**Ілюстрація роботи RSA на прикладі**

**Крок перший. Підготовка ключ**ів

Генерування публічного та приватного ключів.

Обираємо два простих числа. Нехай це буде p=3 та q=7.

Обчислюємо модуль - добуток наших p і q: n=p×q=3×7=21.

Обчислюємо функцію Ейлера: φ=(p-1)×(q-1)=2×6=12.

Вибираємо число e, що відповідає наступним критеріям: (i) воно має бути просте, (ii) воно має бути меншим за φ — залишаються варіанти: 3, 5, 7, 11, (iii) воно має бути взаємно просте з φ; залишаються варіанти 5, 7, 11. Виберемо e = 5. Це так звана відкрита експонента.

Тепер пара чисел {e, n} – це мій відкритий ключ. Я надсилаю його вам, щоб ви зашифрували своє повідомлення. Але для мене це ще не все. Я мушу отримати закритий ключ.

Мені потрібно обчислити число d, обернене по модулю φ. Тобто залишок від розподілу за модулем φ твору d×e має дорівнювати 1. Запишемо це в позначеннях, прийнятих у багатьох мовах програмування: (d×е)%φ=1. Або (d×5)%12=1. d може бути рівним 5 ((5×5)%12=25%12=1), але щоб воно не плуталося з e в подальшому оповіданні, давайте візьмемо його рівним 17. Можете перевірити самі, що (17×5)%12 дійсно одно 1 (17×5-12×7=1). Отже, d=17. Пара - це секретний ключ, його я залишаю у себе. Його не можна повідомляти нікому. Тільки власник секретного ключа може розшифрувати те, що було зашифровано відкритим ключем.

**Крок другий. Шифрування**

Тепер настала ваша черга шифрувати ваше повідомлення. Припустимо, повідомлення це число 19. Позначимо його P=19. Крім нього, у вас вже є мій відкритий ключ: {e, n} = {5, 21}. Шифрування виконується за таким алгоритмом:

Зводьте ваше повідомлення у ступінь e за модулем n. Тобто, обчислюєте 19 ступенем 5 (2476099) і берете залишок від розподілу на 21. Виходить 10 - це ваші закодовані дані.

Строго кажучи, вам зовсім нема чого обчислювати величезне число «19 ступенем 5». При кожному множенні досить обчислювати не повний твір, лише залишок від розподілу на 21. Але це вже деталі реалізації обчислень, давайте у них заглиблюватися.

Отримані дані E=10 ви надсилаєте мені.

Тут слід зазначити, що повідомлення P=19 має бути більше n=21. інакше нічого не вийде.

**Крок третій. Розшифровка**

Я отримав ваші дані (E=10), і я маю закритий ключ {d, n} = {17, 21}.

Зверніть увагу, що відкритий ключ не може розшифрувати повідомлення. А закритий ключ я нікому не говорив. У цьому вся краса асиметричного шифрування.

Починаємо розкодувати:

Я роблю операцію дуже схожу на вашу, але замість e використовую d. Зводжу E у ступінь d: отримую 10 у ступеню 17 (дозвольте, я не писатиму одиначку з сімнадцятьма нулями). Обчислюю залишок від розподілу на 21 і отримую 19 - ваше повідомлення.

Зверніть увагу, ніхто, крім мене (навіть ви!) не може розшифрувати ваше повідомлення (E=10), тому що ні в кого немає закритого ключа.