```
                                          $==$';
                                         $;||$.|  $|;$_
            ='*$  (                   ^@(%_+&~~;#  ~~/.~~
        ;_);;.);;#)                 ;~~~~;_,.~~,.*  +,./|~
   ~;_);@—,   .;.);  ~             ~,./@@—__);@—);~~,.*+,.
 /|);;;~~@— ~~~~;;(),.            ;.,./@,./@,.;_~~@—););,.
 ;_);~~,./@,.;;;./@,./          |~~~~;#—(@—__@—__&$#%^';$__
  =''&'&';$___="''''"     |"$['$["|''%",';$~=("$___$__—$[''$__"|
             "$___"|         ("$___$__—$[.%")).("''"|"'$["|"'#").
       '/.*?&([^&]*)&.*/$'.++$=.("/‘‘"|"/$[‘"|"/#'").(";‘/[\\‘\\‘$__]//‘;"
       |";$[/[\\$[\\‘$__]//‘;"|";#/[\\\$\\.$__]//'").'@:=("@—","/.",
      "~~",";#",";;",";.",",.",");","()","*+","__","—(","/@",".%","/|",
       ";_");@:{@:}=$%..$#:;'.('‘'|"$["|'#')."/(..)(..)/".("‘‘‘"|"‘‘$["|
       '#("').'(($:{$'.$=.'}<<'.(++$=+$=).')|($:{$'.$=.'}))/'.("‘‘‘;"|
       "‘‘$[;"|"%'#;").("‘‘‘‘'$__"|"%$[‘‘"|"%&!,").${$[};‘$~$__>&$=‘;$_=
      '*$(^@(%_+&@—__~~;#~~@—;.;;,.(),./.,./|,.—();;#~~@—);;;,.;_~~@—,./.,
       ./@,./@~~@—);;;,.(),.;.~~@—,.,.,.;_,./@,.—();;#~~@—,.;_,./|~~@—,.
          ,.););@—@—__~~;#~~@—,.,.,.;_);~~~~@—);;;,.(),.*+);;#  ~~@—,
          ./|,.*+,.,.);;;);*+~~@—,.*+,.;;,.;.,./.~~@—,.,.,.;_)     ;~~~
            ~@—,.;;,.;.,./@,./.);*+,.;.,.;;@—__~~;#~~@—,.;;,.*     +);;
              #);@—,./@,./.);*+~~@—~~.%~~.%~~@—;;__,.  /.);;#@—    __@—
                __   ~~;;);/@;#.%;#/.;#—(@—__~~;;;.;_  ;#.%~~~~   ;;()
                      ,.;.,./@,.   /@,.;_~~@— );); ,.;_    );~~,./   @,.
                      ;;;./@,./|   ~~~~;#—(@— __,.,.,.     ;_);~~~  ~@
                       —~~());;    #);@—,./@,   .*+);;;      ~~@—~~
                       );~~);~~   *+~~@—);—(    ~~@—@—_       _~~@—
                       ~~@—);;    #,./@,.;.,     .;.);@       —~~@—;
                      #/.;#—(    ~~@—@—__       ~~@—~~        @—);@
                       —);~~,     .*+,./        |);;;~         ~@—~~
                        ;;;.;      _~~@—@      —__);.          %;#—(
                        @—__@      —__~~;#   ~~@—;;            ;#,.
                        ;_,..          %);@—,./@,              .*+,
                        ..%,            .;.,./|)               ;;;)
                        ;;#~             ~@—,.*+,.             ,.~~
                      @—);              *+,.;_);;.~           ~););
                      ~~,.;          .~~@—);~~,.;.,           ./.,.;
                      ;,.*+         ,./|,.);   ~~@—          );;;,.(
                    ),.*+);                                 ;#~~/|@—
                  __~~;#~~                                   $';$;;
```

Is There Hope for Obfuscation?

Jasvir Nagra

Department of Computer Science
University of Trento
jas@nagras.com

June, 2007

```
#!/usr/bin/perl

                                           $==$';
                                          $;||$.|  $|;$_
            ='*$  (                      ^@(%_+&~~;#  ~~/.~~
        ;_);;.);;#)                    ;~~~~;_,.~~,.*  +,./|~
   ~;_);@-,    .;.);  ~                ~,./@@-__);@-);~~,.*+,.
 /|);;;~~@-~~~~;;(),.                 ;.,./@,./@,.;_~~@-););,.
 ;_);~~,./@,.;;;./@,./              |~~~~;#-(@-__@-__&$#%^';$__
  ='`'&'&';$___="````"    |"$[`$["|'`%",';$~=("$___$__-$[``$__"|
             "$___"|         ("$___$__-$[.%")).("'`"|"'$["|"'#").
       '/.*?&([^&]*)&.*/$'.++$=.("/``"|"/$[`"|"/#'").(";`/[\\`\\`$__]//`;"
       |";$[/[\\$[\\`$__]//`;"|";#/[\\\$\\.$__]//'").'@:=("@-","/.",
      "~~",";#",";;",";.",",.",");","()","*+","__","-(","/@",".%","/|",
       ";_");@:{@:}=$%..$#:;'.('``|"$["|'#')."/(..)(..)/".("```"|"``$["|
       '#("').'(($:{$'.$=.'}<<'.(++$=+$=).')|($:{$'.$=.'}))/'.("```;"|
       "``$[;"|"%'#;").("````'$__"|"%$[``"|"%&!,").${$[};`$~$__>&$=`;$_=
      '*$(^@(%_+&@-__~~;#~~@-;.;;,.(),./.,./|,.-();;#~~@-);;;,.;_~~@-,./.,
       ./@,./@~~@-);;;,.(),.;.~~@-,.,.,.;_,./@,.-();;#~~@-,.;_,./|~~@-,.
          ,.););@-@-__~~;#~~@-,.,.,.;_);~~~~@-);;;,.(),.*+);;#  ~~@-,
          ./|,.*+,.,.);;;);*+~~@-,.*+,.;;,.;.,./.~~@-,.,.,.;_)    ;~~~
            ~@-,.;;,.;.,./@,./.);*+,.;.,.;;@-__~~;#~~@-,.;;,.*    +);;
              #);@-,./@,./.);*+~~@-~~.%~~.%~~@-;;__,.  /.);;#@-    __@-
                 __    ~~;;);/@;#.%;#/.;#-(@-__~~;;;.;_  ;#.%~~~~   ;;()
                      ,.;.,./@,.   /@,.;_~~@-  ););  ,.;_    );~~,./   @,.
                      ;;;./@,./|   ~~~~;#-(@- __,.,.,.     ;_);~~~  ~@
                       -~~());;    #);@-,./@,   .*+);;;      ~~@-~~
                       );~~);~~   *+~~@-);-(    ~~@-@-_       _~~@-
                       ~~@-);;    #,./@,.;.,      .;.);@      -~~@-;
                      #/.;#-(    ~~@-@-__        ~~@-~~        @-);@
                       -);~~,      .*+,./        |);;;~        ~@-~~
                        ;;;.;      _~~@-@      -__);.          %;#-(
                        @-__@      -__~~;#   ~~@-;;            ;#,.
                        ;_,..           %);@-,./@,             .*+,
                        ..%,              .;.,./|)             ;;;)
                        ;;#~               ~@-,.*+,.           ,.~~
                      @-);                *+,.;_);;.~         ~););
                      ~~,.;             .~~@-);~~,.;.,        ./.,.;
                      ;,.*+            ,./|,.);  ~~@-        );;;,.(
                    ),.*+);                                 ;#~~/|@-
                 __~~;#~~                                    $';$;;
```

```
    3.14159265358979323
  846264338327950288419
71    69      399
3     75      105
      82      097
      49      445
      92      307
     816      406
    286       208
  9986        2834    8
25342          11706798
2148             08651
```

Outline

- Obfuscation
  - Why RE-TRUST should be interested?
  - Why is obfuscation impossible?
  - Why all hope may not be lost (yet)?
- Amitabh's Talk
  - Extended notions of obfuscation
  - What kind of obfuscation is possible?

Why are we interested in obfuscation?

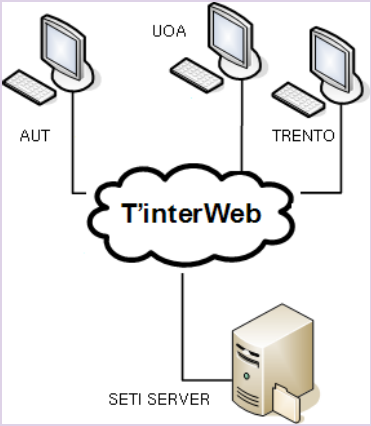
- Recreation
- Cryptography
- Distributed computing
- Protecting intellectual property (IP)

- Viruses
- Trojans
- Browser popups
- Digital Rights Management (DRM)

- RE-TRUST

RE-TRUST Problem

SETI@HOME



- Potential for clients to "cheat"
  - For ranking (Olli)
  - For marketing (MS)
  - For profit
- Solution
  - Embed a private-key in each client
  - Digitally sign responses
  - Hide the private key with obfuscation

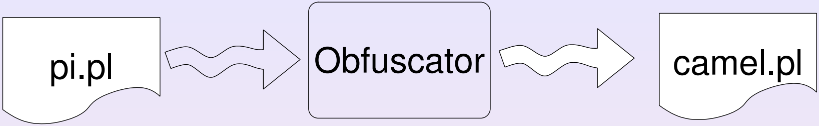
P != NP

Become Famous!

1. Develop perfect obfuscation
2. Use obfuscation to build a provable one-way function
3. One-way functions prove that P != NP ...

4. ??
5. Profit

What is an Obfuscator?



```
#!/usr/bin/perl
print "3.1415926..."
```

`Acme::Smirch`

`Acme::Smirch` converts any perl program into a version that has no letters or numbers

Collberg et al. Obfuscation

A program transformer $\mathcal{O}$ is an obfuscator if:

- $\mathcal{O}(P)$ is functionally the same as P
- The software engineering complexity $E(\mathcal{O}(P)) > E(P)$

Barak et al. Obfuscation

A program transformer $\mathcal{O}$ is an obfuscator if:

- $\mathcal{O}(P)$ is functionally the same as P

- $\mathcal{O}(P)$ is at most polynomially larger than P
- $\mathcal{O}(P)$ is at most polynomially slower than P

- $\mathcal{O}(P)$ is a virtual blackbox: All properties that you can determine from source-code access to $\mathcal{O}(P)$, you can also determine from oracle access to P with very high probability.

Why might obfuscation exist?

Pragmatic

- Program analysis
- Reverse engineering
- Software engineering

Theoretical

- Halting Problem
- Indistinguishability Problem
- Rice's Theorem

Understanding programs is already hard.

Perhaps we can make use of this hardness to build obfuscation.

Halting Problem

Problem

Given a program P...

...decide whether P halts when run with an input x.

```
$ java isValidPassword yellowblue
yes

$ java Pi
3.14159265358979323846264338327950288419716 93...
```

Halting Problem: Impossible

```
boolean halts ( String program, int arg ) {
  if ( something really clever ) {
    return true;
  else
    return false;
}

void sneaky ( String program, int arg ) {
  if ( halts ( program, int arg ) ) {
    // loop forever
    while ( true ) {}
  } else {
    // return immediately
    return;
  }
}
```

Note

The program sneaky needs the source of the halt method.

Indistinguishability Problem

Problem

Given programs P_1 and P_2

…decide whether P_1 and P_2 compute the same function.

Indistinguishability Problem: Impossible

Problem

Given programs P_1 and P_2

…decide whether P_1 and P_2 compute the same function.

```
void P1 ( ) {
  while ( true ) {}
}
```

```
void P2 ( ) {
  sneaky ( program );
}
```

Obfuscation Problem

?

Obfuscation

A program transformer $\mathcal{O}$ is an obfuscator if:

- $\mathcal{O}(P)$ is functionally the same as P

- $\mathcal{O}(P)$ is at most polynomially larger than P
- $\mathcal{O}(P)$ is at most polynomially slower than P

- $\mathcal{O}(P)$ is a virtual blackbox: All properties that you can determine from source-code access to $\mathcal{O}(P)$, you can also determine from oracle access to P with very high probability.

Virtual Blackbox

For any source-code analyser A,
there exists a oracle-access only simulator Sim, such that
for any P and $P' = \mathcal{O}(P)$:

$$A(P') = 1$$

Virtual Blackbox

For any source-code analyser A,
there exists a oracle-access only simulator Sim, such that
for any P and $P' = \mathcal{O}(P)$:

$$A(P') = 1 \qquad Sim^{P'} = 1$$

Virtual Blackbox

For any source-code analyser A,
there exists a oracle-access only simulator Sim, such that
for any P and $P' = \mathcal{O}(P)$:

$$A(P') = 1 \approx Sim^{P'} = 1$$

Virtual Blackbox

For any source-code analyser A,
there exists a oracle-access only simulator Sim, such that
for any P and $P' = \mathcal{O}(P)$:

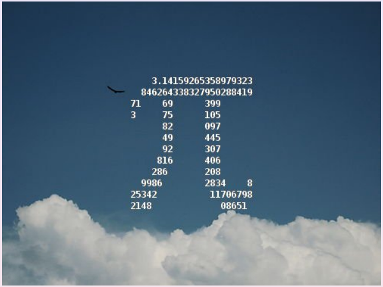
$$Pr[A(P') = 1] \approx Pr[Sim^{P'} = 1]$$

How Is An Oracle Different From A Program?

Program

- Description of I/O
- Can be analysed

Oracle



- Access to I/O
- Access to running time
- All you know is what you query

Obfuscating Password Functions

Original

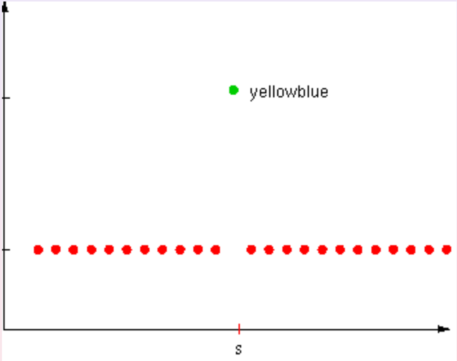
```
boolean isValidPassword ( String password ) {
  if ( password = "yellowblue" )
    then return true;
    else return false;
}
```

Obfuscated

```
boolean isValidPassword ( String password ) {
  if (md5sum(password) = "44d3aa30c6bbd44f8f1fa2470daab8df")
    then return true;
    else return false;
}
```

Point functions

- Password functions are examples of point functions



- Defined over a large domain
- Small probability of guessing secret s
- Unlearnable

Obfuscation: Impossible?

- We need a function f_s that is:
    - unlearnable
    - contains a secret s
    - no algorithm using f_s as an oracle can obtain s

    - given *any* program that computes f_s, we can compute s

- If such f_s exists, it will imply general obfuscators do *not* exist.

Obfuscation: Impossible?

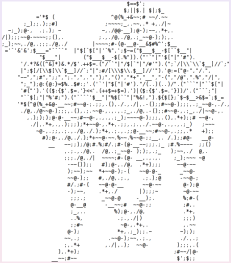
- Difficult to rely on features of *A*
  - How about a program which prints out the secret?

```
    3.14159265358979323
  846264338327950288419
71    69      399
3     75      105
      82      097
      49      445
      92      307
     816      406
    286       208
  9986        2834    8
25342          11706798
2148             08651
```

  - Great! *A* gets the secret.
  - Unfortunately, so does *Sim*

Obfuscation: Impossible?

- How about a program which prints out its own source?



```
                                     $==$';
                                    $;||$.| $|;$_
          ='*$ (                ^@(%_+&~~;# ~~/.~~
       ;_);;.);;#)             ;~~~~;_,.~~,.* +,./|~
  ~;_);@-,  .;.); ~           ~,./@@-__);@-);~~,.*+,.
/|);;;~~@-~~~~;;(),.         ;.,./@,./@,.;_~~@-););,.
;_);~~,./@,.;;;;./@,./     |~~~~;#-(@-__@-__&$#%^';$__
 ='`'&'&';$___="`````"  |"$[`$["|'`%",';$~=("$___$__-$[``$__"|
           "$___"|      ("$___$__-$[.%")).("'`"|"'$["|"'#").
      '/.*?&([^&]*)&.*/$'.++$=.("/``"|"/$[`"|"/#'").(";`/[\\`\\`$__]//`;"
      |";$[/[\\$[\\`$__]//`;"|";#/[\\\$\\.$__]//'").'@:=("@-","/.",
     "~~",";#",";;",";.",",.",");","()","*+","__","-(","/@",".%","/|",
      ";_");@:{@:}=$%..$#:;'.('`'|"$["|'#')."/(..)(..)/".("```"|"``$["|
      '#("').'(($:{$'.$=.'}<<'.(++$=+$=).')|($:{$'.$=.'}))/'.("```;"|
      "``$[;"|"%'#;").("````'$__"|"%$[``"|"%&!,").${$[};`$~$__>&$=`;$_=
     '*$(^@(%_+&@-__~~;#~~@-;.;;,.(),./.,./|,.-();;#~~@-);;;,.;_~~@-,./.,
      ./@,./@~~@-);;;,.(),.;.~~@-,.,.,.;_,./@,.-();;#~~@-,.;_,./|~~@-,.
        ,.);););@-@-__~~;#~~@-,.,.,.;_);~~~~@-);;;,.(),.*+);;# ~~@-,
        ./|,.*+,.,.);;;);*+~~@-,.*+,.;;,.;.,./.~~@-,.,.,.;_)   ;~~~
          ~@-,.;;,.;.,./@,./.);*+,.;.,.;;@-__~~;#~~@-,.;;,.*   +);;
            #);@-,./@,./.);*+~~@-~~.%~~.%~~@-;;__,. /.);;#@-   __@-
              __    ~~;;);/@;#.%;#/.;#-(@-__~~;;;.;_ ;#.%~~~~  ;;()
                   ,.;.,./@,.  /@,.;_~~@- );););,.;_   );~~,./  @,.
                   ;;;./@,./|  ~~~~;#-(@- __,.,.,.     ;_);~~~ ~@
                    -~~());;   #);@-,./@,   .*+);;;      ~~@-~~
                    );~~);~~  *+~~@-);-(   ~~@-@-_      _~~@-
                    ~~@-);;   #,./@,.;.,     .;.);@      -~~@-;
                    #/.;#-(   ~~@-@-__       ~~@-~~       @-);@
                    -);~~,    .*+,./        |);;;~       ~@-~~
                    ;;;.;     _~~@-@      -__);.        %;#-(
                    @-__@      -__~~;#  ~~@-;;          ;#,.
                    ;_,..        %);@-,./@,            .*+,
                    ..%,          .;.,./|)             ;;;)
                    ;;#~           ~@-,.*+,.           ,.~~
                   @-);           *+,.;_);;.~         ~););
                   ~~,.;        .~~@-);~~,.;.,        ./.,.;
                   ;,.*+        ../|,.);  ~~@-       );;;,.(
                 ),.*+);                            ;#~~/|@-
               __~~;#~~                             $';$;;
```

- Great! *A* gets the secret.
- Unfortunately, so does *Sim*

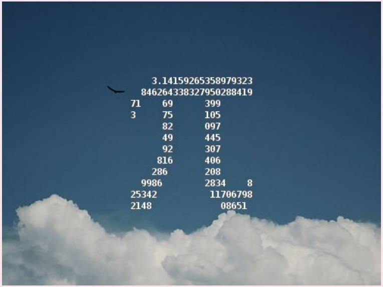
Obfuscation: Impossible?

A has a executable description of *P*! *Sim* does not!

Source code

vs.

Oracle



Obfuscation: Impossible?

A has a executable description of P! Sim does not!

If in a special mode, P asks for a program and the user supplies P with a program that behaves just like P then P tells the secret.

Point Function

```
public class f_s {
  final long SECRET = 6793370272;

  public int pointFunction ( long x ) {
    if ( x == SECRET )
      return 1;
    else
      return 0;
  }

  public void main ( long input ) {
    ...
    System.out.println ( pointFunction (input) );
  }
}
```

Point Function With A Secret Spy

```
public class f_s {
  final long SECRET = 6793370272;
  final boolean spy_mode;

  public int pointFunction ( long x ) {...}
  public void main ( long input,
                     boolean spy_mode,
                     Program program ) {
    ...
    if ( spy_mode )
      if ( behavesLikeMe ( program ) )
        System.out.println ( SECRET );
      else
        System.out.println ( "I␣know␣nothing." );
    else
      System.out.println ( pointFunction (input) );
  }
}
```

Self-recognition

```
public boolean behavesLikeMe ( Program p ) {
  int testPoint = SECRET;
  int tests = 1000;
  boolean result = true;

  do {
    if ( p.run ( testPoint ) !=
           pointFunction ( testPoint ) )
      return false;
      int testPoint = Math.randomInt();
      test--;
  } until ( test == 0 );
}
```

The Secret Revealed

```
public void main ( long input , boolean spy_mode , Program program )
```

A

- Simply calls $f_s(0, true, f_s)$
- Gets the secret

Sim

- Cannot generate a program that will fool f_s
- Does not get the secret

Encryption Problem: Impossible

```
if ( behavesLikeMe ( program ) )
then System.out.println ( SECRET );
else System.out.println ( encrypt(message,SECRET) );
```

- Program is secure if attacker is given only oracle-access
- Any source-code access to this encryption algorithm will reveal SECRET

Obfuscation Problem: Impossible

- Does this matter?
- Is this an important property to hide?
- Is a oracle-free definition of obfuscation susceptible?
- Is this the only family of functions we cannot obfuscate?
    - functions that are *trying* to reveal themselves