Lab Report 2
Due: 10/31/24
Adrian Nelson Aidan Chin
Code

- Question 1 (5 points): Give a short description for each of the 5 network security principles: **C**onfidentiality, **I**ntegrity, **A**uthentication, **A**ccessibility, and **A**vailability
    - Confidentiality
        - Both the sender the receiver should be the only recipients that can understand the transmission, sender encrypts and receiver decrypts
    - Integrity
        - The sent message is verifiably not edited in transit or otherwise
    - Authentication
        - The sender confirms the identity of the receiver and vice versa
    - Accessibility
        - Service must be accessible to all users, for example the security should be able to work on all different types of used hardware
    - Availability
        - Service must be made available to use for all users.

- Question 2 (3 points): Explain playback attack in the network with an example. How does the use of a random Nonce prevent such an attack?Q
    - A playback attack is when someone intercepts a transmission and plays it back again later maliciously. For example if someone sends a transaction to a bank and it gets intercepted, the attacker later could send it again and make the person make another transaction unknowingly. A random nonce helps prevent this as it is a random string of numbers that serve as a one time use transaction ID and if the re-sent transaction matches that ID, the bank knows not to process it.

- Question 3 (2 points): What is the difference between public key encryption and private key encryption?
    - Public key encryption uses a pair of mathematically linked keys where one is private and the other is public. The public key encrypts the data and the private key decrypts the data. It is slower but also more secure as only 1 key is public, this is what RSA uses.
    - Private key encryption is when there is 1 key that encrypts and decrypts the data. It is quick and not computationally heavy, but the 1 key needs to be securely transferred between users. This is what DES uses.
- Question 4 (2 ponts): Why did we use RSA for encrypting the key and not the

whole image and instead used DES for the image?

  - The reason we did this is because DES is fast and suitable for large amounts of data (like an image) and RSA is relatively very slow and would make encryption and decryption non-accessible to those who don’t have powerful computing power. Instead we make DES more secure by encrypting the key using RSA, then we get the best of both methods.