Report

[redacted]

Name: Pranav Sudeendra
NUID: [redacted]

Explanation:

1. **Key Sizes:**
   - **a.** RSA: 2048-bit keys are used for both sender and receiver. This key size is considered secure for the foreseeable future. This is the recommended min key size for resistance against brute-force attacks.
   - **b.** AES: 256-bit key for symmetric encryption. This provides a high level of security and is recommended by the NSA for protecting classified information.

2. **Algorithms:**
   - **a.** RSA for asymmetric encryption and digital signatures.
   - **b.** AES for symmetric encryption of the file content.
   - **c.** This combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem.

3. **Modes:**
   - a. AES-GCM (Galois/Counter Mode) for symmetric encryption. This mode provides both confidentiality and integrity protection. Also, this is more efficient than other modes like CBC as they can incur pipeline stalls.
   - b. OAEP (Optimal Asymmetric Encryption Padding) with SHA-256 for RSA encryption of the symmetric key. This prevents partial decryption of cipher texts and adds randomness to the encryption.
   - c. PSS (Probabilistic Signature Scheme) with SHA-256 for RSA signatures. This adds randomness to signature generation.

4. **Efficiency considerations:**
   - a. We use a hybrid cryptosystem, encrypting the file content with a fast symmetric algorithm (AES) and only using the slower asymmetric algorithm (RSA) to encrypt the symmetric key.
   - b. AES-GCM is chosen for its speed and built-in authentication, eliminating the need for a separate MAC.