Cryptography and Network Security

Final Exam (2014/01/13)

1. What is Private Information Retrieval (PIR)? Please explain it.

2. Describe RSA key generation, encryption, and decryption algorithms. Then show that RSA works correctly.

3. Find the small positive integer X satisfying
   (a) $X \equiv 2 \bmod 3$; $X \equiv 5 \bmod 6$; $X \equiv 3 \bmod 7$.
   (b) $X \equiv 2 \bmod 3$; $X \equiv 3 \bmod 5$; $X \equiv 3 \bmod 21$.
   You need show how you get the answers.

4. Find the results of the following, using Fermat's little theorem:
   (a) $456^{17} \bmod 17$
   (b) $70^{-1} \bmod 101$

5. Write the pseudocode for Miller-Rabin test.

6. Show the ciphertext stealing technique in ECB mode and CBC mode respectively.

7. List the parameters (block size, key size, and the number of rounds) for the three AES versions.

8. What is the block size in DES? What is the cipher key (excluding parity bits) size in DES? What is the round-key size in DES? What is the number of rounds in DES?

9. Explain why there is no need for ciphertext stealing in CFB, OFB, and CTR modes.

10. Write the pseudocode for square-and-multiply algorithm.