[How to generate a /etc/shadow compatible password for Ubuntu](https://serverfault.com/questions/259722/how-to-generate-a-etc-shadow-compatible-password-for-ubuntu-10-04)

If salt is a character string starting with the characters "$id$" followed by

a string terminated by "$":

$id$salt$encrypted

then instead of using the DES machine, id identifies the encryption method

used and this then determines how the rest of the password string is

interpreted. The following values of id are supported:

ID | Method

---------------------------------------------------------

1 | MD5

2 | Blowfish (not in mainline glibc; added in some Linux distributions)

5 | SHA-256 (since glibc 2.7)

6 | SHA-512 (since glibc 2.7)

So $5$salt$encrypted is an SHA-256 encoded password and $6$salt$encrypted is

an SHA-512 encoded one.

"salt" stands for the up to 16 characters following "$id$" in the salt. The

encrypted part of the password string is the actual computed password. The

size of this string is fixed:

MD5 | 22 characters

SHA-256 | 43 characters

SHA-512 | 86 characters

The characters in "salt" and "encrypted" are drawn from the set [a-zA-Z0-9./].

In the MD5 and SHA implementations the entire key is significant (instead of

only the first 8 bytes in DES).