# CSE215
# Foundations of Computer Science


**Instructor: Zhoulai Fu**

**State University of New York, Korea**


**May 11, 2022**

# Agenda

- Attendance
- Pigeonhole principle
- Inverse functions
- Function composition

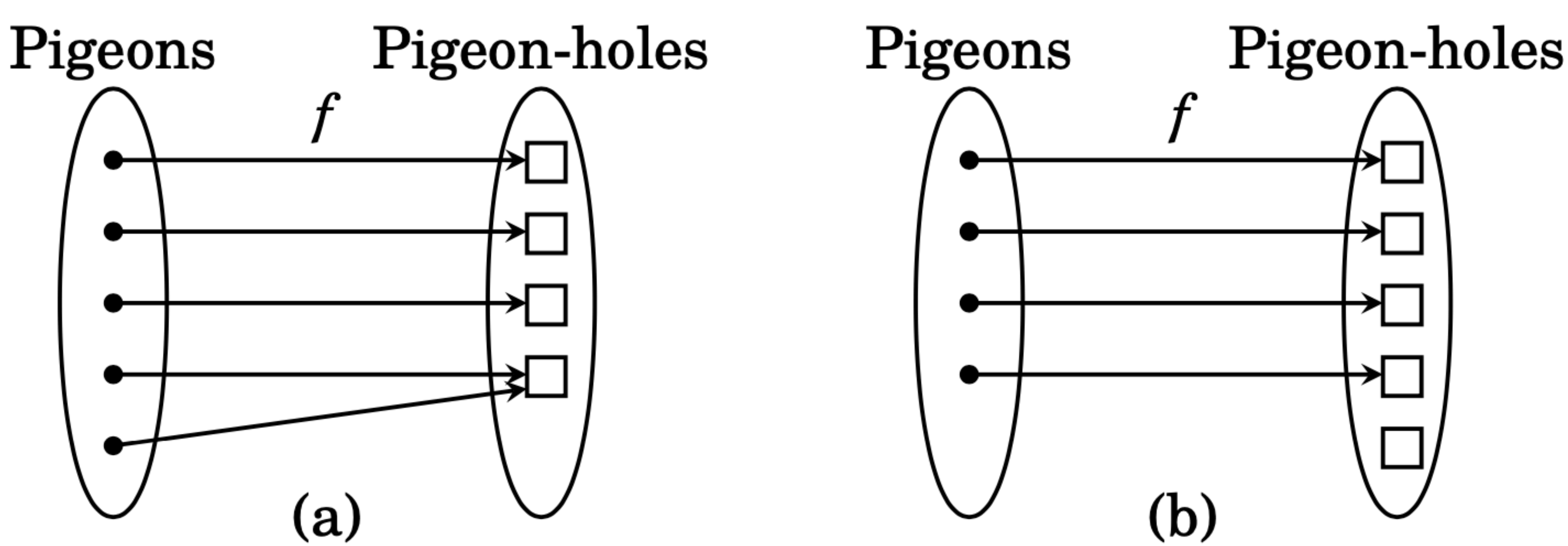
**To finish around 4h45**

**Zoom on today!**

# The Pigeonhole Principle

# Intuition

- Imagine there is a set A of pigeons and a set B of pigeonholes, and all the pigeons fly into the pigeonholes. You can think of this as describing a function $f : A \rightarrow B$, where pigeon X flies into pigeonhole f(X).



# The Pigeonhole Principle (function version)

Suppose $A$ and $B$ are finite sets and $f : A \to B$ is any function. Then:

- If $|A| > |B|$, then $f$ is not injective.
- If $|A| < |B|$, then $f$ is not surjective.

# Example 1

- Prove the following statement: If A is any set of 10 integers between 1 and 100, then there exist two different subsets X ⊆ A and Y ⊆ A for which the sum of elements in X equals the sum of elements in Y .

To illustrate what this proposition is saying, consider the random set

$$A = \{5, 7, 12, 11, 17, 50, 51, 80, 90, 100\}$$

of 10 integers between 1 and 100. Notice that $A$ has subsets $X = \{5, 80\}$ and $Y = \{7, 11, 17, 50\}$ for which the sum of the elements in $X$ equals the sum of those in $Y$. If we tried to "mess up" $A$ by changing the 5 to a 6, we get

$$A = \{6, 7, 12, 11, 17, 50, 51, 80, 90, 100\}$$

which has subsets $X = \{7, 12, 17, 50\}$ and $Y = \{6, 80\}$ both of whose elements add up to the same number (86). The proposition asserts that this is always possible, no matter what $A$ is. Here is a proof:

# Solution

*Proof.* Suppose $A \subseteq \{1,2,3,4,\dots,99,100\}$ and $|A| = 10$, as stated. Notice that if $X \subseteq A$, then $X$ has no more than 10 elements, each between 1 and 100, and therefore the sum of all the elements of $X$ is less than $100 \cdot 10 = 1000$. Consider the function

$$f : \mathscr{P}(A) \to \{0,1,2,3,4,\dots,1000\}$$

where $f(X)$ is the sum of the elements in $X$. (Examples: $f\left(\{3,7,50\}\right) = 60$; $f\left(\{1,70,80,95\}\right) = 246$.) As $|\mathscr{P}(A)| = 2^{10} = 1024 > 1001 = \left|\{0,1,2,3,\dots,1000\}\right|$, it follows from the pigeonhole principle that $f$ is not injective. Therefore there are two unequal sets $X, Y \in \mathscr{P}(A)$ for which $f(X) = f(Y)$. In other words, there are subsets $X \subseteq A$ and $Y \subseteq A$ for which the sum of elements in $X$ equals the sum of elements in $Y$. ■

# Example 2

- Prove the following statement: There are at least two people in Incheon with the same number of hairs on their heads.
-

# Solution

- Let A be the set of all people of Incheon and let B = {0,1,2,3,4,…,1000000}. Let f : A → B be the function for which f (x) equals the number of hairs on the head of x. Since |A| > |B|, the pigeonhole principle asserts that f is not injective. Thus there are two people of Incheon x and y for whom f(x) = f (y), meaning that they have the same number of hairs on their heads.

# Exercise 1

- Prove that if six numbers are chosen at random, then at least two of them have the same remainder when divided by 5.

- We accept two facts. First, the population of Incheon is around 2.93 million.  Second, it is a biological fact that every human head has fewer than one million hairs.

# Solution

- Suppose we randomly choose 6 integers.
- Let A be the set of the six integers.
- Let B the the set {0,1,2,3,4}
- Let f: A -> B be the function defined as f(a) = a mod 5
- Then f cannot be bijective
- Therefore there exists a1, a2 of A such that f(a1) = f(a2)

# Exercise 2

- Prove that if a is a natural number, then there exist two unequal natural numbers k and l for which $a^k - a^l$ is divisible by 10.

# Solution

- Suppose we randomly choose a natural number “a”.
- Let f: N -> {0,1,2,…,9} be a function defined as f(k) = last digit of a^k
- Following the pigeonhole principle, f cannot be injective.
- Thus there exists k and l such that f(k) = f(l)
- Thus a^k and a^l have the same last digit. Thus a^k - a^l is a multiple of 10.

# Summary: one-to-one and onto functions

**How to show a function $f: A \to B$ is injective:**

| **Direct approach:** | **Contrapositive approach:** |
| --- | --- |
| Suppose $x, y \in A$ and $x \neq y$. | Suppose $x, y \in A$ and $f(x) = f(y)$. |
| $\vdots$ | $\vdots$ |
| Therefore $f(x) \neq f(y)$. | Therefore $x = y$. |

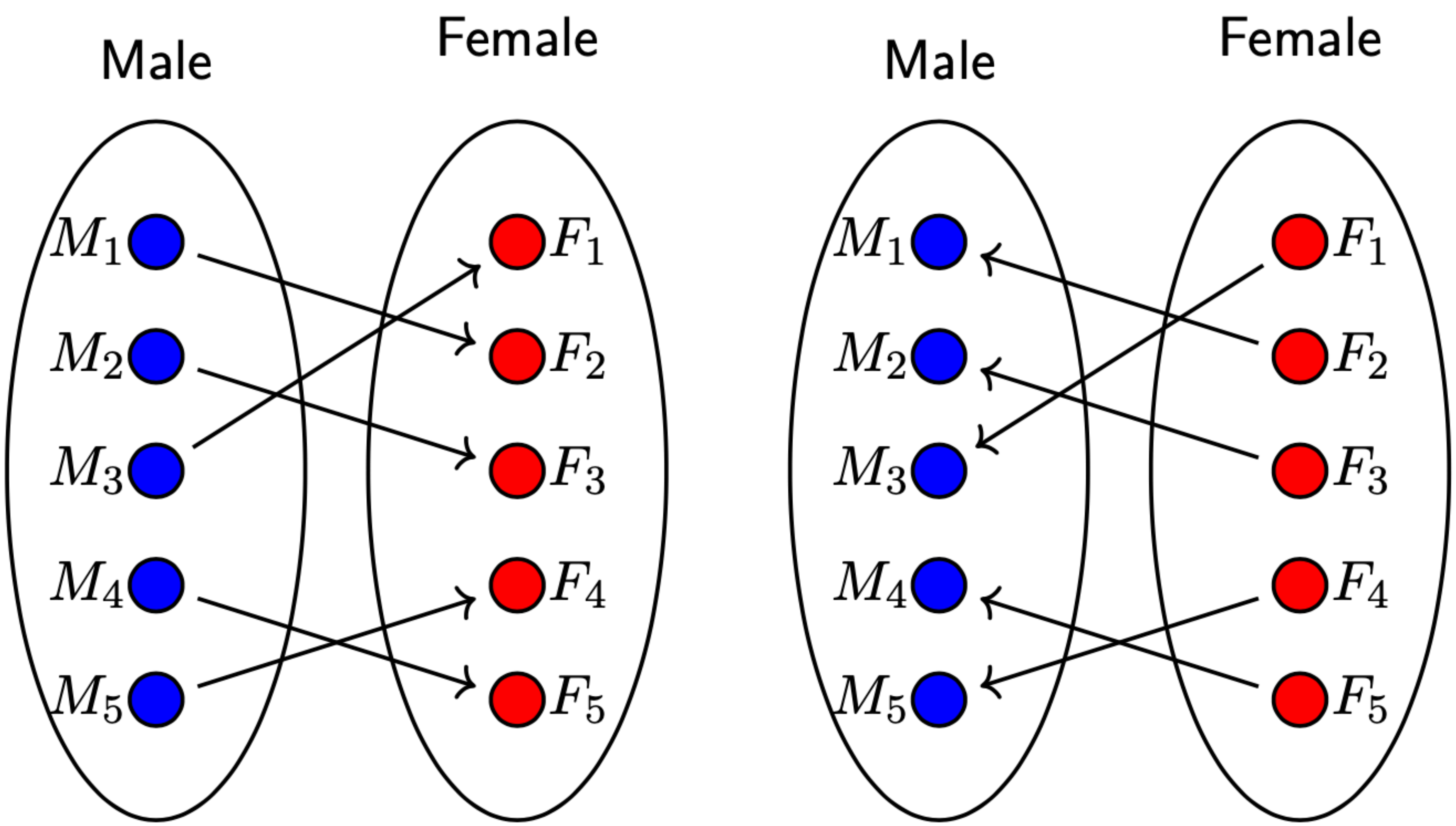
**How to show a function $f: A \to B$ is surjective:**

Suppose $b \in B$.
[Prove there exists $a \in A$ for which $f(a) = b$.]

# Inverse functions

# Inverse functions

- What is the difference between the two marriage functions?

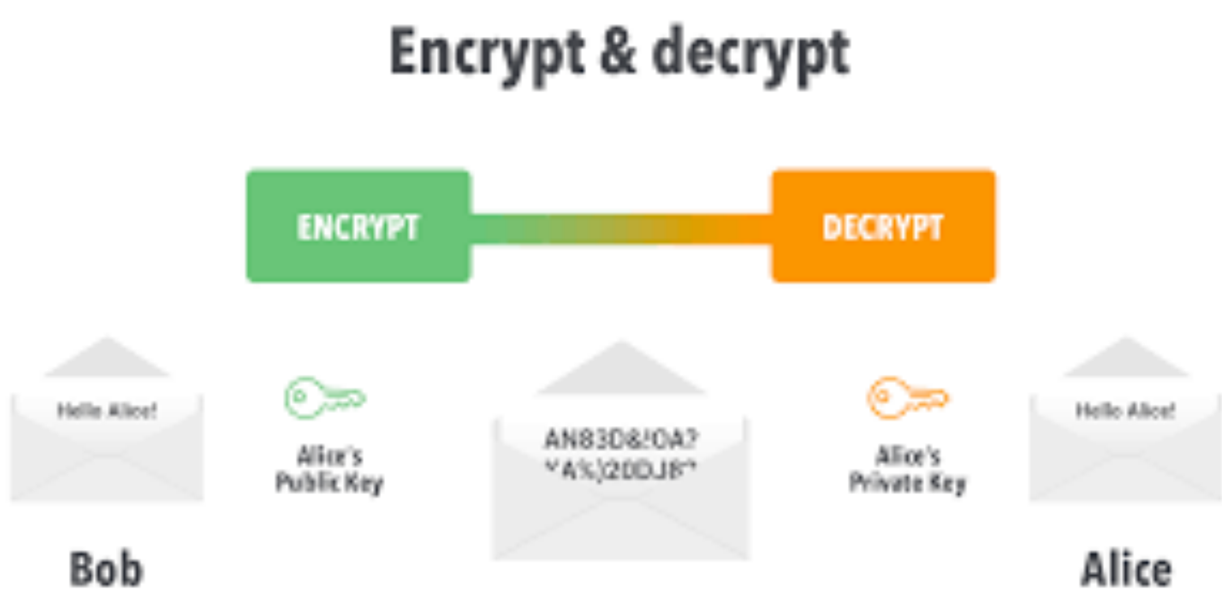


# Inverse functions

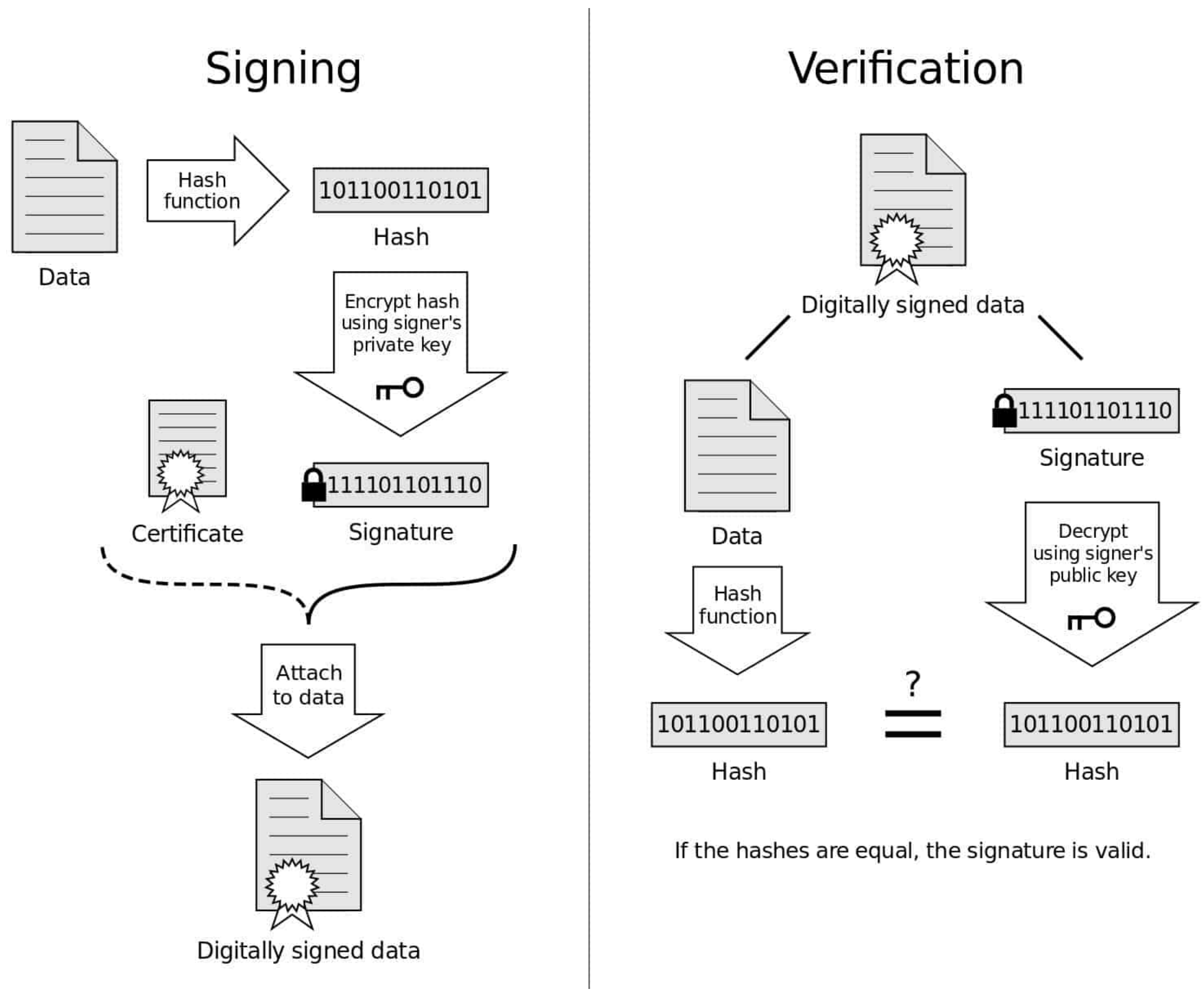
**Definition**

- Suppose $F : X \to Y$ is a one-to-one correspondence.
  Then, the inverse function $F^{-1} : Y \to X$ is defined as follows:
  Given any element $y$ in $Y$,
  $F^{-1}(y) =$ that unique element $x$ in $X$ such that $F(x) = y$.
- $F^{-1}(y) = x \Leftrightarrow y = F(x)$.

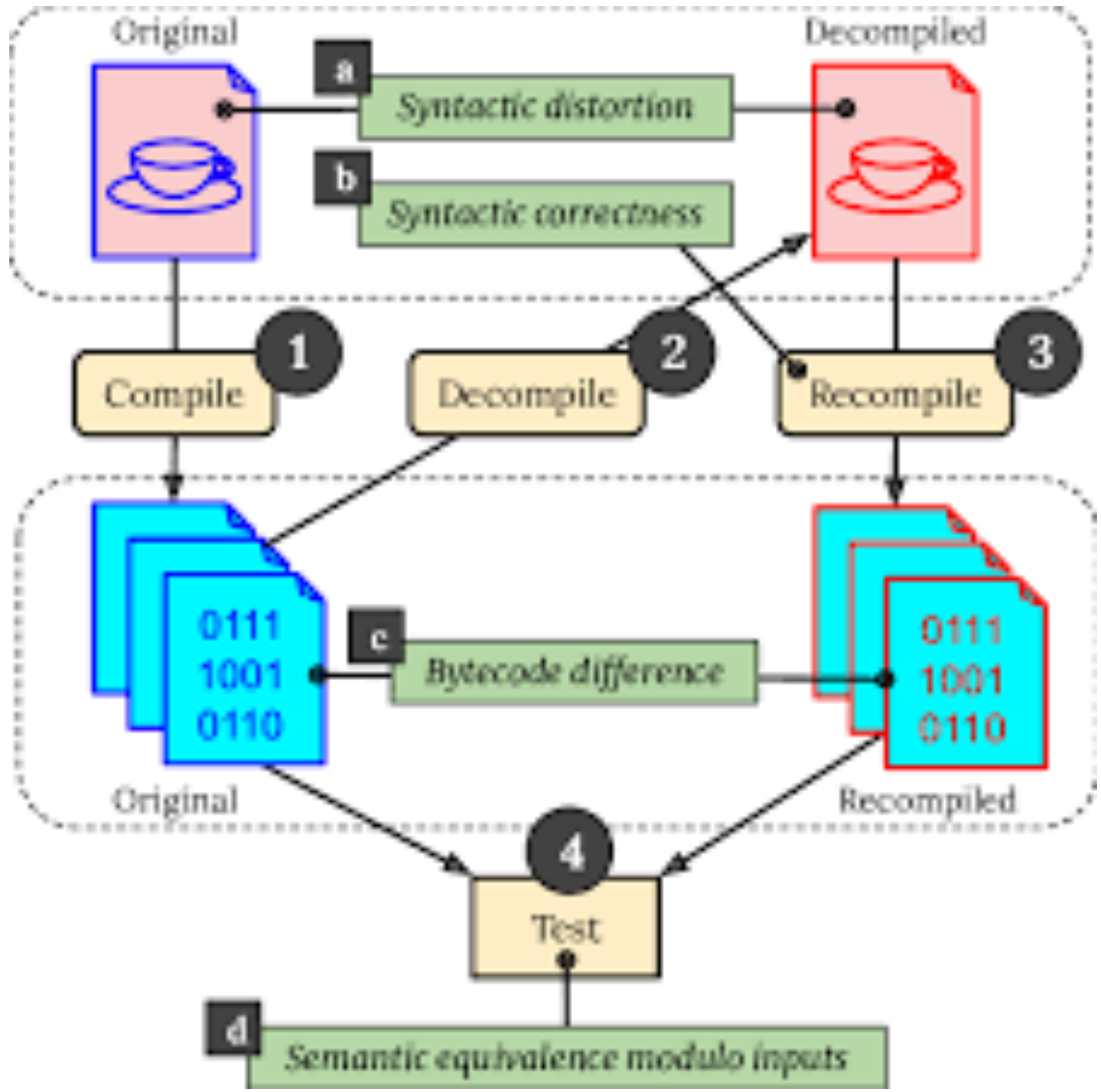
# Does encryption have an inverse function?



# Does digital signing have an inverse function?



# Does Java compilation have an inverse function?



# Inverse functions: Example 1

| Subset of $\{a, b, c, d\}$ | | 4-tuple of $\{0, 1\}$ |
|---|---|---|
| $\{\}$ | $\longleftarrow$ | $(0, 0, 0, 0)$ |
| $\{a\}$ | $\longleftarrow$ | $(1, 0, 0, 0)$ |
| $\{b\}$ | $\longleftarrow$ | $(0, 1, 0, 0)$ |
| $\{c\}$ | $\longleftarrow$ | $(0, 0, 1, 0)$ |
| $\{d\}$ | $\longleftarrow$ | $(0, 0, 0, 1)$ |
| $\{a, b\}$ | $\longleftarrow$ | $(1, 1, 0, 0)$ |
| $\{a, c\}$ | $\longleftarrow$ | $(1, 0, 1, 0)$ |
| $\{a, d\}$ | $\longleftarrow$ | $(1, 0, 0, 1)$ |
| $\{b, c\}$ | $\longleftarrow$ | $(0, 1, 1, 0)$ |
| $\{b, d\}$ | $\longleftarrow$ | $(0, 1, 0, 1)$ |
| $\{c, d\}$ | $\longleftarrow$ | $(0, 0, 1, 1)$ |
| $\{a, b, c\}$ | $\longleftarrow$ | $(1, 1, 1, 0)$ |
| $\{a, b, d\}$ | $\longleftarrow$ | $(1, 1, 0, 1)$ |
| $\{a, c, d\}$ | $\longleftarrow$ | $(1, 0, 1, 1)$ |
| $\{b, c, d\}$ | $\longleftarrow$ | $(0, 1, 1, 1)$ |
| $\{a, b, c, d\}$ | $\longleftarrow$ | $(1, 1, 1, 1)$ |

# Inverse functions: Example 2

**Problem**

- Define $f : \mathbb{R} \to \mathbb{R}$ by the rule $f(x) = 4x - 1$ for all $x \in \mathbb{R}$. Find its inverse function.

**Proof**

For any $y$ in $R$, by definition of $f^{-1}$

- $f^{-1}$ = unique number $x$ such that $f(x) = y$
  Consider $f(x) = y$
  $\implies 4x - 1 = y \qquad (\because \text{Defn. of } f)$
  $\implies x = \frac{y+1}{4} \qquad (\because \text{Simplify})$
- Hence, $f^{-1}(y) = \frac{y+1}{4}$ is the inverse function.

# Exercise 0

- Check that the function $f : Z \to Z$ defined by $f(n) = 6 - n$ is one-to-one correspondence. Then compute its inverse.

# Exercise 1

- The function f : R → R defined as $f(x) = x^3 + 1$ is a one-t-one correspondence. Find its inverse.

# Exercise 2

- Earlier, you proved that $f : R - \{2\} \to R - \{5\}$ defined by $f(x) = (5x+1)/(x-2)$ is bijective. Now find its inverse.

# Solution

- Earlier, you proved that f : R–{2} → R–{5} defined by f(x) = (5x+1)/(x-2) is bijective. Now find its inverse.

- Let y be an element of R - {5}. We have y = f(x) if and only if x = 11/(y-5)+2.

- Thus f^{-1} (x) = 11/(y-5)+2

# Exercise 3

- The function $g:Z\times Z\rightarrow Z\times Z$ defined by the formula $g(m,n)=(m+n, m+2n)$ is a one-to-one correspondence. Find its inverse.

# Solution

- Let (u,v) be an arbitrary element if Z x Z. Then f(m,n) = (u,v) if and only if m = 2u-v and n = v-u.
- Thus, f^{-1) (u,v) = (2u-v, v-u).

# Exercise 4
# Prove the following theorem

**Theorem**

- If $X$ and $Y$ are sets and $F : X \to Y$ is a one-to-one correspondence, then $F^{-1} : Y \to X$ is also a one-to-one correspondence.

# Inverse functions

**Theorem**

- If $X$ and $Y$ are sets and $F : X \to Y$ is a one-to-one correspondence, then $F^{-1} : Y \to X$ is also a one-to-one correspondence.

**Proof**

- $F^{-1}$ is one-to-one.
  Suppose $F^{-1}(y_1) = F^{-1}(y_2)$ for some $y_1, y_2 \in Y$.
  We must show that $y_1 = y_2$.
  Let $F^{-1}(y_1) = F^{-1}(y_2) = x \in X$. Then
  $y_1 = F(x)$ since $F^{-1}(y_1) = x$ and
  $y_2 = F(x)$ since $F^{-1}(y_2) = x$.
  So, $y_1 = y_2$.
- $F^{-1}$ is onto.
  We must show that for any $x \in X$, there exists an element $y$ in $Y$ such that $F^{-1}(y) = x$.
  For any $x \in X$, we consider $y = F(x)$.
  We see that $y \in Y$ and $F^{-1}(y) = x$.