**Лабороторна работа №7**

**Тема:** Алгоритмалгоритм “EL Gamal”

**Мета:** Відпрацювання та закріплення теоретичних відомостей з криптоалгоритму “EL Gamal”

**Короткі відомості****:**

Криптосистема Ель-Гамаля (El Gamal) — Криптосистема з відкритим ключем, заснована на труднощі обчислення дискретних логарифмів в кінцевому полі. Криптосистема включає в себе алгоритм шифрування і алгоритм цифрового підпису. Схема Ель-Гамаля лежить в основі колишніх стандартів електронного цифрового підпису в США (DSA) і Росії (ГОСТ Р 34.10-94).

Схема була запропонована Тахера Ель-Гамаль в 1985. Ель-Гамаль розробив один з варіантів алгоритму Діффі-Хеллмана. Він удосконалив систему Діффі-Хеллмана і отримав два алгоритми, які призначені для шифрування і для автентифікації. На відміну від RSA алгоритм Ель-Гамаля не запатентований і тому, став дешевшою альтернативою, оскільки не потрібна оплата внесків за ліцензію. Вважається, що алгоритм потрапляє під дію патенту Діффі-Геллмана.

Генерація ключів

1. Генерується випадкове просте число ***p*** бітів.
2. Вибирається випадковий примітивний елемент ***g,*** (***1<g<p-1***)
3. Вибирається випадкове ціле число ***x*** таке, що ***1<x<p-1***.
4. Обчислюється ***y=g^x mod p*** .
5. Відкритим ключем є трійка ***(p,g,y)***, закритим ключем — число ***x***.

**Робота в режимі шифрування**

Шифрування:

Повідомлення ***M*** шифрується таким чином:

* 1. Вибирається сесійний ключ - випадкове ціле число ***k*** таке, що ***1<k<p-1***
  2. Обчислюються числа ***a=g^k mod p*** і ***b=y^k M mod p*** .
  3. Пара чисел (***a***, ***b)*** є шифротекстом.

Неважко побачити, що довжина шифротекста у схемі Ель-Гамаля довша за вихідне повідомлення ***M*** вдвічі.

Розшифрування:

Знаючи закритий ключ ***x***, вихідне повідомлення можна обчислити з шифротекста ***(a, b)*** за формулою:

***M=b(a^x)^-1 mod p***

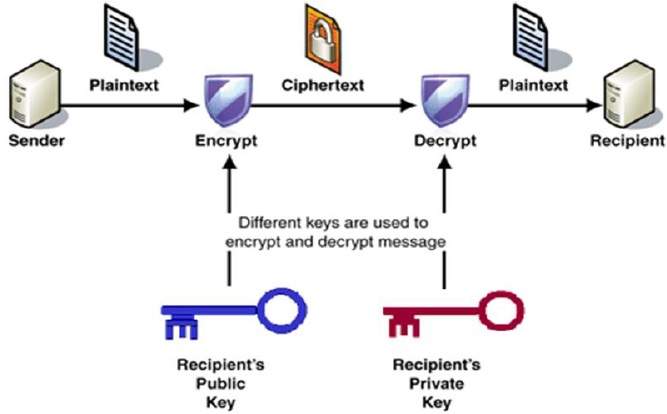
При цьому неважко перевірити, що

***(a^x)^-1 = g^-kx (mod p)*** і тому

***b(a^x)^-1 = (y^k M)g ^ -xk = (g^xk M)g^-xk = M mod p***

Для практичних обчислень більше підходить наступна формула:

***M=b(a^x)^-1 mod p = b\*a^(p-1-x) mod p***

**Робота в режимі підпису**

Підпис повідомлень

Для підпису повідомлення ***M*** виконуються наступні операції:

1. Обчислюється дайджест повідомлення ***M***: ***m = h (M)***.

2. Вибирається випадкове число ***1<k<p-1*** взаємно просте з ***p-1*** і обчислюється ***r = g^k mod p***

3. Обчислюється число ***s = (m – xr ) k^-1 (mod p-1).***

4. Підписом повідомлення ***M*** є пара ***( r, s ).***

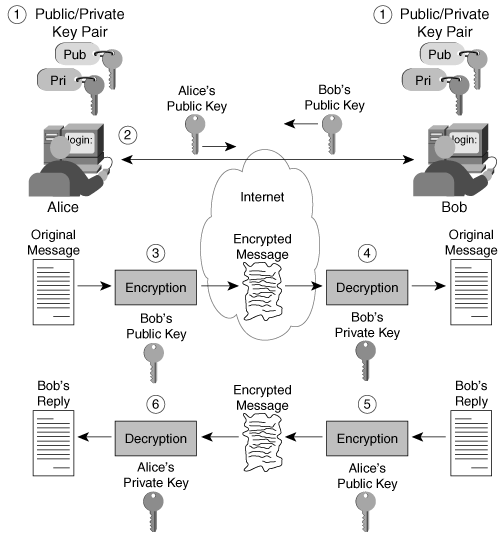
Перевірка підпису

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

1. Перевіряється здійснимість умов: ***0<r<p*** і ***0<s<p-1***. Якщо хоча б одна з них не виконується, то підпис вважається невірним.

2. Обчислюється дайджест ***m=h(M)***

3. Підпис вважається вірним, якщо виконується порівняння: ***y^r r^s = g^m (mod p )***



**Висновок:** Шифрування El Gamal відноситься до асиметричного шифрування та криптостійкості. Криптостійкість Ель-Гамаля і Діффі-Хеллмана забезпечується проблемою вирахувань дискретного логарифма. Алгоритм Ель-Гамаля являється логічним продовження алгоритма Діффі-Хеллмана. В алгоритмі Ель-Гамаля використовується математична функція операції піднесення в степінь по модулю простого числа. Алгоритм Ель-Гамаля використовується для шифрування/дешифрування повідомлень та створення електронноцифрового підпису, а алгоритм Діффі-Хеллмана використовується для генерації і розподілу ключів.