Project on Cryptography

Section1--Document

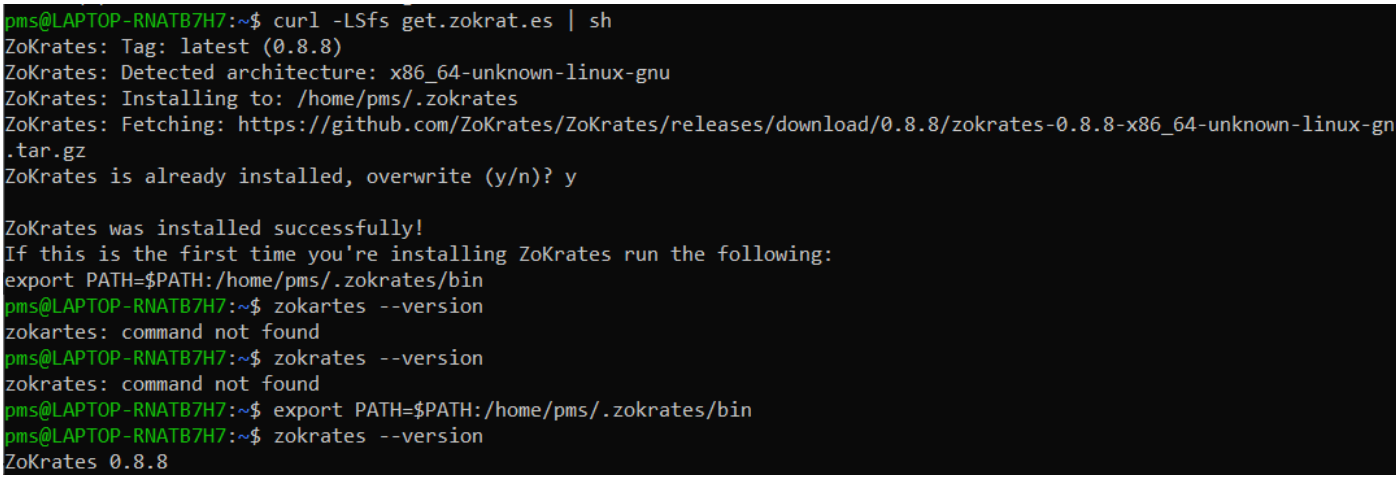
Team: Code clash

Objective:

To demonstrate creating and verifying a Zero Knowledge Proof (ZKP) to prove knowledge of a SHA256 hash pre-image without revealing the secret, highlighting ZKPs' use in secure authentication.

Execution of commands in terminal

Installing zokrates



Compilation stage

```
pms@LAPTOP-RNATB7H7:~$ ls
input.txt  sha256.zok
pms@LAPTOP-RNATB7H7:~$ zokrates compile -i sha256.zok
Compiling sha256.zok

Compiled code written to 'out'
Number of constraints: 48886
pms@LAPTOP-RNATB7H7:~$ ls
abi.json  input.txt  out  out.r1cs  sha256.zok
```

Setup phase where compiled code is used to generate proving & verification keys.

```
pms@LAPTOP-RNATB7H7:~$ zokrates compute-witness -a 0 0 0 1129529685 285551088474675990519063
903894825317322 192916772619636604765586326883831074249
Computing witness...
Witness file written to 'witness'
pms@LAPTOP-RNATB7H7:~$ ls
abi.json   out       out.wtns     sha256.zok        witness
input.txt  out.r1cs  proving.key  verification.key
pms@LAPTOP-RNATB7H7:~$ zokrates generate-proof
Generating proof...
Proof written to 'proof.json'
pms@LAPTOP-RNATB7H7:~$
```

```
Performing verification...
PASSED
```