**Signing of the kernel eBPF program (i.e., byte code)**

 Steps to get signature:

Convert a bytecode file into some hash using hashing algorithms.

By Using hash and Private key we can generate signatures using signing algorithms.

 If a user has

 1. File

 2. Signature

 3. Public Key

Then he can verify that a file is authentic.

Why are we using hashing ?

 We are using hashing Because if we change the input slightly,the output hash changes completely.

Hashing Algorithms

 1.SHA 256 (Secure Hash Algorithm)

 SHA 256 is one of the strongest hash functions available.

 **SHA-256 is not a secure password hashing algorithm**

2. MD5 (message-digest algorithms)

3. Base32 & Base64

Signing Algorithms

1. DSA **(Digital Signature Algorithm)**
2. RSA (**Rivest-Shamir-Adleman)**
3. Ecdsa ( Elliptic Curve Digital Signature Algorithm)