

**Exemplul 1.** de scriere a unei aplicatii care include functia SHA1 oferita de mediul criptografic de dezvoltare **openssl** pe sisteme Debian/Linux. Procedura este :

1. se instaleaza biblioteca **libssl-dev**

```
#apt-get install libssl-dev
```

2. se editeaza fisierul sursa incluzand apelul functiei SHA1(.) cu prototipul specificat in exemplul de mai jos.
3. se compileaza fisierul sursa cu comanda:

```
$ gcc <filename.c> -lssl -o <output_filename>
```

### Codul sursa

```
#include <openssl/sha.h>
#include <stdio.h>

int main(){
    unsigned char ibuf[] = "Hello World!"
    unsigned char obuf[20];

    SHA1(ibuf, strlen(ibuf), obuf);
    for(int i = 0; i < 20; i++) printf("%02x ", obuf[i]);
    printf("\n");
    return 0;
}
```

**NOTA:** prototipul functiei SHA1 este urmatorul (/usr/include/openssl/sha.h):

```
unsigned char *SHA1(const unsigned char *, size_t, unsigned char)
```

- Valoarea intoarsa de functie este un pointer la valoarea hash.
- **Param\_1:** este pointer la datele de intrare;
- **Param\_2:** precizeaza lungimea datelor de intrare in octeti;
- **Param\_3:** este un pointer la spatiul de memorie unde va fi copiat rezultatul