# STUDY ON HASH FUNCTION

TEAM NAME : INNOVATORS

Aldrin R J 22BME007
[Email address]

## STATEMENT

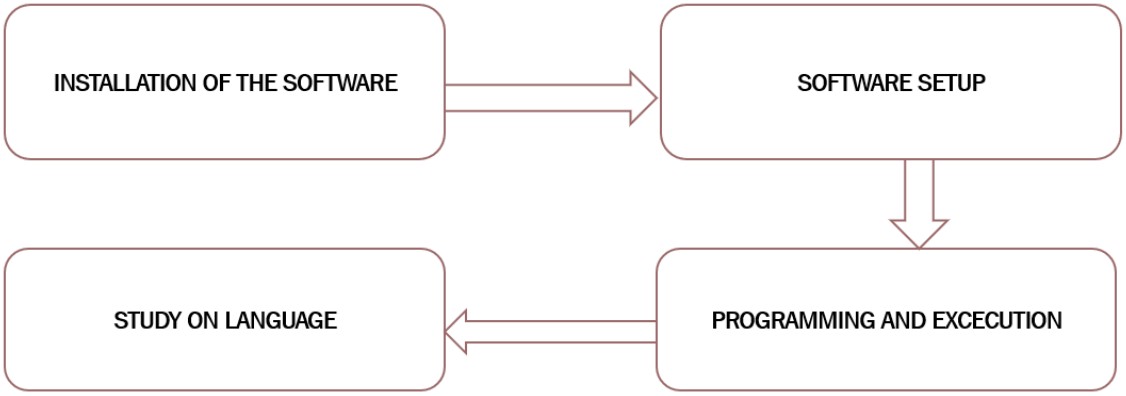
- In the second section various functions of hash functions were to be studied and to secure the data from ethical hackers

## OBJECTIVE

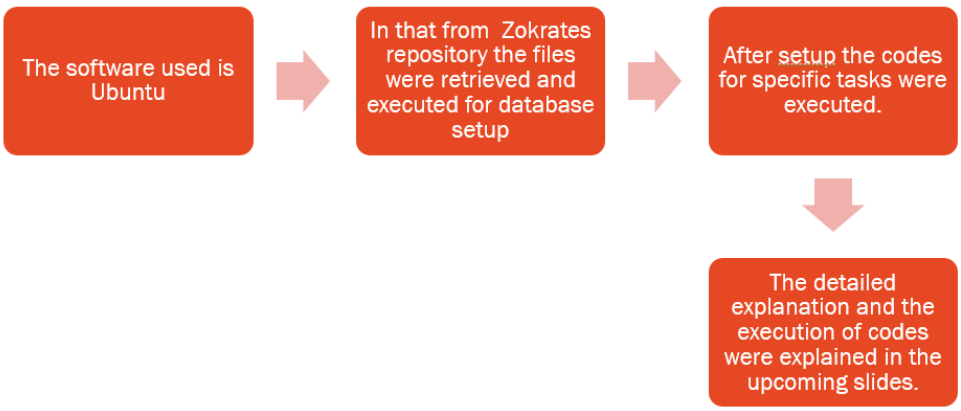
The main objective of this is to study is to know about various hash functions.

To execute the code and learn the language sucessfully

# FLOW DIAGRAM




# INSTALLATION



**GITHUB ZOKRATES REPOSITORY PROGRAAMING LEARNING:**

dark64 merge staging

e75552b · 2 years ago History

Code Blame 8 lines (8 loc) · 181 Bytes

Raw

```
def main<N>(bool[N] bits) -> field {
    field mut out = 0;
    for u32 j in 0..N {
        u32 i = N - (j + 1);
        out = out + (bits[i] ? 2 ** j : 0);
    }
    return out;
}
```

ZoKrates / zokrates_stdlib / stdlib / utils / pack / bool / pack128.zok

dark64 change syntax in core and stdlib tests

Code Blame 8 lines (6 loc) · 158 Bytes

```
#pragma curve bn128

import "./pack" as pack;

// pack 128 big-endian bits into one field element
def main(bool[128] bits) -> field {
    return pack(bits);
}
```

ZoKrates / zokrates_stdlib / stdlib / utils / pack / bool / pack256.zok

dark64 change syntax in core and stdlib tests

Code Blame 10 lines (8 loc) · 312 Bytes

```
#pragma curve bn128

import "./pack" as pack;

// pack 256 big-endian bits into one field element
// Note: This is not a injective operation as `p` is smaller than `2**256 - 1` for bn128
// For example, `[0, 0,..., 0]` and `bits(p)` both point to `0`
def main(bool[256] bits) -> field {
    return pack(bits);
}
```

a

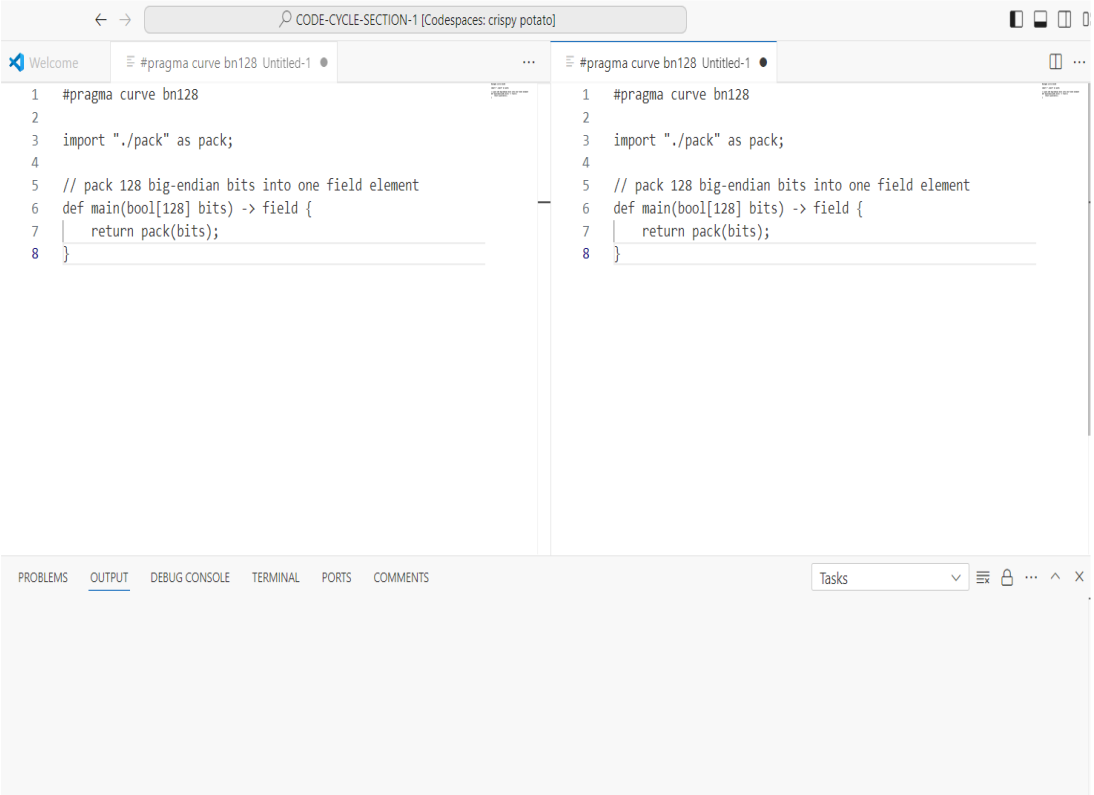
= 21267647932558653966532970558541271056

GENERATE HASH CLEAR

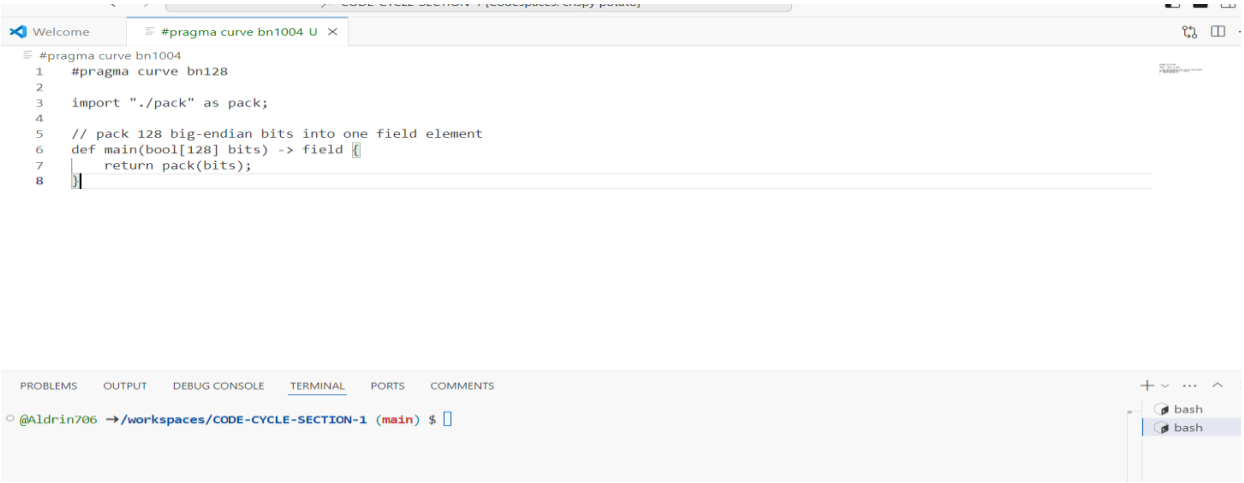
**SHA-512 OUTPUT:**

7c7e8842b312faeae9f981b8e746dab65a5ff76e31ecbd1d83125e955a516595070febaa02896aeddb8593967f8a7619fa85e4af277b6f90c713d617519fcdb3

ORIGINAL FLE SIZE : 128 bit




FILE SIZE CHANGE : 1004 bit



**CONCLUSION**:

- ❑Therefore the language was able to learn as much as possible
- ❑The various features were explored
- ❑The coding is executed
- ❑The file size was changed

Overall a clear overview about the programming language was able to learn in a fruitful manner.