Алгоритм ElGamal:

Алгоритм ElGamal є криптографічним алгоритмом, який використовується для забезпечення конфіденційності повідомлень та обміну ключами в криптографії на основі відкритого ключа. Він був названий на честь свого автора, криптографа Тахера Ель-Гамаля.

Алгоритм ElGamal використовує математичні властивості теорії чисел та складність обчислення для забезпечення безпеки. Його використання передбачає два ключі: публічний ключ та приватний ключ.

Процес шифрування повідомлення за допомогою алгоритму ElGamal включає наступні кроки:

Виберіть публічний ключ і приватний ключ.

Перетворіть повідомлення у числове значення, яке є меншим за певне число, відоме як модуль.

Застосуйте математичні обчислення, використовуючи публічний ключ та отримане числове значення повідомлення, щоб згенерувати шифрований текст.

Отриманий шифрований текст може бути відправлений отримувачу.

Процес розшифрування зашифрованого тексту з використанням алгоритму ElGamal включає такі кроки:

Отримайте зашифрований текст від відправника.

Застосуйте математичні обчислення, використовуючи свій приватний ключ та отриманий зашифрований текст, щоб відновити початкове числове значення повідомлення.

Поверніть початкове числове значення в його текстову форму.

Алгоритм ElGamal є безпечним, оскільки підтримується складність обчислень і пов'язані з нею математичні проблеми. Використовуючи цей алгоритм, можна забезпечити конфіденційність повідомлень та безпеку обміну ключами між відправником та отримувачем.

Система PGP (Pretty Good Privacy):

PGP є системою шифрування та цифрового підпису, розробленою для забезпечення безпеки комунікацій, конфіденційності та автентифікації даних. Вона широко використовується для захисту електронної пошти, файлів і передачі повідомлень через Інтернет.

Система PGP використовує комбінацію асиметричного та симетричного шифрування для забезпечення безпеки даних. Основна ідея полягає в тому, що кожен користувач має свою пару ключів: приватний ключ і публічний ключ.

Процес використання системи PGP включає наступні кроки:

Генерація ключів:

Користувач генерує свою пару ключів, яка складається з приватного ключа (який залишається в таємниці) та публічного ключа (який може бути поширений).

Публічний ключ слугує для шифрування повідомлень, а також для перевірки цифрового підпису.

Шифрування повідомлення:

Відправник отримує публічний ключ отримувача і використовує його для шифрування повідомлення.

Зашифроване повідомлення відправляється отримувачу.

Розшифрування повідомлення:

Отримувач використовує свій приватний ключ для розшифрування отриманого зашифрованого повідомлення.

Цифровий підпис:

Відправник може також створити цифровий підпис для повідомлення, використовуючи свій приватний ключ.

Отримувач може перевірити цифровий підпис, використовуючи публічний ключ відправника, щоб підтвердити автентичність повідомлення.

Система PGP використовує надійні алгоритми шифрування та цифрового підпису, такі як RSA або ElGamal, для забезпечення безпеки комунікацій. Вона дозволяє користувачам здійснювати конфіденційну комунікацію та підтверджувати автентичність даних, забезпечуючи високий рівень безпеки.

цфвфцвфцв