Точоний Володимир ІПС-32

Варіант 8

Завдання 1 (Algorithm EIGamal)

Алгоритм шифрування ElGamal — це метод відкритого ключа, заснований на протоколі узгодження ключів Діффі-Хеллмана. Його описав Тахер Ельгамал у 1985 році. Система шифрування ElGamal відома як імовірнісна, тобто вона генерує різні зашифровані тексти для одного повідомлення відкритого тексту, що додає додатковий рівень безпеки.

Він включає три основні кроки:

1. Генерація ключа

Алгоритм починається з вибору великого простого числа p і основи g, яка є первісним коренем за модулем p. Первісний корінь за модулем p — це число g, степені якого конгруентні p - 1 різним цілим числам за модулем p. Це просто означає, що g може генерувати p-1 різних чисел, якщо звести до степеня цілих чисел від 1 до p-1.

Потім приватний ключ a вибирається з {1, ..., p-2}, а відповідний відкритий ключ A обчислюється як A = g^a mod p.

1. Шифрування

Для шифрування повідомлення M вибирається випадкове число k з {1, ..., p-2}. Зашифрований текст C є парою (C1, C2), де C1 = g^k mod p і C2 = M \* A^k mod p.

1. Дешифрування

Щоб розшифрувати зашифрований текст C = (C1, C2), спочатку обчислюється s = C1^a mod p. Початкове повідомлення M потім відновлюється шляхом обчислення M = C2 \* (s^-1) mod p.

Безпека алгоритму шифрування ElGamal полягає в складності проблеми дискретного логарифмування. Враховуючи p, g і g^a mod p, обчислювально важко визначити a. Це «важка» проблема, яка забезпечує основу для безпеки ElGamal і кількох інших криптосистем з відкритим ключем.

Завдання 2 (PGP System)

Система шифрування Pretty Good Privacy (PGP) використовує комбінацію симетричних і асиметричних алгоритмів шифрування, а також хешування та цифрові підписи для забезпечення цілісності. Ось- пояснення процесу:

Стиснення:

Оригінальне повідомлення стискається, щоб заощадити місце та посилити криптографічний захист.

Шифрування з симетричним ключем:

Повідомлення шифрується за допомогою алгоритму симетричного ключа. Для цього генерується одноразовий сеансовий ключ. Найчастіше використовуються такі алгоритми, як AES (Advanced Encryption Standard) або IDEA (International Data Encryption Algorithm). Це блочні шифри, які шифрують дані в блоках фіксованого розміру (128 біт для AES, 64 біти для IDEA).

Шифрування відкритим ключем:

Потім ключ сеансу з попереднього кроку шифрується за допомогою відкритого ключа одержувача. Зазвичай це робиться за допомогою асиметричного алгоритму шифрування, наприклад RSA (Rivest–Shamir–Adleman) або ElGamal. Ці алгоритми засновані на таких математичних задачах, як розкладання великих цілих чисел на множники або проблема дискретного логарифмування, які забезпечують односторонню функцію, необхідну для шифрування з відкритим ключем.

Цифровий підпис:

Хеш вихідного повідомлення створюється за допомогою криптографічної хеш-функції (наприклад, SHA-256), потім цей хеш шифрується за допомогою закритого ключа відправника, створюючи цифровий підпис. Одержувач, використовуючи відкритий ключ відправника, може розшифрувати хеш і порівняти його з хешем отриманого повідомлення, підтверджуючи цілісність і походження повідомлення.