CSC 116 Introduction of Cybersecurity

Assignment 1

Notes:
1 Write your answers in a new word document including your team number and members, and share it with our TA Caden before **02/03/2025.**
email: crh873@miami.edu.
2 No ChatGPT or any other generative AI solutions (e.g., Calude or Copilot) are allowed for answering all the assignments. **Generative AI is only eligible for grammar editing and sentence improvements.**

1. Understanding Real-World Use Cases

Many hospitals use **end-to-end encryption** for transmitting patient data. If a hospital uses **AES (Advanced Encryption Standard)** for encrypting medical records before sending them to another hospital, **which type of encryption is being used?** （**End-to-end:** it means a direct communication between the source and destination without intermediaries altering the content**.**）

- **a)** Symmetric
- **b)** Asymmetric
- **c)** Hashing
- **d)** None of the above

Explain why your choice is correct：

2. Encryption in Emergency Situations

A nurse is using a secure **medical alert system** that relies on **asymmetric encryption** for sending emergency alerts to doctors.

- **Why do you think asymmetric encryption is more suitable for this scenario rather than symmetric encryption?**
  (Hint: Consider how keys are shared.)

3. The Secret Code Experiment

You and one of your colleagues in a tech company decide to send secret messages using an encryption method. If you both use **the same key** for encryption and decryption, which encryption type are you using?

- **a)** Symmetric
- **b)** Asymmetric
- **c)** Hybrid
- **d)** One-time pad

4 Fast vs. Secure: A Nursing Decision

A hospital needs to choose between **symmetric encryption** (AES) and **asymmetric encryption** (RSA) for **real-time patient monitoring data**.

- **Which encryption method should they choose and why?**
  (Hint: Consider speed, security, and data volume.)

5. Encryption & HIPAA Compliance (Open questions, just share your comments and reasons)

The Health Insurance Portability and Accountability Act (HIPAA) requires hospitals to protect sensitive patient information.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 establishes federal standards protecting sensitive health information from disclosure without the patient's consent. The US Department of Health and Human Services issued the HIPAA Privacy Rule to implement HIPAA requirements. The HIPAA Security Rule protects specific information covered by the Privacy Rule.
https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html

- Which encryption method (symmetric or asymmetric) is more commonly used to encrypt stored patient records, and why?

6. The Risk of Shared Keys

A team of nurses or doctors shares an encryption key to access encrypted patient data. One day, one nurse resigns.

- How should the hospital ensure that the former nurse can no longer access the encrypted data?
  - a) Generate a new key and distribute it to all current nurses.
  - b) Continue using the old key but add an extra password.
  - c) Switch to asymmetric encryption so each nurse has their own private key.
  - d) Manually remove the nurse’s account from the hospital database.

7. The Future of Data Security (Open questions, just share your comments and reasons)

Quantum computers may be able to break asymmetric encryption (e.g., RSA, ECC) by quickly factoring large numbers.

- What steps do you think should take to protect patient/financial/IoT data against future quantum attacks?
  (Hint: Research "post-quantum cryptography.")