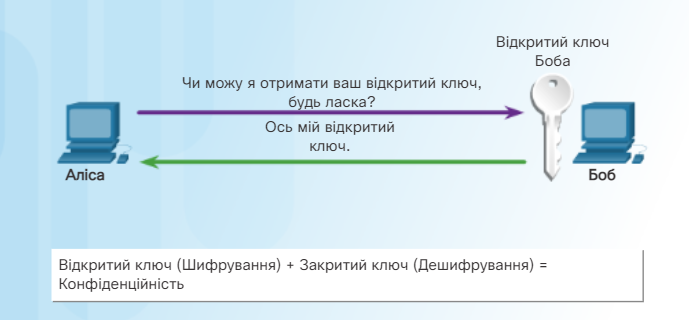
# Асиметричне шифрування

**Асиметричне шифрування**, також відоме як шифруванням з відкритим ключем, для шифрування використовує ключ, який відрізняється від ключа для дешифрування. Злочинець не може в прийнятні терміни обчислити ключ дешифрування, знаючи ключ шифрування і навпаки.



Якщо Аліса і Боб обмінюються секретними повідомленнями за допомогою шифрування з відкритим ключем, вони використовують асиметричний алгоритм. На цей раз Боб і Аліса не обмінюються ключами до відправки секретних повідомлень. Замість цього у Боба і Аліси є окремі замки з відповідними ключами. Якщо Аліса надсилає секретне повідомлення Бобу, вона має спочатку зв'язатися з ним і попросити його надіслати свій відкритий замок. Боб надсилає замок, але зберігає свій ключ. Коли Аліса отримує замок, вона пише своє секретне повідомлення і вкладає його в маленьку коробку. В ту ж коробку вона кладе свій відкритий замок, але залишає у себе свій ключ. Потім вона замикає коробку замком Боба. Коли Аліса закриє коробку, вона більше не зможе її відкрити, тому що у неї немає ключа до цього замку. Вона відправляє коробку Бобу, і, поки відправлення проходить через поштову систему, ніхто не зможе її відкрити. Коли Боб отримує коробку, він може відкрити її своїм ключем і отримати повідомлення від Аліси. Щоб відправити секретну відповідь, Боб кладе своє секретне повідомлення в коробку разом зі своїм відкритим замком і блокує коробку замком Аліси. Боб відправляє закриту коробку назад Алісі.

Наприклад, Аліса запитує і отримує відкритий ключ Боба. Аліса використовує відкритий ключ Боба для шифрування повідомлення з використанням узгодженого заздалегідь алгоритму. Аліса відправляє зашифроване повідомлення Бобу, а Боб використовує свій закритий ключ для дешифрування повідомлення.

# Процес асиметричного шифрування

Асиметричне шифрування, також відоме як шифруванням з відкритим ключем, для шифрування використовує ключ, який відрізняється від ключа для дешифрування. Злочинець не може в прийнятні терміни обчислити ключ дешифрування, знаючи ключ шифрування і навпаки.

Якщо Аліса і Боб обмінюються секретними повідомленнями за допомогою шифрування з відкритим ключем, вони використовують асиметричний алгоритм. На цей раз Боб і Аліса не обмінюються ключами до відправки секретних повідомлень. Замість цього у Боба і Аліси є окремі замки з відповідними ключами. Якщо Аліса надсилає секретне повідомлення Бобу, вона має спочатку зв'язатися з ним і попросити його надіслати свій відкритий замок. Боб надсилає замок, але зберігає свій ключ. Коли Аліса отримує замок, вона пише своє секретне повідомлення і вкладає його в маленьку коробку. В ту ж коробку вона кладе свій відкритий замок, але залишає у себе свій ключ. Потім вона замикає коробку замком Боба. Коли Аліса закриє коробку, вона більше не зможе її відкрити, тому що у неї немає ключа до цього замку. Вона відправляє коробку Бобу, і, поки відправлення проходить через поштову систему, ніхто не зможе її відкрити. Коли Боб отримує коробку, він може відкрити її своїм ключем і отримати повідомлення від Аліси. Щоб відправити секретну відповідь, Боб кладе своє секретне повідомлення в коробку разом зі своїм відкритим замком і блокує коробку замком Аліси. Боб відправляє закриту коробку назад Алісі.

Наприклад, Аліса запитує і отримує відкритий ключ Боба. Аліса використовує відкритий ключ Боба для шифрування повідомлення з використанням узгодженого заздалегідь алгоритму. Аліса відправляє зашифроване повідомлення Бобу, а Боб використовує свій закритий ключ для дешифрування повідомлення.