**Chapter 9:** **Public-Key Cryptography and RSA**

**TRUE OR FALSE**

1. F
2. F
3. T
4. F
5. T
6. F
7. T
8. T
9. F
10. T
11. T
12. F
13. T
14. T
15. F

**MULTIPLE CHOICE**

1. A
2. B
3. A
4. C
5. C
6. B
7. A
8. B
9. C
10. A
11. B
12. C
13. C
14. B
15. A

**SHORT ANSWER**

1. Asymmetric
2. key exchange
3. ciphertext
4. RSA
5. symmetric
6. Public Key Certificate
7. Public Key Infrastructure (PKI)
8. ciphertext
9. one-way function
10. digital signature
11. RSA
12. Euclid
13. timing attacks
14. chosen ciphertext attack (CCA)
15. optimal asymmetric encryption padding (OAEP)