УДК 004.056.55+003.26.09

Старший викладач Копичко С.М., студент Легеза Д.В.

Національний технічний університет України
«Київський політехнічний інститут»

КРИПТОГРАФІЧНИЙ ПРОТОКОЛ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ СИСТЕМ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

Abstract

Sergiy M. Kopychko, senior lecturer; Dmytro V. Legeza, student
Cryptographic protocols of information protection for e-voting systems

In this work the method of encryption based on chaos theory was formulated. Encryption protocol based on chaos theory was created and tested on cryptostability. These results indicate the adequacy of the proposed method and the potential to use it for encrypting data.

Вступ

Шифрування є криптографічним методом, що широко використовується для збереження конфіденційності інформації, захищає дані від несанкціонованого доступу до них.

Криптографічні методи можуть бути класифіковані різним чином.

Один з методів класифікації полягає у поділі в залежності від кількості ключів, на яких базується відповідний криптоалгоритм [1-4]:

1. Безключові, в яких не використовуються будь-які ключі;
2. Одноключові (симетричні) – в них використовується якийсь додатковий ключовий параметр - зазвичай це секретний ключ;
3. Двохключові (асиметричні), які використовують у своїх обчисленнях два ключі: закритий і відкритий.

У роботі розглядаються одноключові методи шифрування. Існуючі криптометоди є дієвими, хоча у їх основі лежать класичні математичні методи (гамування складними алгебраїчними функціями). Саме тому існує нагальна необхідність вдосконалення або створення нових алгоритмів шифрування на основі сучасного математичного апарату.

У роботі описується новий криптопротокол, що базується у своєму математичному апараті на методиках динамічного хаосу.

Постановка задачі

Мета роботи – проектування криптографічного протоколу захисту інформації на основі динамічного хаосу для захищеної передачі інформації в системах електронного голосування та перевірка його криптостійкості.

Термінологічний словник

Гамма – псевдовипадкова послідовність байтів, що додається до вихідних даних за модулем 2 з метою усунення в них можливих статистичних залежностей.

Гамування – метод шифрування, що оснований на «накладанні» гаммапослідовності на відкритий текст. У більшості випадків використовується додавання у певному скінченному полі (у полі GF(2) таке додавання перетворюється в операцію виключаючого АБО – XOR). Для розшифрування інформації операція гамування проводиться ще раз.

Гаммапослідовність – послідовность псевдовипадкових елементів, найчастіше бітів даних.

Шифртекст – інформація, до якої застосована операція шифрування.

Проектування крипто протоколу

Можливі учасники криптографічного протоколу електронного голосування:

- Сервер реєстрації;
- Сервер анонімізації;
- Сервер підрахунку голосів;
- Середовище зв'язку.

Криптографічні примітиви, що використовуються для забезпечення коректності процедури електронного голосування:

- Схема електронного цифрового підпису;
- Схема шифрування;
- Схема прив'язки до біта.

Протокол, що розглядається у роботі, створений на основі протоколу Фуджіокі-Окамото-Охти. Нижче будуть описані основні складові протоколу.

Етап реєстрації. Користувач:

1. Заповнює бюлетень v_i;
2. Формує прив'язку до біта (формує зашифрований бюлетень на основі відкритого ключа, вигаданого користувачем)

3. Отримує підпис від сервера реєстрації під бюлетенем. Це забезпечує анонімність користувача.

Етап подачі голосу

Користувач направляє підписаний сервером реєстрації бюлетень серверу підрахунку голосів по анонімному каналу зв'язку (через сервер анонімізації). Сервер підрахунку голосів перевіряє підпис сервера реєстрації під зашифрованим бюлетенем і додає його до списку.

Етап підрахунку голосів

Користувач перевіряє наявність зашифрованого підписаного бюлетеня в загальнодоступному списку і знімає прив'язку до біта, направляючи серверу підрахунку голосів ключ шифрування по анонімному каналу (через сервер анонімізації). Сервер розшифровує зашифрований бюлетень і обробляє його.

Протокол був удосконалений наступними пунктами:

- Користувачеві немає необхідності вигадувати ключ для зашифровування бюлетеня. При ініціації події «генерація бюлетеня», у внутрішній службовий список сервера реєстрації додається запис з наступною інформацією: унікальний ID номер бюлетеня та динамічно згенерований ключ. Як тільки користувач заповнив бюлетень, він відразу ж шифрується згенерованим відкритим ключем, який передається по загальнодоступному каналу. Таким чином вирішується проблема з можливим ускладненням при створенні надійного ключа користувачем, крім того забезпечується надійне збереження інформації за рахунок алгоритму із закритим ключем.
- Крім того попереднім пунктом вирішується проблема повторного використання системи користувачем: немає необхідності перевіряти наявність бюлетеня і вводити ключ для його розшифрування. Все забезпечується алгоритмом із закритим ключем.

Таким чином бюлетень проходить наступні стадії:

- Бюлетень та унікальний ключ згенеровано. Після голосування бюлетень зашифровується хаотичним криптоалгоритмом. Після цього шифрується за допомогою алгоритму RSA для сервера анонімізації.
- Після того, як бюлетень доставлено на сервер, алгоритм RSA знімає свій підпис та зберігає бюлетень до моменту підрахунку голосів у зашифрованому стані.
- Як тільки ініціюється процес підрахунку голосів, бюлетень розшифровується за допомогою хаотичного ключа, що зберігається у базі. Адміністратор отримує повністю розшифрований бюлетень та має можливість проводити підрахунок.

Одним з найбільш важливих компонентів протоколу є хаотичне шифрування, яке описано нижче.

Хаотичне шифрування

У роботі пропонується підхід до використання динамічного хаосу в шифруванні інформації. Запропонований підхід є варіантом гамування – процесу "накладання" гаммапослідовності на відкриті дані, де в якості гаммапослідовності використовується послідовність динамічного хаосу, а точніше набір послідовних точок, що моделюють поведінку атрактора Лоренца:

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = x(r - z) - y \\ \dot{z} = xy - bz \end{cases},$$

де σ, r, b – характеристики атрактора.

Ідея застосування атрактора Лоренца з метою генерації випадкової послідовності бітів виходить з того, що траєкторія атрактора буде випадковою за умови навіть незначної зміни початкових умов. Якщо у певній точці два різних атрактори з різними початковими точками перетнуться, то ключ, що буде згенеровано обома атракторами, буде абсолютно різним.

У роботі досягнуто формування ключа розміром 4096 біт, що дозволяє шифрувати інформацію з достатнім рівнем захисту.

Висновки

Спроектовано криптографічний протокол захисту інформації для систем електронного голосування. Проведені випробування дозволяють стверджувати наступне:

1) даний криптопротокол підтвердив потенційну можливість його використання для шифрування інформації;
2) проведений диференційний та статистичний криптоаналіз довів стабільність розробленого криптопротоколу;
3) при найменших змінах параметрів та початкових умов (зміни $>10^{-9}$), отримано абсолютно різні шифртексти;
4) проведено тестування навантаженням і доведено, що з 1 млрд. ключів, що згенеровані блоком хаотичного криптоалгоритму, жоден не співпадає. Період генерації склав 2 години.

Література

1. *Баричев С. В.* Криптография без секретов. – М.: Наука, 1998. – 120 с.
2. *Диффи У.* Первые десять лет криптографии с открытым ключом // ТИИЭР – 1988 – т. 76 – С. 54-74.
3. Панасенко С.П. Назначение и структура алгоритмов шифрования //Русский Bugtraq. – 2002. [Електронний ресурс]. URL: http://www.ixbt.com/soft/alg-encryption.shtml (12.02.2011).
4. Панасенко С.П. Применение шифрования и стойкость RSA // IXBT. – 2006. [Електронний ресурс]. URL: http://www.bugtraq.ru/library/crypto/rsa.html (14.02.2011).