УДК 681.3.07

АНАЛІЗ КРИПТОСИСТЕМИ RSA НА МОВІ Java

Кичак В. В.
Науковий керівник - к.т.н, доц. Гикавий В. А.

Метою даної праці є розробка та аналіз швидкодії криптосистеми RSA при його реалізації на мові програмування Java. RSA протокол відноситься до несиметричної криптографії, де для обміну повідомленнями використовуються два ключі: відкритий і закритий. При симетричній криптографії кожна з сторін що обмінюється повідомленнями повинна мати копію загального ключа, що створює складну проблему керування ключами.

Проведено аналіз макету криптосистеми RSA, розробленої на мові програмування JAVA. Програма складається з 3 діалогових вікон, які у свою чергу працюють за допомогою 5 класів (підпрограм): основи (RSAMainFrame), генератора ключів (RSAkeyGen), шифратора (RSAEncrypt), дешифратора (RSADecrypt) та класу захисту (RSASecurity).

На панелі вікна «Генерація ключів» знаходиться панель динамічного вибору розміру відкритого ключа, яка у свою чергу підвищує захищеність системи. На кожний символ, з якого складається ключ, припадає 8 бітова комірка, в яку вноситься значення друкованих і не друкованих символів від 1 до 256. У вікні шифрування обирається файл для криптуваня, попередньо отриманий відкритий ключ та вихідний крипто-файл. У вікні дешифрування обирається файл закритого ключа, криптований файл з інформацією та декриптований файл. Для коректної подальшої роботи з файлом його потрібно перейменувати, з зазначенням попереднього розширення (.doc, .bmp, .xml,…).

Дана програма розроблена на базі Java, що ні чим особливо не відрізняється від C++, але характеризується родом переваг при використанні. . Перевагою Java є повна незалежность байт-кода від операційної системи і устаткування дозволяє виконувати Java - програми на будь-якому пристрої, для якого існує відповідна JVM. Іншою важливою особливістю технології Java є гнучка система безпеки завдяки тому, що виконання програми повністю контролюється віртуальною машиною. Результати аналізу швидкодії криптосистеми RSA представлені у таблиці.

Таблиця – Швидкість роботи криптосистеми RSA на мові Java

Тип файлу	Розмір файлу (байт)	Розмір відкритого ключа (байт)	Час шифрування (с)	Розмір шифрованого файлу (байт)	Час розшифрування (с)
ZIP	656 193	64	4,42	666 688	43,31
		96	4,77	663 668	1хв. 32,96
		128	5,21	661 204	2хв. 21,35
		160	5,48	659 242	3хв. 38,87
		192	5,74	659 804	4хв. 55,82
		224	6,55	660 426	6хв. 44,15
		256	7,36	659 200	8хв. 34,24