Agenda

- PROBLEM DOMAIN: NUMBER THEORY
- APPLICATION DOMAIN: CRYPTOGRAPHY
- BASICS OF CRYPTOGRAPHY
  - SECRECY OR CONFIDENTIALITY
  - SHARED KEY AND PUBLIC KEY SYSTEMS

Cryptography - Secrecy

- Communication from Alice to Bob:
  - A sends a message M to B on a public channel
    - i.e. any one can read from the channel
- (Desired) Property of said communication:
  - ***Secrecy*** or ***Confidentiality***:
    - No one other than A and B can "get" the message.

Cryptography: Protocol for Secrecy

- **Straw Man Protocol**:
  1. A applies a function f on message M i.e. computes M′ = f(M)
  2. A sends M′ to B on a public channel
  3. B receives M′ and inverts i.e. B applies f^{-1} on M′ to get M
- **Requirements**:
  - f^{-1} cannot be computed by any one other than A or B.
    - **Solution**: Keep f and f^{-1} secret
    - **Pragmatics:**
      - *Obscurity is not security*
      - *Complexity weakens security*
        - Every pair of communicators - A and B - will have to invent their own functions
          - i.e. O(N*N) functions for a group of N communicators
          - i.e. this is not suitable for mass usage.

Cryptography – Secrecy and Encryption

- **Tin Man Protocol:**
  - A applies a function E on message M and a key K_A i.e. computes M′ = E(M,K)
  - A sends M′ to B
  - B receives M′ and inverts it by applying a function E^{-1} on M′ and a key K_B to get M i.e. M = $E^{-1}(M', K_B)$
- **Requirements**:
  - K_B must not be known to any one other than A or B.
  - Without K_B, $E^{-1}(M', K_B)$ cannot be computed.
- **Note:**
  - **E** is referred to as an ***encryption*** function and $\mathbf{E^{-1}}$ is referred to a ***decryption*** function. **End of Note.**

Shared Key Encryption

- **Tin man Protocol:**
  - A sends $M' = E(M, K_A)$ to B
  - B receives M' and computes $M = E^{-1}(M', K_B)$
- **Requirements:**
  - K_B must not be known to any one other than A or B.
  - **Solution 1 :** *Shared Key encryption*:
    - A and B share a secret (K_A, K_B)
    - K_A and K_B can be computed easily from each other; simplest case: $K_A == K_B$
  - **Pragmatics:**
    - Every pair of communicators A and B will require a pair of keys (K_A, K_B)
      - i.e. O(N*N) keys are required for a group of N communicators

Public Key Encryption

- **Tin Man Protocol:**
  - A sends M′ = $E(M,K_A)$ to B
  - B receives M′ and computes M = $E^{-1}(M', K_B)$
- **Requirements:**
  - K_B must not be known to any one other than A or B.
    - **Solution 2** : *Public Key encryption*:
      - K_B is private to B: *denote it* $\boldsymbol{K_{Bv}}$,
      - K_A is public (but associated with B): *denote it* $\boldsymbol{K_{Bu}}$
        - *K_{Bv} cannot be computed easily from K_{Bu}*
    - **Pragmatics:**
      - Every receiver B will require a pair of keys ($\mathbf{K_{Bv}}$, $\mathbf{K_{Bu}}$)
      - All public keys can be published (say, in a directory)
        - i.e. N key pairs are required for a group of N communicators

Public Key Encryption

- **Iron Man Protocol:**
  - A sends $M' = E(M, K_{Bu})$ to B
  - B receives M′ and computes $M = E^{-1}(M', K_{Bv})$
- **Requirements:**
  - E and E^{-1} are computable in polynomial time with keys K_{Bu} and K_{Bv} respectively but
    - *they are not computable in polynomial time without.*
  - Public Key encryption:
    - **Pragmatics:** *K_{Bv} should not be computable in polynomial time from K_{Bu}.*