ПЕРЕДАЧА ДАНИХ В МОДЕЛІ ГРИ ІЗ ЗАХИСТОМ ДАНИХ

ст. викл. В.М. Гугнін, студ. Д.В. Халій, Національний технічний університет "Харківський політехнічний інститут", м. Харків

В даному проекті розглянуто питання захисту даних при передачі їх через мережу інтернет в простій моделі мережної гри, та розробка такої моделі, яка реалізує зазначені можливості.

У комп'ютерних іграх для шифрування даних як на самих комп'ютерах / пристроях, так і при їх передачі через мережу інтернет використовується безліч різноманітних способів, при цьому в основному відразу декілька з них. У сучасний час при передачі даних по інтернету простих засобів шифрування недостатньо для захисту цих даних, а їх відсутність – категорично не рекомендується, особливо якщо йдеться про внутрішньоігрові покупки за реальні гроші. Тому при розробці будь-яких подібних ігор захист переданих даних є досить категоричним питанням. Також треба враховувати, щоб процес шифрування / дешифрування даних не сильно уповільнював роботу самої програми, оскільки ця робота проходить в режимі онлайн (реального часу).

Хоча передача даних по мережі інтернет є дуже зручним способом передачі даних на відстані, не використовуючи фізичних носіїв, вона всеж-таки є не легкою задачею, оскільки треба враховувати багато проблем при з'єднанні до іншого комп'ютера / сервера, контролювати моменти роз'єднання. Але більш всього потрібно враховувати, що при передачі дані можуть бути перехоплені іншою третьою особою і або використані в своїх цілях, або ж змінені будь-яким зручним і/або корисливим способом, тому створення захищених каналів передачі даних є одним з основних завдань при реалізації.

У даному проекті при передачі даних через мережу інтернет для їх захисту використовується:

– алгоритм RSA з асиметричним ключем, причому ключі при кожній передачі даних будуть змінюватися на одній і іншій стороні передачі. Це дасть те, що навіть у разі перехоплення даних третя особа не зможе швидко підібрати закритий ключ і розшифрувати ці дані. Самий же ключ до цього моменту може стати вже не актуальний, бо буде використовуватися новий.

– хешування переданих даних. Це дасть те, що навіть у разі перехоплення, як даних, так і відкритого ключа будь-кого з сторін, третя особа не зможе непомітно для кінцевого вузла змінити дані і передати їх йому при передачі.