



Audit Details

Auditor: joel ong

Weighted Score: 10

Weighted Score: 20

Weighted Score: 35

Weighted Score: 15

Weighted Score: 20

Full RSA

1. **Key generation**

1.1. Choose two large primes p and q .
1.2. Compute $n = p \cdot q$.
1.3. Compute $\phi(n) = (p-1)(q-1)$.
1.4. Choose e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$.
1.5. Compute d such that $ed \equiv 1 \pmod{\phi(n)}$.
1.6. Public key is (n, e) .
1.7. Private key is (n, d) .

2. **Encryption**

2.1. Convert message M to integer m .
2.2. Compute $c = m^e \pmod{n}$.
2.3. Send c to receiver.

3. **Decryption**

3.1. Receive c .
3.2. Compute $m = c^d \pmod{n}$.
3.3. Convert m back to message M .

Handwritten notes:

1. **Key generation**

1.1. Choose two large primes p and q .
1.2. Compute $n = p \cdot q$.
1.3. Compute $\phi(n) = (p-1)(q-1)$.
1.4. Choose e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$.
1.5. Compute d such that $ed \equiv 1 \pmod{\phi(n)}$.
1.6. Public key is (n, e) .
1.7. Private key is (n, d) .

2. **Encryption**

2.1. Convert message M to integer m .
2.2. Compute $c = m^e \pmod{n}$.
2.3. Send c to receiver.

3. **Decryption**

3.1. Receive c .
3.2. Compute $m = c^d \pmod{n}$.
3.3. Convert m back to message M .

Handwritten notes:

1. **Key generation**

1.1. Choose two large primes p and q .
1.2. Compute $n = p \cdot q$.
1.3. Compute $\phi(n) = (p-1)(q-1)$.
1.4. Choose e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$.
1.5. Compute d such that $ed \equiv 1 \pmod{\phi(n)}$.
1.6. Public key is (n, e) .
1.7. Private key is (n, d) .

2. **Encryption**

2.1. Convert message M to integer m .
2.2. Compute $c = m^e \pmod{n}$.
2.3. Send c to receiver.

3. **Decryption**

3.1. Receive c .
3.2. Compute $m = c^d \pmod{n}$.
3.3. Convert m back to message M .

