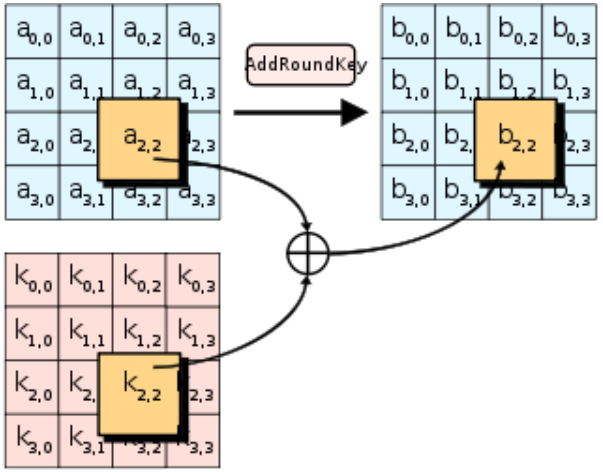
- Використання AES в шифруванні трафіку
- Використання SSL в шифруванні трафіку
- Використання шифру Вернама в шифруванні трафіку
- Використання додаткового каналу для передачі AES-ключа

Основні операції при шифруванні даних за допомогою AES

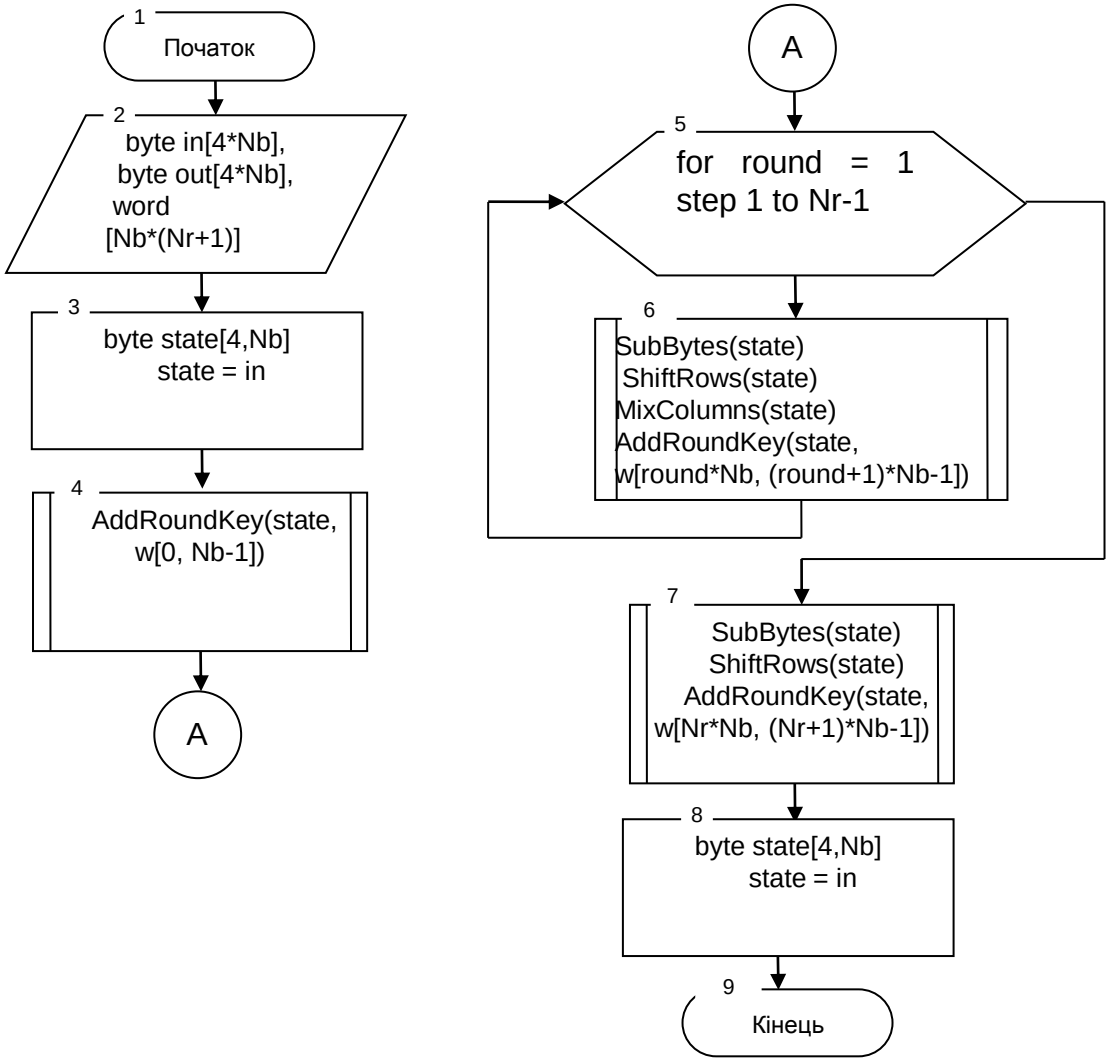




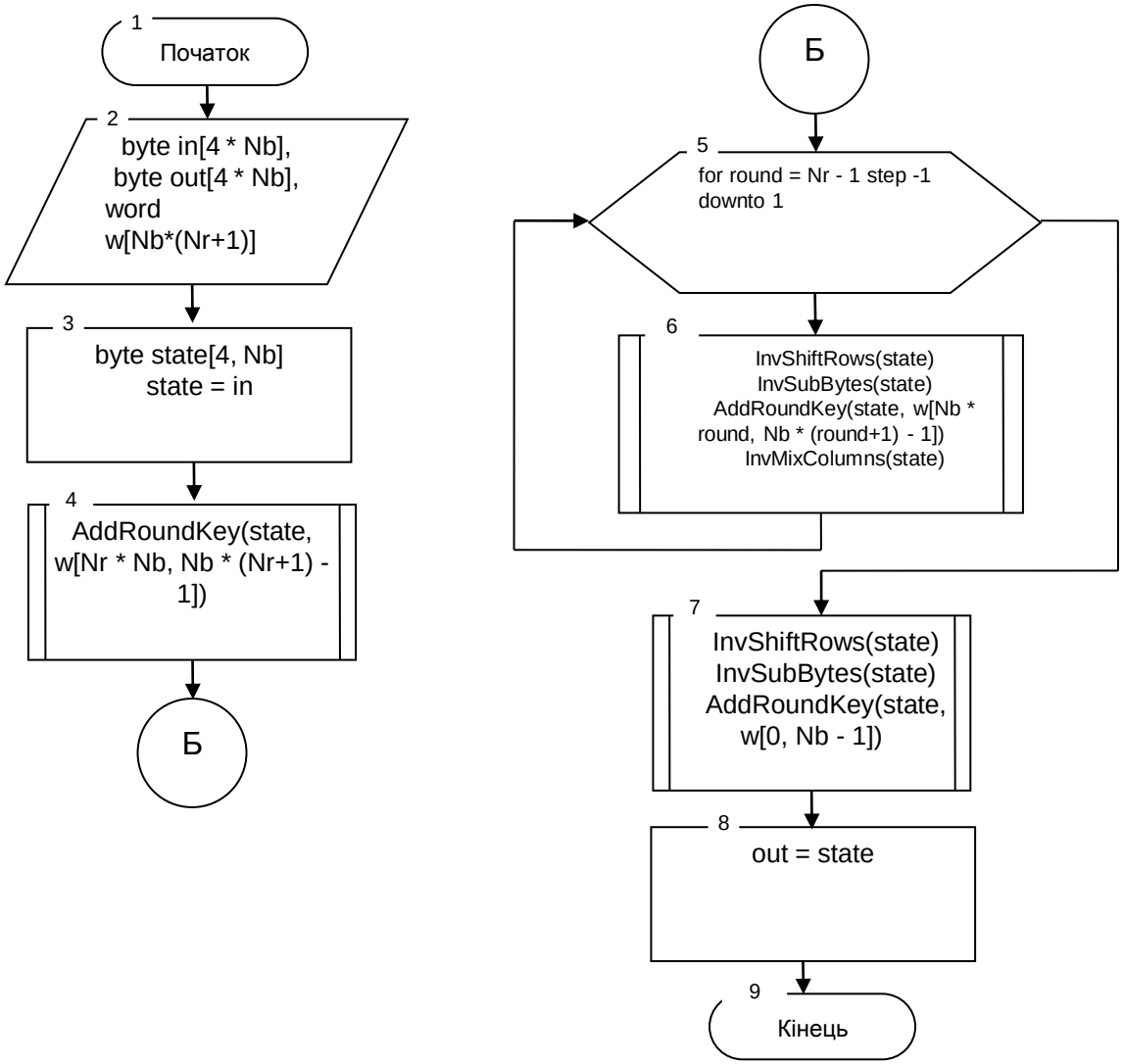




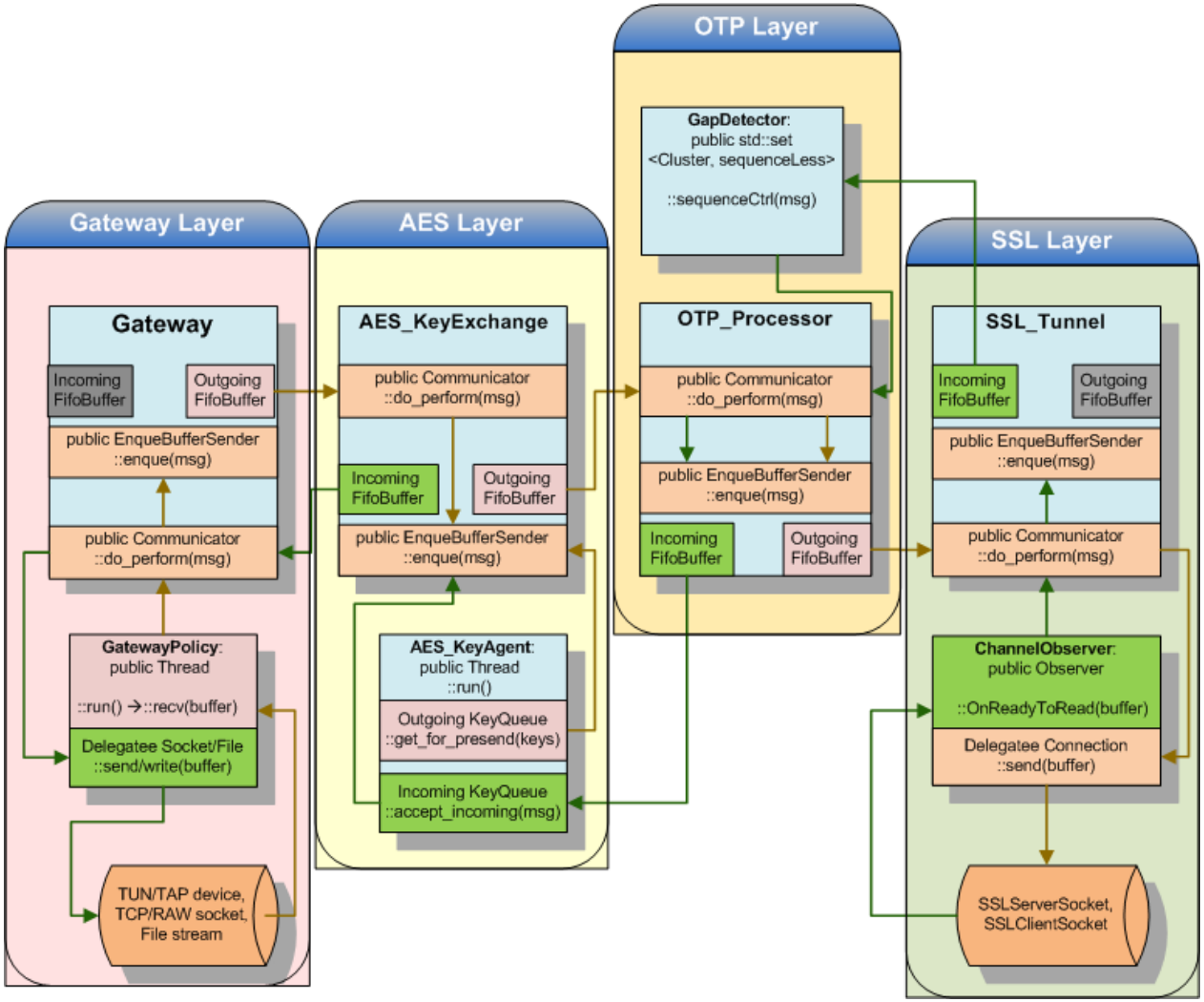
Граф-схема алгоритму шифрування AES



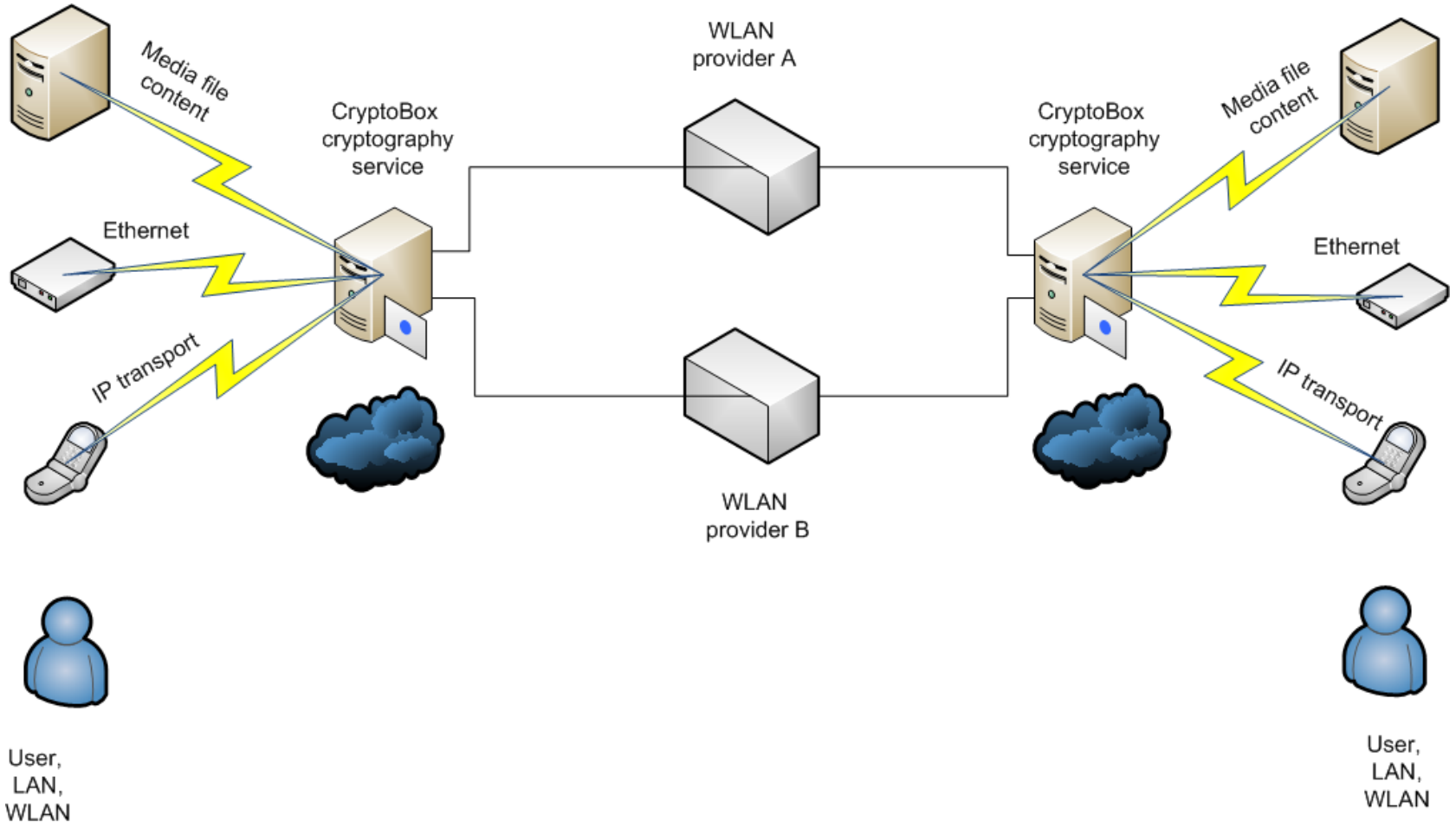
Граф-схема алгоритму дешифрування AES



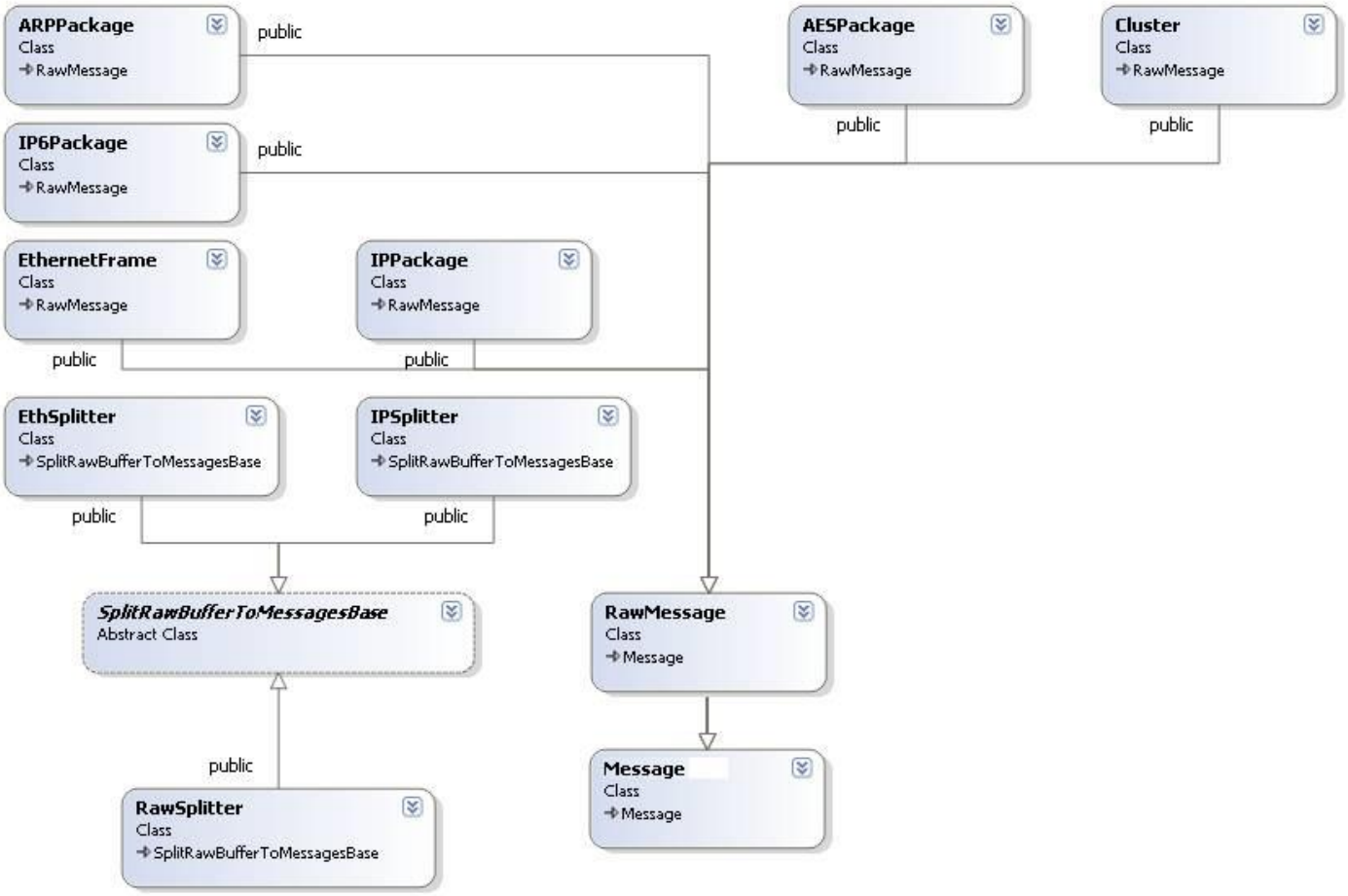
Архітектура програмного забезпечення



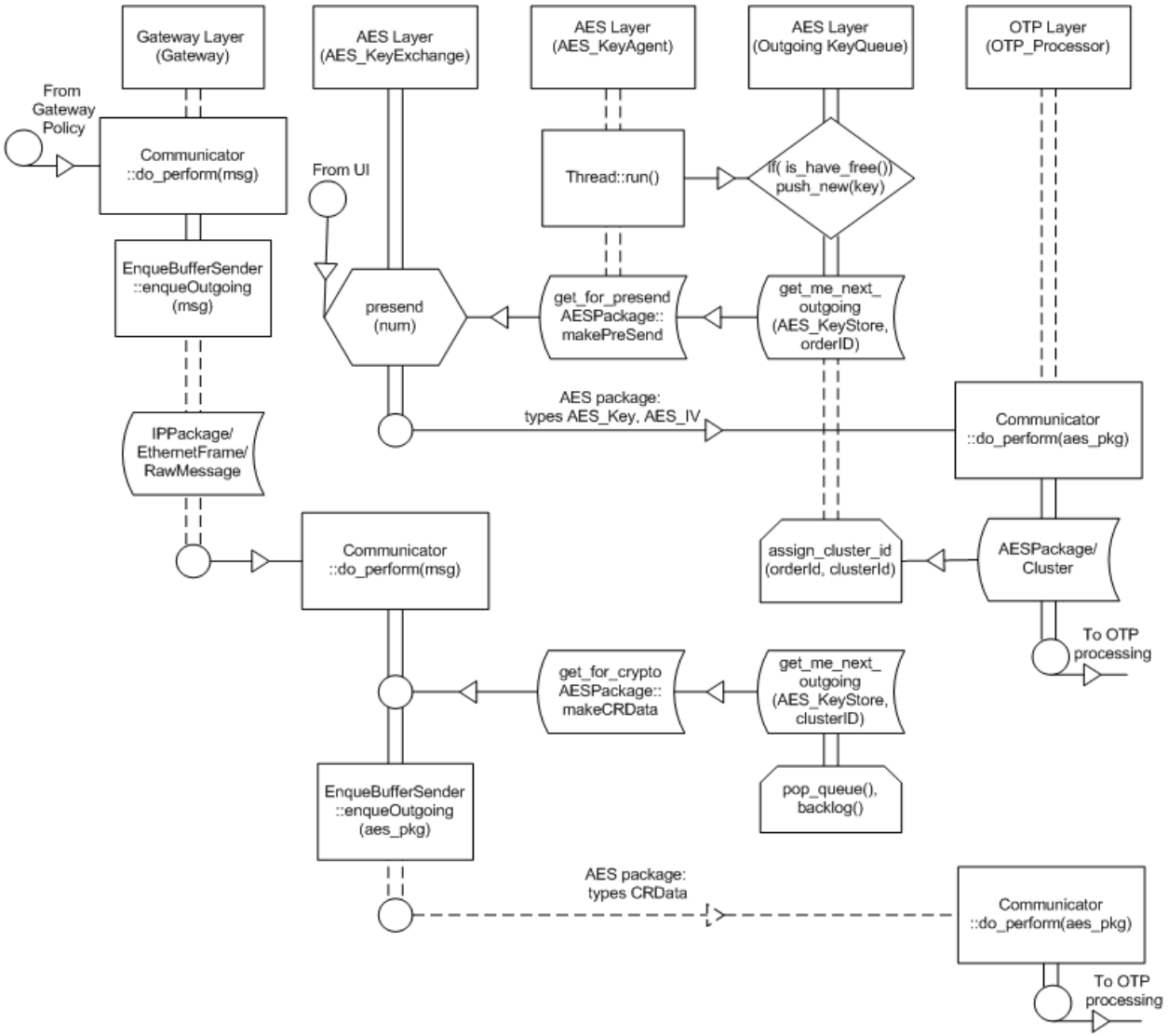
Апаратна платформа



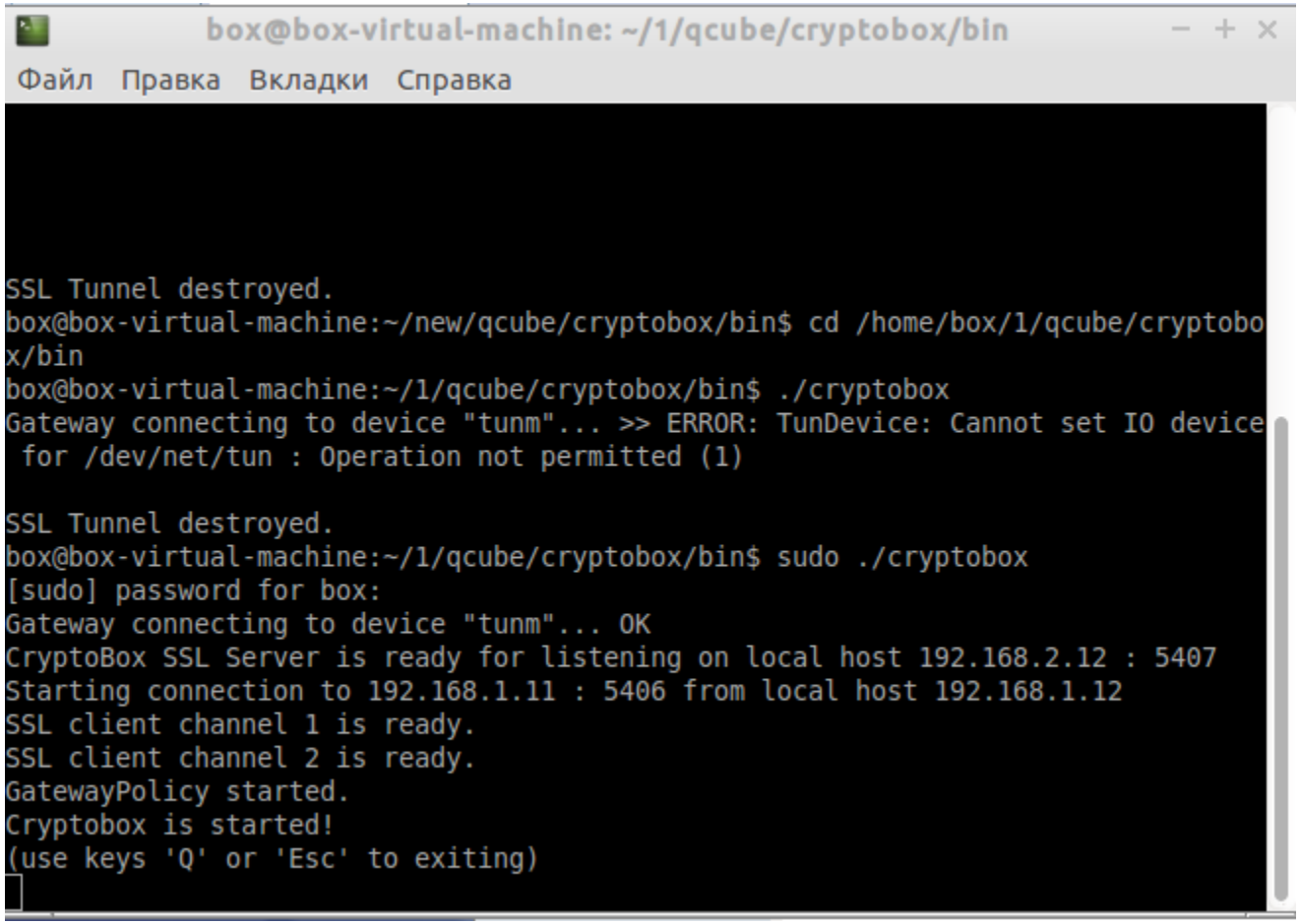
Діаграма класів



Діаграмма станів



Графічний інтерфейс програмного продукту



Висновки

Наукова новизна роботи полягає в шифруванні мережевого трафіку за допомогою AES, шифру Вернама та SSL і використанні додаткового каналу для передачі AES-ключа.

В процесі розробки програмного забезпечення для створення захищеного каналу для передачі даних та оформлення дипломної роботи на практиці були закріплені теоретичні знання, вдосконалено навички програмування мовою C++ та навички оформлення технічної документації з використанням текстових та графічних редакторів.

Дякую за увагу!