ОПИСАНИЕ

crypt() — функция шифрования пароля. Она основана на алгоритме стандарта шифрования данных (Data Encryption Standard) с различными расширениями, нацеленными (помимо прочего) на усложнение задачи поиска ключа при помощи специального оборудования.

key — задаваемый пользователем пароль.

salt (соль) — двухсимвольная строка, выбираемая из набора [**a-zA-Z0-9./**]. Эта строка используется для направления алгоритма по одному из 4096-и путей.

Если взять младшие 7 битов каждого из первых 8 символов *key*, то получается 56-битный ключ. Этот ключ используется для многократного шифрования константной строки (обычно строки, состоящей из символов «0»). Возвращаемое значение — указатель на зашифрованный пароль, серия из 13-и печатных ASCII-символов (первые два символа содержат *salt*). Возвращаемое значение указывает на статические данные, которые перезаписываются при каждом вызове.

Предупреждение: количество ключей равно 2**56 т. е. существует 7.2e16 возможных вариантов. Полный перебор этого множестве возможен с помощью большого количества параллельных компьютеров. Программное обеспечение, такое, как **crack** (1), способно отыскать часть ключей из этого множества, обычно используемых людьми для создания пароля. Поэтому в качестве пароля не стоит, как минимум, использовать простые слова и имена. Рекомендуется использовать программу **passwd** (1), которая проверяет сложность пароля уже на стадии ввода.

Алгоритм DES имеет некоторые особенности, которые не позволяют использовать интерфейс **crypt**() для чего-то кроме аутентификации пользователя по паролю. Если вы планируете использовать интерфейс **crypt**() в проекте шифрования, то лучше не делайте этого. Вместо этого возьмите хорошую книгу по шифрованию или одну из общедоступных библиотек DES.

Функция **crypt_r**() является реентерабельной версией **crypt**(). Для учёта и хранения результата в ней используется структура, на которую указывает *data*. Перед первым вызовом **crypt_r**() требуется выделить место под структуру и присвоить *data->initialized* значение 0.

ВОЗВРАЩАЕМОЕ ЗНАЧЕНИЕ