How to create Bitcoin Address

The correct way to create a Bitcoin address is to use well tested, open source, peer reviewed wallet software. Manually handling keys has resulted in funds loss over and over again. Unlike other centralized systems losses in Bitcoin are usually unrecoverable.

Here is a brief overview of how address generation works, for informational purposes:

0 - Having a private ECDSA key

```
18e14a7b6a307f426a94f8114701e7c8e774e7f9a47e2c2035db29a206321725
```

1 - Take the corresponding public key generated with it (33 bytes, 1 byte 0x02 (y-coord is even), and 32 bytes corresponding to X coordinate)

```
0250863ad64a87ae8a2fe83c1af1a8403cb53f53e486d8511dad8a04887e5b2352
```

2 - Perform SHA-256 hashing on the public key

```
0b7c28c9b7290c98d7438e70b3d3f7c848fbd7d1dc194ff83f4f7cc9b1378e98
```

3 - Perform RIPEMD-160 hashing on the result of SHA-256

```
f54a5851e9372b87810a8e60cdd2e7cfd80b6e31
```

4 - Add version byte in front of RIPEMD-160 hash (0x00 for Main Network)

```
00f54a5851e9372b87810a8e60cdd2e7cfd80b6e31
```

(note that below steps are the Base58Check encoding, which has multiple library options available implementing it)
5 - Perform SHA-256 hash on the extended RIPEMD-160 result

```
ad3c854da227c7e99c4abfad4ea41d71311160df2e415e713318c70d67c6b41c
```

6 - Perform SHA-256 hash on the result of the previous SHA-256 hash

```
c7f18fe8fcbed6396741e58ad259b5cb16b7fd7f041904147ba1dcffabf747fd
```

7 - Take the first 4 bytes of the second SHA-256 hash. This is the address checksum

```
c7f18fe8
```

8 - Add the 4 checksum bytes from stage 7 at the end of extended RIPEMD-160 hash from stage 4. This is the 25-byte binary Bitcoin Address.

```
00f54a5851e9372b87810a8e60cdd2e7cfd80b6e31c7f18fe8
```

9 - Convert the result from a byte string into a base58 string using Base58Check encoding. This is the most commonly used Bitcoin Address format

```
1PMycacnJaSqwwJqjawXBErnLsZ7RkXUAs
```