МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

**ЛАБОРАТОРНА РОБОТА №3**

**з дисципліни**

**«МЕТОДИ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ МЕХАНІЗМІВ»**

**на тему: «РОЗРОБКА РЕАЛІЗАЦІЇ АСИМЕТРИЧНОЇ КРИПТОСИСТЕМИ»**

Виконала:

студентка 6 курсу ФТІ

група ФБ-11мн

Чуракова Єкатєріна

Перевірив:

Байденко П.В.

Київ 2022

Варіант 2А: OPENSSL ПІД WINDOWS ПЛАТФОРМУ. КР/С ЕЛЬ ГАМАЛЯ

Схема Ель-Гамаля – криптосистема з відкритим ключем, заснована на труднощі обчислення дискретних логарифмів у кінцевому полі. Криптосистема включає алгоритм шифрування і алгоритм цифрового підпису. Схему було запропоновано Тахером Эль-Гамалем в 1985 году. Ель-Гамаль розробив один із варіантів алгоритму Діффі-Хеллмана. Він удосконалив систему Діффі-Хеллмана і отримав два алгоритми, які використовувалися для шифрування та забезпечення аутентифікації.

Генерація ключів

Генерація ключів проходить у 5 етапів:

1. Генерується випадкове просте число *p*.
2. Вибирається ціле число *g* – первісний корінь *p*.
3. Вибирається випадкове ціле число *x* таке, що (1<*x*<*p*-1).
4. Обчислюється *y=gx* mod *p*.
5. Відкритим ключем є (*y*,*g*,*p*), закритим ключем - число *x*.

Робота в режимі шифрування

Повідомлення *M* має бути менше числа *p*. Повідомлення шифрується так:

1. Вибирається сесійний ключ – випадкове ціле число, взаємно просте з (*p*-1), *k* таке, що 1 <*k*<*p*-1.
2. Обчислюються числа *a* = *gk* mod *p* і *b* = *yk M* mod *p*
3. Пара чисел (*a*,*b*) є шифротекстом.

Знаючи закритий ключ *x*, вихідне повідомлення можна обчислити із шифротексту (*a*,*b*) за формулою: *M*=*b*(*ax*)*-1* mod *p*.

Робота у режимі підпису

При роботі в режимі підпису передбачається наявність фіксованої хеш-функції *h()*, значення якої лежать в інтервалі (1, *p*-1).

1. Обчислюється хеш повідомлення *M*: *m*=*h*(*M*).
2. Вибирається випадкове число 1<*k*<*p*-1 взаємно просте з *p*-1 і обчислюється *r* = *gk* mod *p*.
3. Обчислюється число *s* = (*m*-*xr*)*k-1*(mod *p*-1), де *k-1* це мультиплікативне зворотне *k* за модулем *p*-1, яке можна знайти за допомогою розширеного алгоритму Евкліда.
4. Підписом повідомлення *M* є пара (*r*, *s*).

Знаючи відкритий ключ (*p*, *g*, *y*) підпис (*r*, *s*) повідомлення *M* перевіряється так:

1. Перевіряється виконання умов 0<*r*<*p* і 0<*s*<*p*-1.
2. Якщо хоча б одна з них не виконується, то підпис вважається недійсним.
3. Обчислюється хеш *m*=*h*(*M*).
4. Підпис вважається дійсним, якщо виконується порівняння: *yrrs* = *gm*(mod *p*)

Отримані результати



Висновки

У роботі була реалізована криптосистема Ель-Гамаля за допомогою бібліотеки OpenSSL. Було протестовано роботу у режимі шифрування (шифрування і розшифрування), та у режимі підпису (підпис і верифікація).