Міністерство освіти і науки України
Сумський державний університет
Наукове товариство студентів, аспірантів,
докторантів і молодих вчених СумДУ

ПЕРШИЙ КРОК У НАУКУ

Матеріали
IX студентської конференції
(Суми, 25 лютого 2018 року)

Суми
Сумський державний університет
2018

ДОСЛІДЖЕННЯ АЛГОРИТМУ ДІФФІ-ХЕЛЛМАНА

Почкун А.В., *студентка*; МКСумДУ, гр. 410-і

Напевно, в кожної людини є хоча б один секрет. До поняття секрету можна віднести багато чого: від коду запуску ядерних ракет до мобільного номеру телефону. Основною задачею є безпечно зберігати та передавати важливу інформацію. В багатьох випадках цю задачу добре вирішує алгоритм Діффі - Хеллмана. Мета моєї роботи - перевірити це твердження, тобто розібратися в можливих варіантах зламу цього алгоритму, а також виділити його переваги та недоліки.

Перш за все, важливо визначити, що сам по собі алгоритм захищає не інформацію, а ключ, який використовується для її шифрування. Якщо в інших симетричних криптографічних системах використовують один ключ, що був не надійно захищеним, то виникло питання генерації секретного ключа з стійкою системою захисту. Тому було створено алгоритм Діффі-Хеллмана, що полягає в забезпеченні конфіденційності ключа між відправником та отримувачем.

В сучасних технологіях алгоритм інтерпретується через логарифмічну функцію. Важкість зламу полягає в складності проблеми дискретного логарифмування. Нехай аргумент і основа модуля функції передані без приховування, тобто публічно. Далі відправник і отримувач обирають власний степінь, а результат обчислення передають іншій стороні. Після отримання необхідно використати це значення як аргумент функції з тим самим степенем і основою модуля, що використовувались в попередньому обчисленні. Таким чином кожна зі сторін отримує одне і теж число, а той, хто перехоплює не може його дізнатись тому що потрібно мати степінь від однієї сторони і результат обчислення від другої, або навпаки.

Безперечно, такий спосіб може мати безліч реалізацій і це є ще однією причиною його популярності у розробників програмного забезпечення. Але вже зараз з'явились теорії щодо його зламу. Хоча, навіть якщо буде знайдено відповідний алгоритм, на це потрібно буде витратити роки.

Керівники**:** Ананченко Ю.М., *викладач*
Ровна А.В.,*викладач*