

MD5 Hashes

```
098f6bcd4621d373cade4e832627b4f6
```

MD5 hashes are 32 characters in length when represented in hexadecimal format. Within a shadow file, the prefix \$1\$ is used.

SHA1 Hashes

```
a94a8fe5ccb19ba61c4c0873d391e987982fbbd3
```

SHA1 hashes are 40 characters in length when represented in hexadecimal format. Within a shadow file, the prefix \$sha1\$ is used.

SHA256 Hashes

```
9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08
```

SHA256 hashes are 64 characters in length when represented in hexadecimal format. Within a shadow file, the prefix \$5\$ is used.

SHA512 Hashes

```
ee26b0dd4af7e749aa1a8ee3c10ae9923f618980772e473f8819a5d4940e0db27ac185f8a0e1d5f84f88bc887fd67b143732c304cc5fa9ad8e6f57f50028a8ff
```

SHA512 hashes are 128 characters in length when represented in hexadecimal format. Within a shadow file, the prefix \$6\$ is used.

Bcrypt Hashes

```
$2a$10$N9qo8uLOickgx2ZMRZoMyeIjZAgcf17p92ldGxad68LJZdL17lhWy
```

Within a shadow file, the prefix \$2a\$ or \$2b\$ or \$2y\$ or \$2y\$ within a hash string indicates that the hash is a bcrypt hash in modular crypt format. The rest of the string includes the cost parameter (128 bit Radix-64 encoded as 22 characters), and 184 bits of the resulting hash value (Radix-64 encoded as 31 characters).

In the above example, \$2a\$ indicates that the hash is bcrypt; the \$10\$ indicates that 2^{10} expansion rounds were used, and the salt is the next 22 characters. The remaining 31 characters are the hash itself.

Hashes by Length

Hash Length Bytes (bits)	Hash Length (chars in Hex)	Likely Hashes
16 (128)	32	MD2, MD4, MD5, RIPEMD
20 (160)	40	SHA1
24 (192)	48	Tiger
32 (256)	64	SHA256, GOST
64 (512)	128	SHA512

Hashes by Prefix (in Shadow Files)

Prefix	Hash
\$1\$	MD5crypt
\$2\$, \$2a\$, \$2b\$, \$2x\$, \$2y\$	Blowfish-based crypt (bcrypt)
\$sha1\$	SHA1crypt
\$5\$	SHA256crypt
\$6\$	SHA512crypt