Justin Ciocoi

Oct. 19, 2023

CSCI 360 Class Notes

Introduction to Public Key Cryptography

- Cryptography can be broken down into 2 main categories
  - **Symmetric Key**
  - **Public Key**
- Cryptography aims to provide certain services, including
  - *Confidentiality*
  - *Privacy*
  - *Integrity*
  - *Non-repudiability*
  - *Authenticity*
- What makes public key cryptography *public key cryptography*
  - In a *symmetric* infrastructure, only one key is shared among communicating parties
  - In *public key* cryptography, there is both a public key, k_{pub}, and a private key, k_{priv}
    - k_{pub} is publicly accessible
    - k_{priv} is only known by you
  - *Digital Signatures* in public key cryptography serve a similar purpose to real signatures and provides integrity *and* non-repudiability to public key cryptography
- Example of a student communication network at JJC using public key cryptography

    - For 14,000 students, each possible communication pair must have their own key when using *symmetric key* cryptography
        - Total keys $\approx 14,000^2/2 \approx 100,000,000$
    - In *public key* cryptography, each individual has one public key, and each individual can utilize their own private key.
        - Total keys $= (14,000 * 1) + (14,000 * 1) = 28,000$
- Public key cryptography alleviates the *key distribution problem* present in symmetric key cryptography
- *Downsides* to public key cryptography
    - 100x-1000x slower than symmetric key cryptography
    - Much larger key size
    - Quantum computers present a large threat to public key cryptography
- *Every* secure public key cryptography algorithm is based on one of the following
    - Integer factorization
    - Discrete Logarithms
    - Integer Lattices
        - *less proven, but less susceptible to quantum computer attack*
    -