МЕТОДИ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ МЕХАНІЗМІВ
ЛАБОРАТОРНА РОБОТА №3

“Реалізація основних асиметричних криптосистем”.

Недождій Максим, Буржимський Ростислав

ФІ-42мн

1 Мета роботи

Дослідження можливостей побудови загальних та спеціальних криптографічних протоколів за допомогою асиметричних криптосистем.

2 Постановка задачі

Підгрупа 2А. Бібліотека OpenSSL під Windows платформу. Кр/с Ель Гамаля.
Примітка. Розробка криптосистеми була виконана під Unix платформу.

3 Хід роботи

Знайдено бібліотеку, обрано необхідні класи для роботи з великими числами, розроблено необхідні функції, протестовано отриману криптосистему, оформлено мінімалістичний інтерфейс, оформлено результати.

4 Розроблені і використані елементи криптосистеми

Алгоритм 1 ElGamal.Encrypt

Вхід: Приватний ключ x, відкритий ключ $y = g^x \bmod p$, генератор g, модуль p, повідомлення m.
Вихід: Шифротекст (c_1, c_2).
1: Вибрати випадкове число $k \in \{1, \dots, p-2\}$.
2: $c_1 \leftarrow g^k \bmod p$
3: $c_2 \leftarrow m \cdot y^k \bmod p$
4: **return** (c_1, c_2)

Алгоритм 2 ElGamal.Decrypt

Вхід: Приватний ключ x, модуль p, шифротекст (c_1, c_2).
Вихід: Розшифроване повідомлення m.
1: $s \leftarrow c_1^x \bmod p$
2: $s^{-1} \leftarrow$ обернений елемент до s за модулем p
3: $m \leftarrow c_2 \cdot s^{-1} \bmod p$
4: **return** m

Реалізували пошук генератора у форматі $p = 2 \cdot q + 1$, де q - ще одне велике число. Тобто p є *hard prime*. Тоді перевірити чи число є генератором буде легко, адже потрібно виконати лише 2 піднесення у степінь: у степені 2 і q.

Алгоритм 3 ElGamal.Sign

Вхід: Приватний ключ x, генератор g, модуль p, повідомлення m.
Вихід: Підпис (r, s).

1: Вибрати випадкове число $k \in \{1, \ldots, p-2\}$, таке що $\gcd(k, p-1) = 1$.
2: $r \leftarrow g^k \bmod p$
3: Обчислити k^{-1} — обернений до k за модулем $p-1$.
4: $s \leftarrow k^{-1} \cdot (m - x \cdot r) \bmod (p-1)$.
5: **return** (r, s)

Алгоритм 4 ElGamal.Verify

Вхід: Відкритий ключ $y = g^x \bmod p$, генератор g, модуль p, повідомлення m, підпис (r, s).
Вихід: Перевірка підпису (**true** або **false**).

1: **if** $r \notin \{1, \ldots, p-1\}$ **then**
2: **return false**
3: **end if**
4: $v_1 \leftarrow y^r \cdot r^s \bmod p$
5: $v_2 \leftarrow g^m \bmod p$
6: **if** $v_1 = v_2$ **then**
7: **return true**
8: **else**
9: **return false**
10: **end if**

5 Приклад роботи криптосистеми

Примітка. Усі повідомлення мають бути подані на вхід у HEX форматі і не перевищувати значення модуля p.

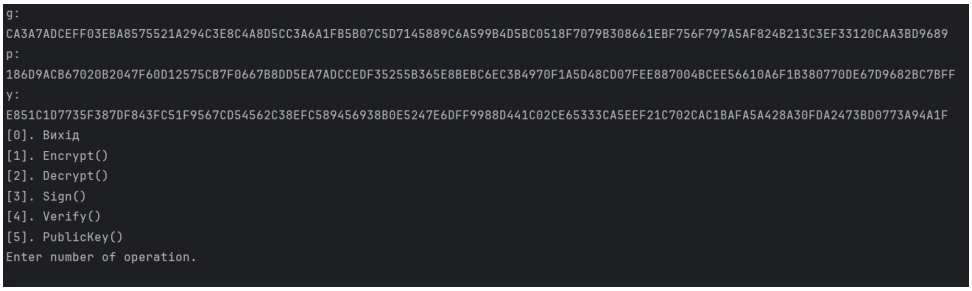

Figure 1: Головне меню з вибором операцій і згенерованим публічним ключем

Figure 2: Шифрування за вказаними параметрами публічного ключа

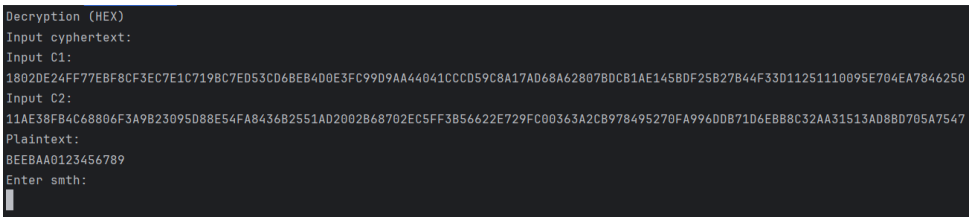

Figure 3: Розшифрування за вказаними значеннями C_1, C_2

Figure 4: Підпис повідомлення

Figure 5: Верифікація підпису повідомлення за згенерованими параметрами підпису і публічним ключем.

Figure 6: Доступне для перегляду значення публічного ключа