Hash function MD5

Алгоритм MD5 (Message Digest Algorithm 5) є одним з найпоширеніших алгоритмів хешування, який використовується для створення 128-бітного хешу з вхідного повідомлення.

Алгоритм складається з наступних кроків:

- В рядок пишеться одиничний байт, далі він доповнюється бітами таким чином, щоб його довжина була кратною 512. Також додаються біти, що кодують початкову довжину повідомлення.
- Далі в рядок дописується 64-бітове представлення довжини вихідного повідомлення.
- Повідомлення розбивається на блоки по 512 бітів. Зазвичай ініціалізуються чотири буфери що складаються із чотирьох констант.
- Кожен блок проходить 4 раунди з 16 операторів. Всі оператори однотипні і мають вигляд: [abcd k s i], визначений як $a = b + ((a + Fun(b,c,d) + X[k] + T < i >) <<< s)$ де X - блок даних, а T[1..64] - 64-елементна таблиця, побудована наступним чином: $T[i] = int(4294967296 * |sin(i)|)$, s - циклічний зсув вліво на s біт отриманого 32-бітного аргументу.
- Після обчислення для всіх блоків даних, отримуємо кінцевий хеш у регістрах A B C D. Якщо вивести слова у зворотному порядку DCBA, то отримаємо MD5 хеш.

Алгоритм AES

AES – це симетричний алгоритм шифрування. В нашому випадку він працює на 128 байтах.

Основні кроки алгоритму AES наступні:

- Вхідне повідомлення розбивається на блоки в матрицю 4 на 4.
- Ключ проходить процес розширення для створення набору раундових ключів і додається до повідомлення.

- SubBytes: Кожний байт вхідного блока даних замінюється на відповідний байт з таблиці Rijndael. Цей крок забезпечує нелінійність та заплутує процес шифрування.
- ShiftRows: Рядки блока даних циклічно зсуваються. У першому рядку зсув не виконується. У другому рядку байти зсуваються на одну позицію вліво. Третій і четвертий рядки зсуваються на дві і три позиції відповідно. Цей крок забезпечує розсіювання та гарантує, що вихідні біти залежать від кількох вхідних бітів.
- MixColumns: Кожний стовпець блока даних множиться на фіксовану матрицю, що перетворює стовпці. Цей крок забезпечує подальше розсіювання та збільшує складність шифрування.
- AddRoundKey: Поточний раундовий ключ, отриманий з розширення ключа, бітовою операцією XOR комбінується з блоком даних. Цей крок поєднує поточний ключовий матеріал з даними, щоб зробити кожен раунд унікальним.

Вищезазначені кроки (SubBytes, ShiftRows, MixColumns та AddRoundKey) повторюються протягом кількох раундів, залежно від довжини ключа. Кількість раундів становить 10 для ключа довжиною 128 біт, 12 для ключа довжиною 192 біти і 14 для ключа довжиною 256 біт.