

Review Session

Course 1-02-328: Communication Security and E-Commerce

Instructor: Michael J. May

June 30, 2010

Abstract

This review session is meant to help review concepts from that we covered over the course of the semester. There are no computation problems, just concepts to review. The students are expected to review the equations and mathematics on their own.

1 Definitions Part 1

Define the following terms as they relate to communications security:

1. Authentication
2. Integrity
3. Fault Tolerance
4. Secrecy
5. Privacy
6. Encryption
7. Code
8. Caesar Cipher
9. Frequency analysis
10. Index of Coincidence
11. Diffusion
12. Confusion
13. Stream Cipher
14. Block Cipher
15. One time pad
16. Transposition cipher
17. Product cipher
18. Computational Security
19. Shared Key Cryptography
20. DES
21. AES
22. Electronic Code Book (ECB)
23. Cipher Block Chaining (CBC)
24. Cryptographic Hash
25. One way function
26. Diffie-Hellman Key exchange
27. Public Key Cryptography
28. RSA Algorithm
29. Euler's Totient Function
30. Galois Field
31. Fermat's Little Theorem
32. Chinese Remainder Theorem

2 Definitions Part 2

1. Cryptographic Protocol
2. Dolev-Yao Model
3. Shared Key Authentication
4. Transferability
5. Impersonation
6. Replay attack
7. Nonce
8. Chosen Plaintext Attack
9. Known Plaintext Attack
10. Ciphertext Only Attack
11. Sequence Number
12. Timestamp
13. Digital Signature
14. Key Distribution Center
15. Needham-Schroeder Protocol
16. Trusted Third Party
17. Public Key Infrastructure
18. X.509 Certificate
19. Top Level Certificate
20. Certificate Revocation
21. Certificate Chain
22. Kerberos
23. Password
24. Prime Mover Problem
25. Salt
26. One time password
27. Hash-based one time password
28. Biometric Authentication
29. Access Control Matrix
30. Capability
31. Secure Sockets Layer (SSL)