**C Based VLSI Project Report**

------------------------------------------------------------------------------------

*Group Members:*

1. Madhurima Sen – 224101034 (Team Leader)
2. Pratik Manoj Rana - 224101040
3. Rohit Kumar – 224101043
4. Subhadeep Saha - 224101049
5. Lijo Raju - 224101033

------------------------------------------------------------------------------------

*Approach*

An oracle was given of C code in the form of an executable file and the locked code equivalent to that code was also provided.

There were 4 outputs to the code and 7 keys that locked all the outputs.

We performed SAT attack

*Method*

1. *First we have converted the given Obfuscated.c into an equivalent python function using Z3 library.*
2. *We are trying to find out Distinguishing Input Pattern(DIP) by checking the condition.*

*DIP is an input pattern for which if we give different keys to Obfuscated.c, it will generate more than 1 output, one of the outputs may be correct, rest are incorrect.*

1. *We are eliminating all the incorrect keys associated with that DIP and again performing step 2 till the unsat condition arrives.*

*Unsat condition implies there is no more DIP possible, thus we have got our correct keys. That means There is no such input possible, for which we are getting different output for different keys, that means, we have obtained possible correct keyset.*

*Tools used*

*Z3 library, python*

*Key values obtained*

key1 = 224238

key2 = 4

key3 = -43224

key4 = 34222

key5 = False

key6 = True

key7 = False