**Chapter 21 – Public-Key Cryptography and Message Authentication**

**Answer Key**

**TRUE/FALSE QUESTIONS:**

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

**MULTIPLE CHOICE QUESTIONS:**

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

**SHORT ANSWER QUESTIONS:**

1. National Institute of Standards and Technology (NIST)
2. SHA-2
3. cost
4. HMAC
5. RSA
6. Timing attacks
7. mathematical
8. Digital Signature Standard (DSS)
9. Diffie-Hellman
10. XOR (bit-by-bit exclusive-OR)
11. SHA-3
12. MD5
13. secret key
14. cryptographic
15. RSA