Хэширование паролей

МАКСИМ БЕЛЯКОВ 10В

Что такое хэш?

- **Хэш** или хэш код – это уникальное имя файла, не зависящее от того, как его назвали вы

Что такое хэширование?

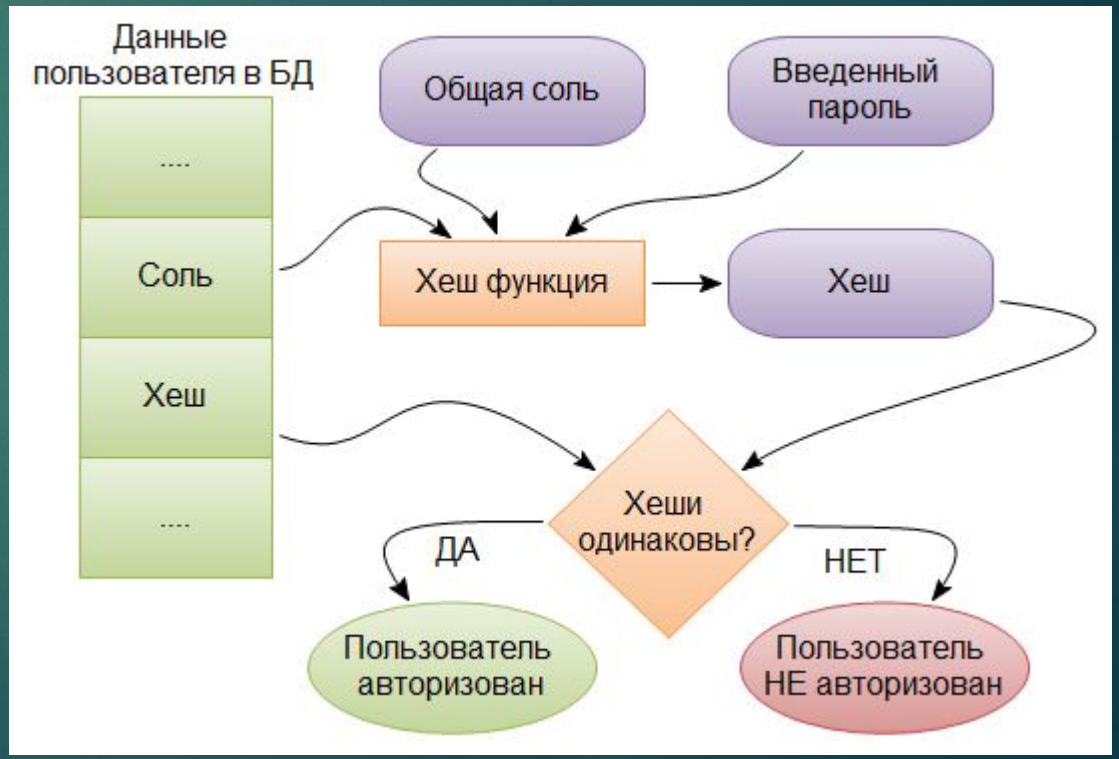
- **Хеширование** или хэширование — преобразование массива входных данных произвольной длины в (выходную) битовую строку установленной длины, выполняемое определённым алгоритмом.

Функцией хеширования (функцией перемешивания, функцией рандомизации) называется **функция,** обеспечивающая **отображение пространства ключей** K **в пространство записей** A (т. е. **преобразование ключа в адрес записи**):
$h: K \rightarrow A$;
$a = h(k)$, где a – адрес, k – ключ.

Идеальной хеш-функцией является такая функция, которая для любых двух неодинаковых ключей дает неодинаковые адреса: $k1 \neq k2 \rightarrow h(k1) \neq h(k2)$. Ей соответствует таблица прямого доступа.

Соль

- **Соль** (также ***модификатор***) — строка данных, которая передаётся хеш-функции вместе с паролем.
- Главным образом используется для защиты от перебора по словарю и атак с использованием **радужных таблиц**, а также сокрытия одинаковых паролей. Однако, соль не может защитить от полного перебора каждого отдельного пароля.



Радужная таблица

- **Радужная таблица** — специальный вариант таблиц поиска для обращения **криптографических хеш-функций**, использующий механизм **разумного компромисса** между временем поиска по таблице и занимаемой памятью.

Современные алгоритмы шифрования

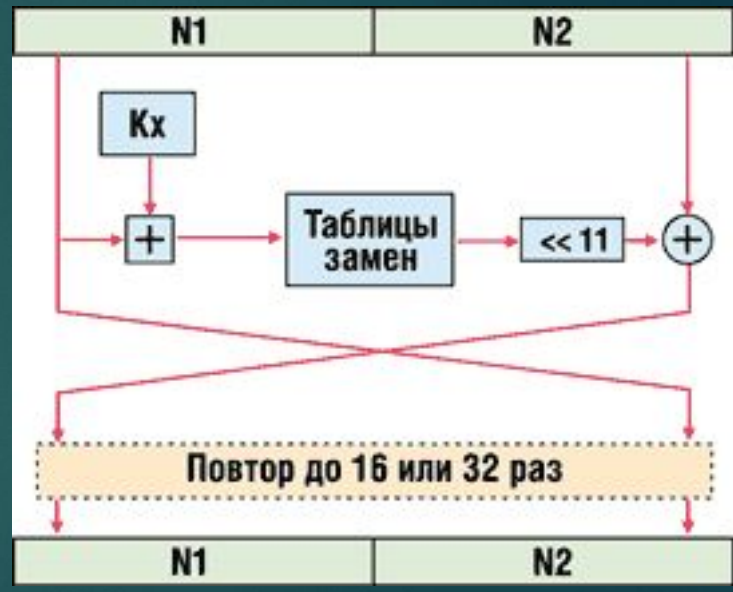
- **Симметричными алгоритмами** шифрования используется один и тот же ключ для шифрования и дешифрования информации.

  Асимметричными алгоритмами используется два ключа – один для шифрования, другой – для дешифрования.

  Ключ шифрования представляет собой случайную или специальным образом созданную последовательность бит, которая является переменным параметром алгоритма шифрования.

Стандарт ГОСТ 28147-89(симметричный)

- Алгоритм, определяемый ГОСТ 28147-89, имеет длину ключа шифрования 256 бит. Он шифрует информацию блоками по 64 бит (такие алгоритмы называются блочными), которые затем разбиваются на два субблока по 32 бит (N1 и N2). Субблок N1 обрабатывается определенным образом, после чего его значение складывается со значением субблока N2 (сложение выполняется по модулю 2, т. е. применяется логическая операция XOR - "исключающее или"), а затем субблоки меняются местами. Данное преобразование выполняется определенное число раз ("раундов"): 16 или 32 в зависимости от режима работы алгоритма. В каждом раунде выполняются две операции.



Стандарт AES(Rijndael)(симметричный)

- В отличие от отечественного стандарта шифрования, алгоритм Rijndael представляет блок данных в виде двухмерного байтового массива размером 4X4, 4X6 или 4X8 (допускается использование нескольких фиксированных размеров шифруемого блока информации). Все операции выполняются с отдельными байтами массива, а также с независимыми столбцами и строками.
  Алгоритм Rijndael выполняет четыре преобразования: BS (ByteSub) - табличная замена каждого байта массива; SR (ShiftRow) - сдвиг строк массива. При этой операции первая строка остается без изменений, а остальные циклически побайтно сдвигаются влево на фиксированное число байт, зависящее от размера массива.

Алгоритм RSA(асимметричный)

- Основной параметр алгоритма RSA - модуль системы N, по которому проводятся все вычисления в системе, а N = P*Q (P и Q - секретные случайные простые большие числа, обычно одинаковой размерности).
  Секретный ключ k2 выбирается случайным образом и должен соответствовать следующим условиям: 1<k2<F(N) ; НОД(k2, F(N))=1, где НОД - наибольший общий делитель, т. е. k1 должен быть взаимно простым со значением функции Эйлера F(N), причем последнее равно количеству положительных целых чисел в диапазоне от 1 до N, взаимно простых с N, и вычисляется как *F(N) = (P - 1)*(Q - 1)*.