Inverses and Decryption

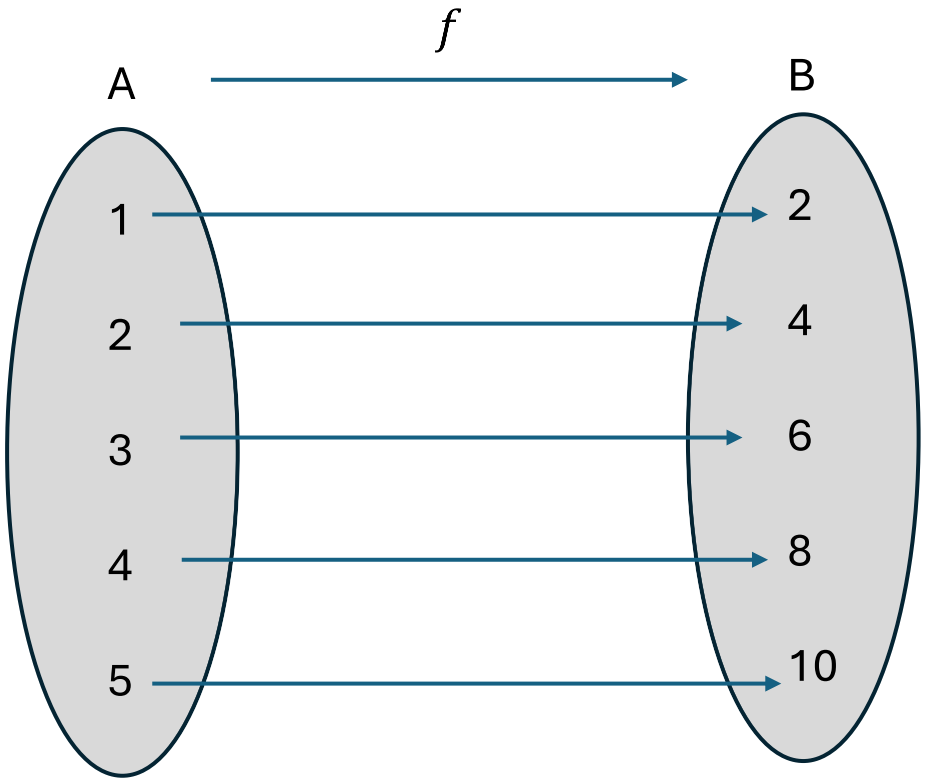
Alex Shaffer

Inverses

- I general an inverse is just an something that reverses a process.
- Some, but not all, functions have corresponding inverse functions.
  - If f is a function which is invertible, then f^{-1} is the notation used for the inverse.
  - If $f: A \to B$ then $f^{-1}: B \to A$
  - If $x_0 \in A$ and $f(x_0) = y_0$ then if f^{-1} exists, $f^{-1}(\mathrm{y}_0) = \mathrm{x}_0$.

Inverses

- $f: A \to B$ has an inverse. $g: A \to B$ does **not** have an inverse



One-to-One Functions

- From the last slide, the function f has the property of being one-to-one.
  - This means that every element of the codomain has at most one element of the domain associated with it.
- g did not have this property because in set B, 4 was associated with 1 and 2 in A.

Onto functions

- The function f is also an “onto” function.
  - This is because it associates an element of A with every element of B.
- g was not an onto function.
  - Not every element of B was mapped to.

Bijective functions

- A function is a bijection if it is one-to-one and onto.
  - f is a bijective function.
- For a global inverse to exist, the function must be a bijection.
  - If the function is only one-to-one, then a local inverse exists.
  - If the function is only onto, then no inverse exists.
  - If the function is neither, then no inverse exists.

Some Inverses

- The inverse of adding a number x is subtracting by the same number x
  - And vice versa
- The inverse of multiplying by a number x is dividing by the same number x.
  - And vice versa

The Modular Multiplicative Inverse

- Consider the modular arithmetic congruence:
  - $ax \equiv 1 \ (mod\ n),$ where a, x, and n are integers, and $n > 0$.
- We want to find the value x:
  - x is the modular multiplicative inverse of a and is useful in cryptography as we will see.
  - We will also denote the modular multiplicative inverse of a as a^{-1}.
- a only has a modular multiplicative inverse if it is coprime to n.
  - Two numbers are coprime if the share no common prime factors.

Coprime Numbers

- Two numbers are coprime if they if they share no prime factors
  - Prime numbers are numbers that have cannot be divided by any numbers besides themselves and 1.
- Numbers coprime to 26.
  - 26 has the prime factors $\{2, 13\}$
  - Coprime and less than 26: {1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25}

Finding a Modular Multiplicative Inverse

- For all $b \in \{0, 1, \ldots, n\ - 1\}$ compute all the values $a \cdot b(\mathrm{mod\ n})$:
- If any of these products is 1, then that b is the modular multiplicative inverse.
- If there is a modular multiplicative inverse, there is no need to check $b \geq n$ because those numbers have corresponding values less than n.

Modular Multiplicative Inverse Example

- We will usually be interested in systems (mod 26) so this is used in this example.
- Find the modular multiplicative inverse of $9 \ (mod\ 26)$:
  - $b \in \{0, 1, 2, \dots, 25\}$
  - Products modulo 26: $\{0, 9, 18, 1 \dots\}$
  - We got $9 \cdot b \equiv 1 \ (mod\ 26)$ when b = 3
  - The modular multiplicative inverse of 9 modulo 26 is 3.

Encryption and Decryption

- Encryption is a function.
  - The corresponding decryption is its inverse.
- Encryption $\rightarrow E(x)$
  - Domain is whatever the plaintext is made up of.
    - Letters
    - Numbers
    - Words
- Decryption $\rightarrow D(x)$
  - Domain is whatever the ciphertext is made up of.

Caesar Cipher

- For an integer key k
- For a Caesar Cipher we may define $E_{caesar}(x) = \mathrm{x} + \mathrm{k}\ (\mathrm{mod}\ 26)$
  - The domain is the integer $\{0, 1, 2, \ldots, 25\}$ which correspond to letters.
- The decryption cipher then is given by:
  - $D_{caesar}(x) = x\ - k\ (mod\ 26)$

The affine cipher

- An affine cipher uses a pair of encryption keys, a and b
  - We define $E_{affine}(x) = (ax + b) \pmod{26}$
- We then can decrypt with the decryption key a^{-1} and b:
  - We see that we need a to be chosen coprime to 26
  - $D_{affine}(x) = a^{-1}(x \ - b)(mod\ 26)$

Justification of the Affine Cipher

- For an arbitrary plaintext number x let us check to see that $D(E(x)) = x$.
  - This is just checking to ensure that $D(x)$ is the inverse of $E(x)$.
- $D\left(E(x)\right) = a^{-1}(E(x) - b)(mod\ 26)$

$$= a^{-1}\left(\left((ax + b)\ (mod\ 26)\right) - b\right)(mod\ 26)$$

$$= a^{-1}(ax + b\ - b)(mod\ 26)$$

$$= a^{-1}ax(mod\ 26)$$

$$= x\ (mod\ 26)$$