Project 1
Title: Verification of obfuscated program code
Note: This is a joint research project of Dr. ZhiQuan (George) Zhou and Dr. Willy Susilo of SITACS

Contact: Dr. ZhiQuan (George) ZHOU
Email: zhiquan@uow.edu.au
Phone: 4221 5399
Office: 3.208

Description:

The term "code obfuscation" refers to a set of transformations on program code, which preserve the same functionality of the original program while making the code very hard to read and understand. Code obfuscation protects the security and secrets of the original program by hiding the information and deterring the reverse engineering.

Here is an infamous example (for recreational purpose only) from the Internet:

```c
#include <stdio.h>
main(t,_,a){return!0<t?t<3?main(-79,-13,a+main(-87,1-_,
main(-86,0,a+1)+a)):1,t<_?main(t+1,_a):3,main(-94,-
27+t,a)&&=2?2<_3?
main(2,1l,"%s\d %d\n");9:16:t<0?t<72?main(_,t,
"@n'++,#'/*()w+/>\#cdnr/\{r/*de)+/*+,/w[%+/,w#q#n+,/#(1,+,/n(n+,/+ #n+,,/#\n;#q#n+,+/k#;*/r:'d'3,}w+K w'K:'+);dq#'1 \nq#'+d'K\x2f;+k#;q#'r)eKK\x2f;w'r)eKK{nl}'#;#q#n'}(#)#w}{)(nl)'+#n'#:d}rw 'i:#
}{nl}/n[n#; r[#w'r nc{nl}'#(1,+K (rw' iK{[{nl}'/w#q#n'wk nw' 
 iwk[KK{nl}!/w(%1#\#w' i: {nl}'*{q#'ldr'}{nlwb!/*de}'c 
';{nl}-{1}w'r')+/+/)#***}#nc','#nw'}/+kd'+e)+;#rdq#w! nr'/ ')
}+1{rl#'{n' ')# 
')++(!/})
:t<50?==a?putchar(31[a]):main(-65,_a+1):main(*a=''/)+t,_,a+1)
:0<t?main(2,2,"%s");a=''/'|main(0,main(-61,*a, 
!ek;dc i0bk'(q)-[w*t+n*r\#1,{}:\nuwloca-0\m .vpbks,fxntdCeghiry"},a+1);}"
```

Although unintelligible at first glance, it is a legal C program. If you compile and run it, you can see the program generates verses as follows:

On the first day of Christmas my true love gave to me ...
There are also programs known as obfuscators that may operate on source code, object code, or both, for the purpose of deterring reverse engineering.

An unsolved problem in code obfuscation, however, is the difficulty in deciding whether the obfuscated code is indeed equivalent to the original code. In this project, we will develop a methodology to address this issue by applying program testing and analysis techniques to cryptographic programs.

/******************************************
The Expected Outcome:
******************************************/

A methodology will be developed to apply software testing and analysis techniques to the verification of cryptographic programs. This research will produce quality research paper(s) in the interdisciplinary area of cryptography and software engineering. This project can be extended into honours, master by research or PhD projects.