УДК 621.396

Т.Б. Любарська
Волинський державний університет ім. Лесі Українки,
кафедра прикладної математики

ЗАСТОСУВАННЯ РОЗПІЗНАВАННЯ СЛІВ В КРИПТОГРАФІЇ

© Любарська Т.Б., 2002

Розглядаються використання зашумлення та розпізнавання слів у криптографії.

In given article consider using fortuitous distortion and recognition of word in cryptography.

На сьогодні досить актуальними є питання комп'ютерної безпеки. Інформація, яка викликає інтерес певних органів, організацій, може зацікавити і протилежну сторону - конкурентів чи інших осіб без санкціонованого доступу до неї. Саме ця противага викликає бурхливий розвиток криптографії та криптоаналізу. З одного боку необхідно забезпечити "абсолютно" надійний алгоритм шифрування інформації, а з іншого - знайти оптимальний метод розшифрування без наявності пароля (ключа)[1].

Оскільки будь-який алгоритм шифрування з часом стає відомим, до нього підбирають методи аналізу, використовуючи можливі недоробки в системах шифрування. Тобто є небезпека, що шифрограму прочитають рано чи пізно. Звісно, можна як завгодно ускладнювати алгоритм шифрування, але якщо він відомий, то завжди є ризик злому [2, 3].

Метод перебору оснований на відборі смислової інформації з-поміж набору символів. Таким чином, підбирається правильний ключ. Але якщо при застосуванні будь-якого пароля (правильного чи ні) результат отримується однакової зрозумілості, то відібрати, де помилковий ключ, а де правильний стає неможливо. А, отже, алоритм стає непідвладний криптоаналізу в зв'язку з невизначеністю правильності результату. І при цьому можна використати навіть найпростіший метод перестановок чи заміни. Текст все одно складно буде розшифрувати.

Саме на такій ідеї базується розробка нового алгоритму шифрування. Початковий текст піддається переробці так, щоб він міг бути розпізнаним при дешифруванні. При цьому допускаються морфологічні помилки. Основне - збереження змісту повідомлення. Людина може керувати спрощенням початкового повідомлення.

Наступним кроком буде створення шумового ефекту. Він випадково змінює початковий текст. Тобто одне і те саме повідомлення з одним і тим самим ключем буде мати зовсім різні варіанти криптотексту. Може змінюватися як довжина повідомлення, так і частота використовуваних букв (що утруднює криптоаналіз, оскільки може бути використана імітація вибраного методу шифрування).

Потім застосовується один з алгоритмів шифрування з використанням ключа. Отриманий результат є достатньо надійним з врахуванням вищенаведених доказів.

При розшифруванні тексту дії здійснюються в протилежному порядку. Застосовується відомий алгоритм з ключем. При цьому отримується незрозумілий набір символів, що при

"кюаиютюхийт алюкюъуюкюя ьнлвнщж чнщнлцнюэ чпшрю нлниф яупэды фэснухэуы еуун ыйхтлуйъьи йыслуйчйш пхйлрк пнзпгеж птеч ггенгп нщгх Р етсржж йпесьи сеупеъжзпж зпеюозр кюаиюкваф кюапюндаиюкж ипкнпьух дчннз"

Єдине, що є спільним в цих шифрограмах - це кількість слів і букв в кожному слові. За необхідності, можна було б зменшити розмір результуючого файла і збільшити криптостійкість. Але розглянемо дешифрування такого простого алгоритму. Припустимо, ми передаємо перший з отриманих текстів. Спробуємо підібрати пароль.

"ключ" – результат:
"длительного вычислением будущее расширены сумма акции глубже превышает хаос алгоритмов ближайшем божьей атакует знаю видеть годы е нельзя выпуск отказаться вкладов разбивает вырабатывает горлышко будем "

"секрет" – результат:
"двухэтажным безнадежную азартно восседали лучше буквы дающих актуально вниз сообщество денежныч божьей игрушку куча бармен годы ^ зданий важных вызванного азартно ближайшем криптосистем аналогов багаж"

Розшифруємо текст. До будь-якого зашифрованого тексту можна застосувати наш правильний пароль і отримати такий результат:

"путишествие закончилось причале приводить толпы людей самого странного вида рассыльные городских отелей мужчины всех цветов кожи m черные желтые коричневые красные наперебой предлагавшие поднести багаж".

На закінчення хотілося б сказати, що при наведенні прикладів застосовувалися самі слабкі алгоритми шифрування тексту. Тобто практично не намагалися захиститися від злому. Крім того, робочий словник мав розмір 16 кб, що для повноцінного "розуміння" недостатньо. Робочий алфавіт складався з 33 символів. Використовувався алгоритм Вижинера з ключем в 5 символів. Загалом, за потреби систему можна ускладнювати до бажаної міри, але результат можна бачити і при наведених вище умовах.

При користуванні цією системою потрібно знати:
- словник (якщо він особистий);
- ключ;
- метод шифрування (при криптоаналізі).

1. Жельников В. Криптоанализ от папируса до компьютера. - М., 1996. - 336 с. 2. Донарев В.В. Защита информации и безопасность компьютерных систем. - К., 1999. – 480 с. 3. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. - М., 2000. - 448 с.