ІНФОРМАЦІЙНА БЕЗПЕКА: КРИПТОГРАФІЯ

Тузовська М., студ. (гр. ФІ-52, ФТІ КПІ ім. Ігоря Сікорського)

Така вже людська природа – що один зберігає в таємниці, то інший завжди хоче розкрити. На цьому не хитрому прагненні і виросла дисципліна – криптологія, яку ділять на дві основні верстви: криптографія і криптоаналіз. Перша – займається розробкою методів шифрування даних, у той час як друга – криптоаналіз займається оцінкою сильних і слабких сторін методів шифрування, а також розробкою методів, які дозволяють зламувати криптосистеми.

Тексти шифрували монахи і закохані, полководці і бізнесмени. Таємні листи розкривали служби безпеки і батьки сімейств, контррозвідники і нудьгуючі інтелігенти. Не варто думати, що криптологія – це щось далеке і позамежне. Будь-якій сучасній людині життєво необхідно знати, як поводитися з шифрами, щоб «тримати свої секрети в секреті».

Ніхто не може сказати точно, коли ж був придуманий найперший шифр у світі. Усім відомо, що це було задовго до Різдва Христового. Швидше за все, відразу після появи писемності [1].

Якщо вірити дослідникам єгипетських пірамід, то під час розкопок були виявлені склепи з дуже дивними написами. Там одні ієрогліфи замінювалися на інші. Робилося це не стільки заради збереження таємниці, скільки для додання текстам більшої важливості. Приклади кодувань можна знайти і в Біблії – так, цар Вавилона за рахунок перестановки алфавіту навпаки (перша буква стала останньою, друга – передостанньою і т.п.) перетворювався на царя «Сессах» [2]. Такий метод перестановки символів називається атбаш. У тій же книзі згадується і нагорода «першого криптоаналітика» – пророка Даниїла за прочитання загадкового напису і проголосили третім володарем царства.

Зрозуміло, що шифри тих часів були примітивні. Замінялися букви, фрази, поняття, так що повідомлення або легко піддавалися дешифрування навіть без знання ключа, або не читалися взагалі.

Сьогодні криптографія в основному вивчає однозначні і механічні (автоматичні) шифри, які мають на увазі жорсткий алгоритм отримання як захищеного, так і відкритого тексту. Найпростіший з подібних алгоритмів - так званий спосіб Цезаря, в якому всі символи вихідного алфавіту замінюються знаками шифрованої абетки зі «зміщенням» на певне значення. Якщо воно дорівнює, наприклад, 3, то замість букви Ю буде Б, замість А - В, замість С - Ф і так далі.

Таких перестановок може бути декілька – наприклад, для першої літери використовується один варіант, для другої – вже наступний, для третьої – ще один. В цьому випадку шифр називається полі-алфавітний. Для розшифровки знадобиться всього-на-всього знати всі значення зсувів. Їх, до речі, можна передавати за допомогою не тільки цифр, але і ключових слів. Яскравим прикладом такого шифру є шифр віженера.

Звичайно ж, «стародавні» шифри розгадати не складно. Щоб дізнатися вихідний текст, застосовуються найрізноманітніші методи, в основному – статистичні. Один з таких алгоритмів – частотний аналіз появи букв. Саме таким методом скористався знаменитий детектив Шерлок Холмс в оповіданні «Танцюючі чоловічки». Коли йому вдалося отримати досить довгий текст, він визначив, з якою частотою повторюються ті чи інші символи. Якщо який-небудь символ повторюється через певні проміжки, то, швидше за все, цей знак позначає «пробіл». Наприклад, Холмс зрозумів, що прапорці в руках чоловічків вживаються лише для того, щоб відзначати кінці окремих слів. Букв в алфавіті багато, і розподіл їх досить традиційно для будь-яких текстів. Досвідчений криптоаналитик може і зовсім вгадати одне із значущих слів. Відомий сищик досить швидко розгадав шифрування послання, оскільки зробив ряд вірних припущень. Так, дві записки починалися зі слова з чотирьох букв, і Холмс здогадався, що це – ім'я дівчини, до якої було звернуто послання. Подальша розшифровка була справою техніки. Так що не варто покладатися на такі коди – вони досить добре вивчені і не раз були описані в художній літературі.

Існує безліч варіантів оцінки стійкості алгоритмів. Але, я не буду наводити складні математичні формули, а обмежуся деякими загальними міркуваннями.

Перш за все необхідно, щоб зашифрований текст був зовсім не схожий на вихідний – структурою, кількістю символів і іншими ознаками. Думаю, це вимога цілком зрозуміла – якщо гіпотетичний зловмисник раптом дізнається, скільки слів в листі, їх довжину і розподіл за частинами мови, то це сильно полегшить розшифровку.

Для надійного шифрування необхідно, щоб при мінімальній зміні початкового тексту або пароля фінальний текст змінювався практично до невпізнання [3]. Щоб зрозуміти, навіщо це потрібно, – приведу приклад: якщо хтось розсилає кілька повідомлень з мінімально зміненим текстом (наприклад, слідом пакету документів летить підправлений варіант), то на підставі знання вихідного тексту, або його зміненої частини можна «розмотати» весь текст і навіть пароль.

Остання вимога – псевдохаотічность вихідної інформації. Шифровка повинна бути складною, щоб в ній неможливо було виявити якісь закономірності [4]. Будь-який текст має досить яскраво виражену структуру, повторювані слова, і .т.п. До речі, псевдохаотічность шифру просто перевірити – досить спробувати заархівувати результуючий документ. Якщо від стиснення розмір зменшиться, значить алгоритм генерує надлишкову інформацію, в якій є закономірності.

Щоб пояснити алгоритм роботи хоча б одного широко використовуваного шифру, знадобилося б з десяток подібних статей. У будь-якому випадку, для непрофесіонала фраза «шифрування за допомогою введення зворотних зв'язків або шляхом генерації довгих шифруючих послідовностей» сама по собі звучить як шифр. У першому випадку кожен наступний блок залежить не тільки від початкового тексту і пароля, а й від тексту попередніх блоків (зрозуміло,

шматки не повинні знаходитися безпосередньо поруч один з одним, їх завдання – передувати в порядку виконання алгоритму). У другому випадку пароль стає «зерном» для генератора довгою шифрувальної послідовності, яка згодом і використовується протягом всього тексту (можливо, в комбінації з початковим шифром).

У обох підходів є свої переваги і недоліки, але другий тип шифрування трохи складніше для реалізації – адже в його основі лежить псевдовипадковий алгоритм. І якщо він «не дуже хороший», тобто починає досить швидко повторюватися або видає однакові значення при різних «зернах», то вся інша робота мало корисна і текст досить просто аналізується. Розумних же критеріїв перевірки «випадковості псевдовипадкових» алгоритмів не існує – хіба можна виміряти хаос? Найчастіше обидва підходи просто використовуються одночасно.

Практично будь-який алгоритм шифрування недосконалий. Завжди можна відстежити закономірності, пройти через «задні двері», врешті-решт, зламати «атакою в лоб», використавши обчислювальну потужність заражених комп'ютерів всього Інтернету. Але є спосіб так закодувати вихідний текст, що він не буде розкритий ніколи – навіть коли зірки згорять і всесвіт перетвориться в чорну діру. Цей метод називається способом Вернама [5]. Його активно використовували під час Другої світової війни, а потім і під час холодної війни для передачі секретної інформації. Суть алгоритму полягає в одноразовому використанні довгою довільній ключовий послідовності розміром з переданий текст. Основна проблема таких «одноразового шифроблокнота» – необхідність постійного оновлення ключів, тому в епоху інформаційних технологій цей алгоритм був замінений іншими, менш стійкими, але набагато більш зручними в застосуванні.

Науковий керівник: Землянська О.В., ст. вик. (каф. ОППЦБ КПІ ім. Ігоря Сікорського)

Література

1. Arto Salomaa. Public-Key Cryptography. – ISBN 3540528318.
2. Singh S. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. – New York City: Doubleday, 1999. – 416 p. с. – ISBN 978-1-85702-879-9.
3. Martin, Keith M. Everyday Cryptography. – Oxford University Press, 2012. – p. 142 с. – ISBN 978-0-19-162588-6.
4. Mollin, R. A. Introduction to Cryptography. – CRC Press, 2007. – P. 80. – 413 p. – ISBN 1584886188.
5. Smith, Laurence D. Substitution Ciphers // Cryptography the Science of Secret Writing: The Science of Secret Writing. – Dover Publications, 1943. – P. 81. – ISBN 0-486-20247-X.