УДК: 004.056.55(003.26)

А.О. Капуста
Національний авіаційний університет, Київ

ЕВОЛЮЦІЯ АЛГОРИТМІВ ШИФРУВАННЯ RC

Алгоритми RC широко використовуються в багатьох мережевих додатках через їх сприятливі можливості швидкості та мінливої довжини ключів. В основному було розроблено шість алгоритмів RC, з яких використовують лише чотири. Незважаючи на подібність у своїх назвах, алгоритми здебільшого не пов'язані між собою.

RC1 так і не був опублікований, це був перший крок, який зробив Рівест для того, щоб продовжити з розробленням серії симетричних ключових алгоритмів, широко відомих як Rivest Cipher Algorithm. Основна ідея дослідження полягала в розробці алгоритму шифрування симетричного ключа, який би користувачі використовували для захисту своїх даних під час проходження через мережу.

RC2 - алгоритм блочного шифрування розроблений у 1987 році, розглядався як пропозиція щодо заміни DES. Шифрує дані блоками по 64 біта з використанням ключів змінного розміру: від 8 до 1024 бітів включно (рекомендованим розміром ключа є 64 біта). . Алгоритм розроблений для легкої реалізації 16-бітних мікропроцесорів. Якщо шифрування ключів було виконано заздалегідь, то цей алгоритм працює вдвічі швидше, ніж DES на IBM AT. Сам алгоритм включає 3 подальших алгоритми, а саме: розширення ключа, шифрування та розшифрування.

Алгоритм ***RC3*** не використовували, тому що він був пошкоджений під час його розробки для захисту RSA.

RC4 - це потоковий шифр з змінним розміром ключа, розроблений в 1987 році. Один і той же алгоритм використовується як для шифрування, так і для дешифрування. Потік даних виконує операцію XOR за допомогою серії згенерованих ключів. Змінна довжина ключа від 1 до 256 біт і використовується для ініціалізації 256-бітної таблиці стану. Він популярний завдяки своїй простоті. Шифр працює дуже швидко в програмному забезпеченні. Він вважався безпечним, поки він не став вразливим до BEAST атак.

RC5 розроблений в 1994 році як змінний на всіх фронтах. Розміри блоків можуть варіюватися від 32, 64 або 128 біт, а розміри ключів від 0-2040 біт і раундів від 0-255. Оригінальною пропозицією щодо параметрів був 64-бітний блок, 128-бітний ключ та 12 раундів. Він підходить для апаратного або програмного забезпечення. Це швидко, а також забезпечує безпеку, якщо обрані відповідні параметри.

RC6 був розроблений у 1997 році. Це блоковий шифр, який використовує 128-бітний розмір блоку і підтримує ключі розміром 128, 192 та 256 біт. Він був розроблений з метою задоволення вимог AES. Це вдосконалений алгоритм RC5. Забезпечує ще кращу безпеку від атак, які можуть бути можливими в алгоритмі RC5. Він використовує 4 регістри (кожен 32-х бітний) і є більш безпечним, ніж RC5. Він також захищений від різних інших можливих атак безпеки. Він використовує менше раундів і пропонує більш високу пропускну здатність.

Отже, запропоновано багато алгоритмів криптографії симетричного ключа. Алгоритми The Rivest Cipher - один із них. У цій роботі проведено огляд еволюції алгоритмів Rivest Cipher. Алгоритм RC6 хоч і не я є вразливим до будь-якої практичної атаки, але деякі теоретичні атаки все ще існують. У наш час, оскільки обчислювальна потужність зростає, RC6 може бути зламаним за кілька років. Таким чином, виникає потреба у більш сильному алгоритмі. Тому алгоритм повинен бути вдосконалений, щоб зробити його захищеним від атак.

ВИКОРИСТАНІ ДЖЕРЕЛА

1) https://en.wikipedia.org/wiki/RC_algorithm
2) https://www.globalsign.com/en/blog/glossary-of-cryptographic-algorithms
3) https://www.ripublication.com/irph/ijict_spl/ijictv4n17spl_13.pdf
4) http://crypto.pp.ua/2010/12/algoritm-rc2/
5) https://www.geeksforgeeks.org/rc4-encryption-algorithm/
6) http://solutionmes.wikidot.com/crypto-rc4