**Код Діффі-Хелмана**

1. Абоненти разом вибирають великі прості числа n і g так, щоб g було примітивом mod n.
2. Абонент 1 вибирає випадкове велике ціле число x і посилає абонентові 2

Х = g^x mod n

1. Абонент 2 вибирає випадкове велике ціле число y і посилає абонентові 1

Y = g^y mod n

1. Абонент 1 обчислює

k1 = Y^x mod n

1. Абонент 2 обчислює

k2= Х^y mod n

1. І k1, і k2 дорівнюють g^xy mod п. Це - секретний ключ, який абоненти обчислюють незалежно.

**Код Ель-Гамаля**

Етап побудови ключів

1. Вибирається довільне (достатньо велике) просте число р.
2. Для цього простого числа визначається будь-який похідний елемент (англ., primitive root) –

тобто таке число а, при багатократному піднесенні якого до степеня по модулю р (a1 mod p, a2 mod p...) перебиратимуться (у довільному порядку, але обов'язково лише по одному разу) всі числа від 1 до (р - 1) включно.

1. Генерується довільне випадкове число х (0 < х < р) – це і є закритий ключ.
2. Обчислюється значення b = а^х mod р – комбінація (а, р, b) є відкритим ключем одержувача.

Етап шифрування

1. Відправник генерує довільне випадкове число y (0 < y < р).
2. Поміщає в початок шифрограми число (а^у mod р).
3. Обчислює величину k = (b^y mod р) = ((а^х mod р)y mod p).
4. Використовуючи деяку, заздалегідь обумовлену в даній реалізації, частину k як симетричний ключ для будь-якого блокового шифру, кодує повідомлення, що відправляється.
5. Необхідно забути числа у і k.

Етап дешифрування

1. По приходу зашифрованого повідомлення одержувач відокремлює від пакету величину (ау mod р) і обчислює на її основі ((ау mod p)x mod р) .
2. Одержувач дешифрує весь пакет, що йде далі, симетричним алгоритмом.