Лабораторна робота 2.2

АЛГОРИТМ ЕЛЬ–ГАМАЛЯ

Мета: отримати навички у створенні програмної реалізації алгоритму асиметричного алгоритму Ель-Гамаля.

Основні завдання:

1. Розробити об’єктно-орієнтованою мовою програмування консольний або віконний додаток, що реалізує шифрування та дешифрування вмісту текстового або виконуваного файлу з використанням асиметричного алгоритму Ель-Гамаля. Програма повинна запитувати ім'я вхідного і вихідного файлів, тип шифру та вхідні параметри для проведення криптографічних перетворень. В якості вхідних параметрів виступають: p – велике просте число, a – первісний корінь простого числа p; x – значення закритого ключа.
2. Представити блок структурну схему своєї програмної реалізації.
3. Зробити висновки на підставі проведених теоретичних та практичних досліджень. У висновках слід зазначити, які навички та знання отримано під час виконання завдань.

Основні теоретичні відомості

Алгоритму Ель-Гамаля альтернатива алгоритму RSA і при рівному значенні ключа забезпечує таку саму криптостійкість. Може використовуватися для формування електронного підпису або для шифрування даних. Безпека алгоритму Ель–Гамаля базується на складності обчислювання дискретних логарифмів.

Розглянемо основні етапи алгоритму Ель–Гамаля:

Учасники інформаційного процесу обирають просте число p p і ціле число q a, який є первісним коренем за модулем p p, $p > a$, $НСД[p,a]=1$.

Сторона A генерує сеансовий ключ $y < p$ при умову, що $НСД[y,\varphi(p)]=1$ $k_a < p$.

Сторона B обирає число $x < p$ $k_b < p$ при умову, що $1 < x < p-1$ та розраховує парамеметр $b = a^x \pmod p$. Таким чином комбінація (a,p,b) представляє собою відкритий ключ отримувача.

При виборі x і y одержувачем і відправником відповідно, природно, повинно виконуватися вимога до їх інформаційної ємності. Для генерації цих чисел повинен використовуватися *криптостійкий генератор псевдовипадкових чисел (КГПВЧ)*. В іншому випадку зловмисник просто визначить x або y повним перебором.

Далі за допомогою відкритого ключа відбувається шифрування повідомлення M M у за формулами.

$$e = a^y \pmod p, \quad Y_a \equiv q^{k_a} (mod\ p) \quad k = \left(b^y m\right) \bmod p$$

Отже, пара чисел (e,k) і виступає в якості шифротексту.

Для проведення процедури дешифрування Одержувач, використовуючи свій закритий ключ дешифрує повідомлення вирішуючи Діофантове рівнянь:

$$m \cdot a^y \pmod p = k \quad m \cdot a^y \pmod p = k$$

Для практичних обчислень більше підходить наступна формула:

$$m = k \cdot \left(e^x\right)^{-1} \bmod p \Rightarrow m = k \cdot e^{(p-1-x)} \bmod p \quad \text{або}$$

$$m = \left(\frac{k}{e^x}\right) \bmod p = \left(k \bmod p \cdot e^{-x} \bmod p\right) \bmod p =$$

$$= \left(k \bmod p \cdot e^{\varphi(p)-x} \bmod p\right) \bmod p$$

Алгоритм Ель–Гамаля – перший криптографічний алгоритм з відкритим ключем, який використовується для шифрування повідомлень і цифрових підписів, використання якого не обмежено патентами США. На відміну від RSA алгоритм Ель-Гамаля не запатентований і, тому, став більш дешевою альтернативою, оскільки не була потрібна оплата внесків за ліцензію. Вважається, що алгоритм потрапляє під дію патенту Діффі-Хеллмана. Існує велика кількість алгоритмів, заснованих на схемі Ель-Гамаля: це алгоритми DSA, ECDSA, KCDSA, схема Шнорра.

По криптостійкості в схемі Ель-Гамаль 512-бітове число p прирівнюється до 56-бітного симетричного ключа. Тому на практиці застосовуються p довжиною в 768, 1024,1536, 2048 біт.

Запитання для самоперевірки

1. Охарактеризуйте основні відмінності алгоритму Ель–Гамаля від RSA.
2. Поясність основні етапи знаходження відкритого ключа шифрування?

3. Поясніть основні умови вибору закритого ключа.
4. Охарактеризуйте основні етапи проведення шифрування алгоритму Ель–Гамаля.
5. Назвіть основні переваги та недоліки алгоритму Ель–Гамаля.