

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 Гамалія.

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 $p \in \text{hard prime}$. 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 $k \in \{1, \dots, p-2\}$, 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** $r \notin \{1, \dots, p-1\}$ **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 .

```
q:
CA3A7ADCEFF03EBA8575521A294C3EBC4A8D5CC3A6A1FB5B07C5D71458B9C6A599B4D5BC0518F7079B308661EBF756F797A5AF824B213C3EF33120CAA3BD9689
p:
186D9ACB67020B2047F60D12575CB7F0667B8D05EA7ADCCEDF35255B365E8BEBC6EC3B4970F1A5D48CD07FEE887004BCCEE56610A6F18380770DE67D9682BC7BFF
y:
E851C1D7735F387DF843FCS1F9567CD54562C38EFC589456938B0E5247E6DFF9988D441C02CE65333CA5EEF21C702CAC1BAFA5A428A30FDA2473BD0773A94A1F
[0]. Вихід
[1]. Encrypt()
[2]. Decrypt()
[3]. Sign()
[4]. Verify()
[5]. PublicKey()
Enter number of operation.
```

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

```

Encryption (HEX)
Input primitive element of group (g):
CA3A7ADCEFF03EBA8575521A294C3E8C4A8D5CC3A6A1F85B07C5D7145889C6A599B4D5BC0518F7079B308661EBF756F797A5AF824B213C3EF33120CAA3BD9689
Input prime mod (p):
186D9ACB67020B2047F60D12575C87F0667B8DD5EA7ADCCEDF35255B365E8BEBC6EC3B4970F1A5D48CD07FEE887004BCEE56610A6F1B380770DE67D9682BC7BFF
y:
E851C1D7735F387DF843FC51F9567CD54562C38EFC589456938B0E5247E6DFF9988D441C02CE65333CA5EEF21C702CAC18AFAS428A30FDA2473BD0773A94A1F
Input message:
8EEBA0123456789
(c1,c2) =
1802DE24FF77EBF8CF3EC7E1C7198C7ED53CD68EB4D0E3FC99D9AA44041CCCD59C8A17AD68A62807BDCB1AE145BDF25B27B44F33D11251110095E704EA7846250
11AE38FB4C68806F3A9B23095D88E54FA8436B2551AD2002B68702EC5FF3B56622E729FC00363A2C8978495270FA996D0B71D6EBB8C32AA31513AD8BD705A7547
Enter smth:

```

Figure 2: Шифрування за вказаними параметрами публічного ключа

```

Decryption (HEX)
Input cyphertext:
Input C1:
1802DE24FF77EBF8CF3EC7E1C7198C7ED53CD68EB4D0E3FC99D9AA44041CCCD59C8A17AD68A62807BDCB1AE145BDF25B27B44F33D11251110095E704EA7846250
Input C2:
11AE38FB4C68806F3A9B23095D88E54FA8436B2551AD2002B68702EC5FF3B56622E729FC00363A2C8978495270FA996D0B71D6EBB8C32AA31513AD8BD705A7547
Plaintext:
8EEBA0123456789
Enter smth:

```

Figure 3: Розшифрування за вказаними значеннями C_1 , C_2

```

Sign (HEX):
Enter message:
0123456789ABCDEF
SIGN (r,s):
0360292977634470E971A4AB3E0663EE0C1915EF31FC6AF32703671A7101EA0EFD0FBAD73E7DB1776B0D071135BE52384A92E808E3E9F42889EC51AACCE95828
F824D56BA4E35449474737B1391BC8C9F9321CBA138F0B4B35EE60EEEC261E6AAD98CE5D9879471B560FE2BB05C36B9B955E5F8523866B192FBE80313D21E84F
Enter smth:

```

Figure 4: Підпис повідомлення

```

Verify (HEX):
Enter r:
0360292977634470E971A4AB3E0663EE0C1915EF31FC6AF32703671A7101EA0EFD0FBAD73E7DB1776B0D071135BE52384A92E808E3E9F42889EC51AACCE95828
Enter s:
F824D56BA4E35449474737B1391BC8C9F9321CBA138F0B4B35EE60EEEC261E6AAD98CE5D9879471B560FE2BB05C36B9B955E5F8523866B192FBE80313D21E84F
Enter m:
0123456789ABCDEF
Input primitive element of group (g):
CA3A7ADCEFF03EBA8575521A294C3E8C4A8D5CC3A6A1F85B07C5D7145889C6A599B4D5BC0518F7079B308661EBF756F797A5AF824B213C3EF33120CAA3BD9689
Input prime mod (p):
186D9ACB67020B2047F60D12575C87F0667B8DD5EA7ADCCEDF35255B365E8BEBC6EC3B4970F1A5D48CD07FEE887004BCEE56610A6F1B380770DE67D9682BC7BFF
y:
E851C1D7735F387DF843FC51F9567CD54562C38EFC589456938B0E5247E6DFF9988D441C02CE65333CA5EEF21C702CAC18AFAS428A30FDA2473BD0773A94A1F
Verify: 1
Enter smth:

```

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

```

g:
CA3A7ADCEFF03EBA8575521A294C3E8C4A8D5CC3A6A1F85B07C5D7145889C6A599B4D5BC0518F7079B308661EBF756F797A5AF824B213C3EF33120CAA3BD9689
p:
186D9ACB67020B2047F60D12575C87F0667B8DD5EA7ADCCEDF35255B365E8BEBC6EC3B4970F1A5D48CD07FEE887004BCEE56610A6F1B380770DE67D9682BC7BFF
y:
E851C1D7735F387DF843FC51F9567CD54562C38EFC589456938B0E5247E6DFF9988D441C02CE65333CA5EEF21C702CAC18AFAS428A30FDA2473BD0773A94A1F
Enter smth:

```

Figure 6: Доступне для перегляду значення публічного ключа