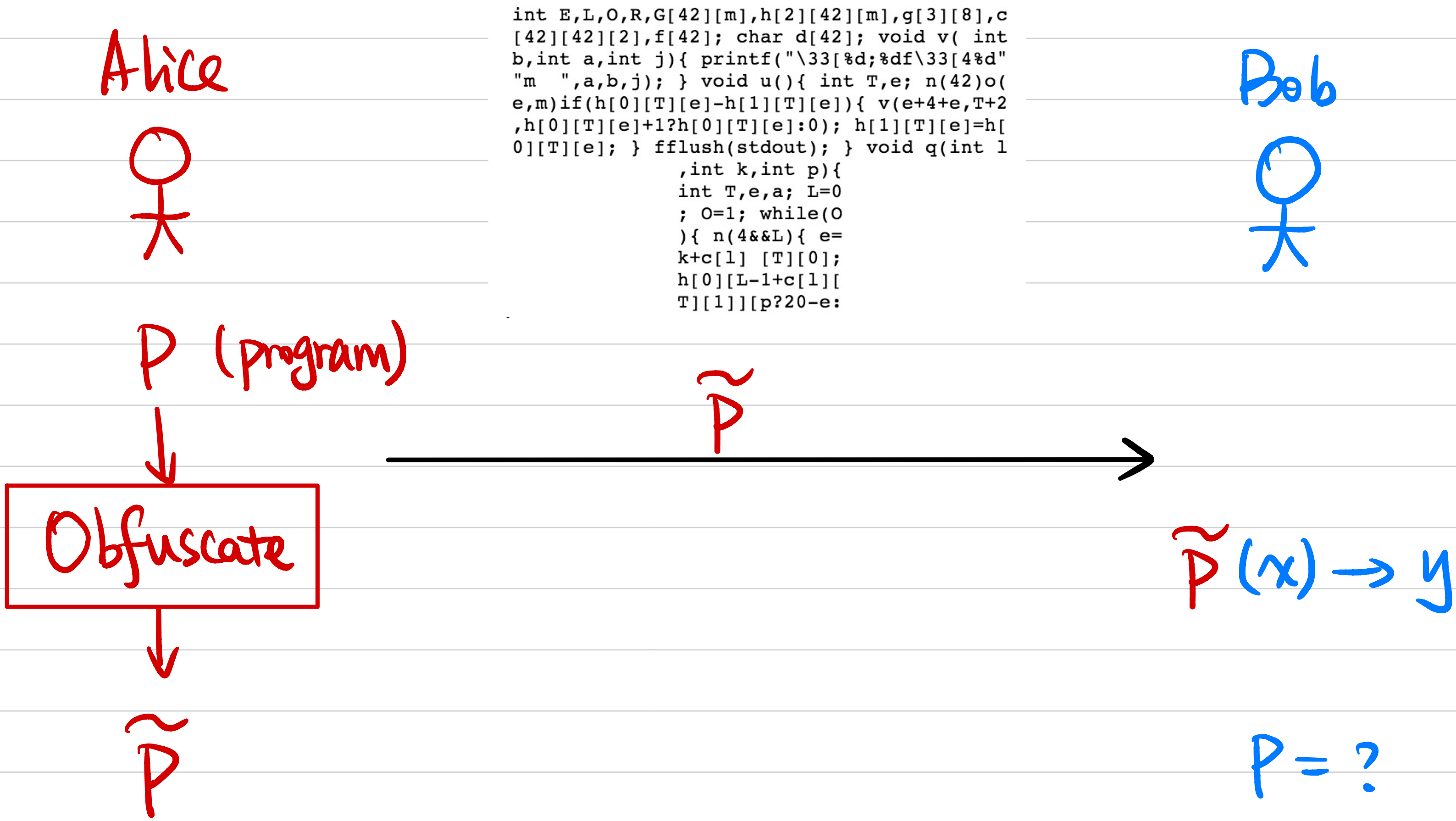
# CSCI 1510

- Program Obfuscation (continued)
- Final Review

ANNOUNCEMENT: Course Feedback & Critical Review

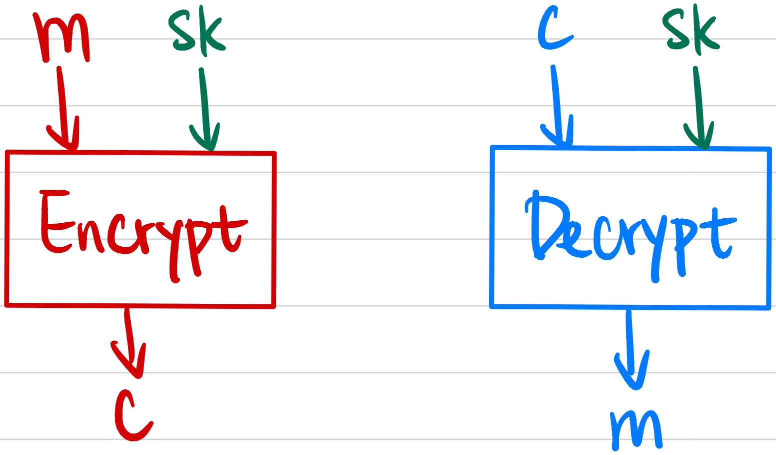
# Program Obfuscation



```
int E,L,O,R,G[42][m],h[2][42][m],g[3][8],c
[42][42][2],f[42]; char d[42]; void v( int
b,int a,int j){ printf("\33[%d;%df\33[4%d"
"m  ",a,b,j); } void u(){ int T,e; n(42)o(
e,m)if(h[0][T][e]-h[1][T][e]){ v(e+4+e,T+2
,h[0][T][e]+1?h[0][T][e]:0); h[1][T][e]=h[
0][T][e]; } fflush(stdout); } void q(int l
               ,int k,int p){
               int T,e,a; L=0
               ; O=1; while(O
               ){ n(4&&L){ e=
               k+c[l] [T][0];
               h[0][L-1+c[l][
               T][1]][p?20-e:
```

Goal: Make the program "unintelligible" without affecting its functionality.

# Symmetric-Key to Public-Key



# Formal Definition: Virtual Black Box (VBB)

Obfuscator $O$: $\quad C \xrightarrow{O} O(C)$

- **Functionality**: $O(C)$ computes the same function as $C$.
- **Polynomial Slowdown**: $|O(C)| \le \text{poly}(n) \cdot |C|$
- **Security (Virtual Black Box)**:

  $\forall$PPT $A$, $\exists$PPT $S$, s.t. $\forall C$, $\quad A(O(C)) \overset{c}{\simeq} S^{C(\cdot)}(1^{|C|})$.

$$\begin{tikzcd} & & \boxed{C(\cdot)} \arrow[d, bend left, "C(x)"] \\ O(C) & \simeq & \text{Simulator} \arrow[u, bend left, "x"] \end{tikzcd}$$

Thm VBB obfuscator for all poly-sized circuits is impossible to achieve.

$$C(x) := \begin{cases} b & \text{if } x = a \\ m & \text{if } x(a) = b \\ 0 & \text{otherwise} \end{cases}$$

# Formal Definition: Indistinguishability Obfuscation (iO)

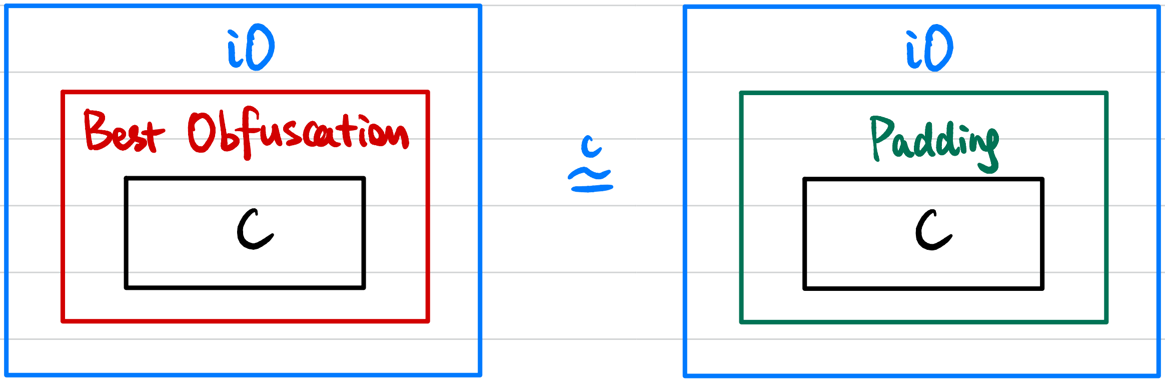
Obfuscator $O$: $\quad C \xrightarrow{O} O(C)$

- **Functionality:** $O(C)$ computes the same function as $C$.
- **Polynomial Slowdown:** $|O(C)| \le \text{poly}(n) \cdot |C|$
- **Security (indistinguishability obfuscation):**

  If $C_0$ & $C_1$ compute the same function and $|C_0| = |C_1|$,

  then $O(C_0) \overset{c}{\simeq} O(C_1)$

- **Best Possible Obfuscation**



# PKE from iO

Let $G: \{0,1\}^n \to \{0,1\}^{2n}$ be a length-doubling PRG.

- $\mathrm{Gen}(1^n)$:

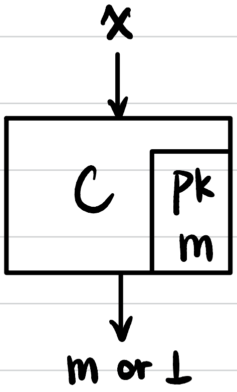
  $sk \xleftarrow{\$} \{0,1\}^n$

  $pk := G(sk)$

- $\mathrm{Enc}_{pk}(m)$:

  $$C_{pk,m}(x) := \begin{cases} m & \text{if } G(x) = pk \\ \perp & \text{otherwise} \end{cases}$$

  Output $c \leftarrow iO(C_{pk,m})$



- $\mathrm{Dec}_{sk}(c)$: ?

**Thm** If $G$ is a PRG and $iO(\cdot)$ is an idistinguishability obfuscator, then this PKE scheme is CPA-secure.

# Is it possible?

- 2001: Notion introduced
- 2013: Fist "candidate" construction from multilinear maps
- 2013-2020: Attack, fixes, new constructions from new assumptions
- 2020: New construction from well-founded assumptions

# Final Review

- Cryptographic Hardness Assumptions
  - Factoring / RSA Assumptions
  - DLOG / CDH / DDH Assumptions
  - LWE Assumption (Post-Quantum)

- Key Exchange
  - Definition
  - Construction: Diffie-Hellman

- Public-Key Encryption
  - Definition: CPA / CCA
  - Constructions: El Gamal / RSA / Regev

# Final Review

- Theoretical Assumptions
  - One-Way Function / Permutation : Definition & Candidates
  - Hard-Core Predicate: Definition & Construction
  - PRG/PRF from OWP

  - Trapdoor Permutation: Definition & Candidate (RSA)
  - PKE from TDP

- Fully Homomorphic Encryption
  - Definition & Applications
  - Somewhat Homomorphic Encryption over Integers & from LWE (GSW)
  - Bootstrapping SWHE to FHE

# Final Review

- Digital Signature
  - Definition
  - Hash-and-Sign Paradigm

  - Construction 1: RSA-FDH
  - Proof in the Random Oracle Model

  - Construction 2: Schnorr
  - Identification Scheme: Definition & Construction from DLOG (Schnorr)
  - Fiat-Shamir Transform

# Final Review

- Zero-Knowledge Proof
  - Definition: Completeness / Soundness / Zero-Knowledge

  - Example: ZKP for Diffie-Hellman Tuples
  - Proof Technique: Rewinding

  - ZKP for All NP (Graph 3-Coloring)
  - Commitment Scheme

  - Non-Interaltive ZK

# Final Review

- Secure Multi-Party Computation
  - Definition: Semi-Honest / Malicious
  - Applications
  - Example: Private Set Intersection from DDH
  - MPC for Any Function (GMW)
  - Oblivious Transfer: Definition & Construction from CDH

- Program Obfuscation
  - Definitions: VBB / iO
  - Example: PKE from iO

THANK YOU ^‿^