Для забезпечення секретності інформації використовують шифри – систему оборотних перетворень, залежних від деякого секретного параметру (ключа). Шифри поділяються на симетричні та асиметричні. Симетричні шифри – шифри в яких для шифрування та дешифрування даних використовується один й той самий секретний ключ. В асиметричних шифрах використовується два ключа – відкритий та закритий. Відкритий ключ може побачити хто завгодно, а секретний доступний тільки сторонам передачі даних. Ідея криптографічних систем з відкритим ключем дуже схожа на ідею однобічних функцій, тобто таких функцій , що по відомому просто знайти , але при відомому значенні функції неможливо знайти значення . Сама однобічна функція безпечна у використовуванні, бо за допомогою неї можна зашифрувати повідомлення, але розшифрувати неможливо. Тому створюються функції, які неможна розшифрувати, але маючи секретне значення це зробити можливо. Також шифри можна поділити на блочні та потокові. Потокові шифри – симетричні шифри, кожен символ яких перетворюється в символ шифротексту, керуючись не тільки ключем, але й положенням символу у відкритому тексті. Блочні шифри – різновид симетричних шифрів, які працюють із групами біт фіксованої довжини – блоками. Далі шифри працюють із кожним блоком окремо (іноді використовуючи результат обробки минулого блоку).

Алгоритми асиметричного шифрування розглядатися не будуть, бо в їх роботі мають учать якість випадкові значення, наприклад великі випадкові прості числа. Далі на прикладі одного з алгоритмів буде показано чому працювати із випадковими числами – погана ідея для чату.