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 $y=g^x \bmod p$.
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 $a = g^k \bmod p$ і $b = y^k M \bmod p$
3. Пара чисел (a,b) є шифротекстом.

Знаючи закритий ключ x, вихідне повідомлення можна обчислити із шифротексту (a,b) за формулою: $M=b(a^x)^{-1} \bmod p$.

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 $r = g^k \bmod p$.
3. Обчислюється число $s = (m-xr)k^{-1} \pmod{p-1}$, 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: $y^r r^s = g^m \pmod p$

Отримані результати

```
Original message: Some message is present here!1
Encrypted message: a = 5721EE997D1F2AB946358A123E9C52B1C85F657B87C78B55050549DBC864
D50E29CDB4CCDCF366327A9915D691D150BCEA9294270F2857712978758479F0FCDF3166ED99B92BBC6
74988A3E3890A5975F3DB51C5F81FDFF5B1E4353FF84BCBBFF42D9384FC756B979282F55B5FCE90D909
A76631DCB01943832350AADB7D32D8; b = D6777AF3E97A8C732219658DCC9E588919B33EA37715F7B
9D73E20A9281756D483C8D5CB4CDAB17746A6EC730CC86DA2C04BD353DF998E3D68EC0EAE3F83A2263F
D1832504A715A6AE03C7E80105979A306AE88BEC274691F95916993FABE4210DED181598BE8313732D8
EC81B5B7A7C402A5EDC917B12536869CC78D70F1F53
Decrypted message: Some message is present here!1
Signing message: Some message is present here!1
Signature: r = EBEE59699B54D6FF4C36BE3E0F4A0370C8A691DF860CF4DB094A05E4C16530EEBAB1
ECDE7FAF79B6539B6F4680CD7FBF5AD93172D3BA8D8E43B26CE842BE445A39E38C7941A2154682723DF
C3848464710F63C52503BBB20A6D0F2000A13D4B13C82A42E93B67CA72BEB39BC4AF9F6F24D05F32F25
E158E82D70354D524FC5AC; s = A8636A91F97A8501E67FDF0C99F1F70CCA70FC4E8B603B2F0560304
D3991EEE3F55B770EC1587FF97CEA8011B858B8B64C1E7323B46DD399BA115CA2EAB2C5BB0162C806AD
58C1541A3C07F881292F4FED2B4302739568A6934D232A069EAB39C50CA31B22B9664F803D94987E8B8
C89FC086105644CF1089696182726C463E7
Verify this message with signature: Some message is present here!1; Result: 1
Verify this message with signature: Some message is present here!2; Result: 0
```

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).