Котлярова Анна ІПС-32

Варіант 5

1. **DSA (Digital Signature Algorithm)** є криптографічним алгоритмом підпису, що використовується для забезпечення автентичності, цілісності та невідмовності повідомлень.

DSA базується на математичних проблемах, таких як обчислення дискретного логарифму в групі простих чисел. В основі DSA лежить принцип використання публічного та приватного ключів. Кожен користувач генерує пару ключів - приватний ключ, який він тримає в секреті, і публічний ключ, який він розповсюджує.

Для створення цифрового підпису за допомогою DSA користувач складає повідомлення, згенерований хеш-код цього повідомлення та свій приватний ключ. За допомогою математичних операцій, таких як піднесення до степеня та взяття залишку від ділення, обчислюється підпис. Цей підпис разом з повідомленням може бути переданий отримувачу.

Отримувач, хто має доступ до публічного ключа користувача, може перевірити автентичність повідомлення. Він обчислює хеш-код отриманого повідомлення і порівнює його з використаним раніше хеш-кодом, який був отриманий з підпису і публічного ключа. Якщо хеш-коди співпадають, то повідомлення не було змінено після підпису, і підпис вважається дійсним.

1. **AES (Advanced Encryption Standard)** - це симетричний алгоритм шифрування, який широко використовується для захисту конфіденційної інформації. Він був обраний Національним інститутом стандартів і технологій США (NIST) у 2001 році як наступник стандарту шифрування даних (DES) через його більшу безпеку.

AES операціонує над блоками даних і підтримує довжини ключів 128, 192 і 256 біт. Він використовує структуру заміно-перестановки (SPN), яка складається з кількох раундів перетворень для забезпечення шифрування і дешифрування. Кількість раундів варіюється залежно від довжини ключа: 10 раундів для 128-бітових ключів, 12 раундів для 192-бітових ключів і 14 раундів для 256-бітових ключів.

Алгоритм використовує декілька операцій над ключем, включаючи заміну, перестановку та змішування, для досягнення поняття заплутаності (confusion) та розсіювання (diffusion), що є важливими властивостями для криптографічної безпеки. AES використовує комбінацію заміночних таблиць (S-блоків), лінійного перетворення, відомого як крок ShiftRows, змішування байтів та інших операцій для шифрування і дешифрування блоків даних.

AES є одним з найпоширеніших алгоритмів шифрування і застосовується в різних областях, включаючи захист інформації в комп'ютерних системах, мережеву безпеку, електронну комерцію та забезпечення конфіденційності даних.