

Computer and Network Security

Fall Semester 2002

Quiz No. 4

October 1, 2002

Time Allowed: 15 Minutes

Name: _____

Total: 30 Points

Question 1: (10 points)

Encrypt the plaintext "ABACUS" using the RSA Public-Key encryption algorithm. Use the following parameters for the algorithm $p=3$, $q=11$. Choose $d = 7$. Use A=1, B=2, C=3, D=4 ... for non-alphabetical characters use +=27, -=28, *=29, /=30, _=31, %=32, \$=33. Provide your answer in character format.

Question 2: (1 point each – 10 points)

Solve the following:

1. $\phi(15) =$
2. $\phi(23) =$
3. $\phi(41) =$
4. $\phi(11) + \phi(13) =$
5. $\phi(7) * \phi(14) =$
6. $8 + 18 \bmod 6 =$
7. $23 + 29 \bmod 7 =$
8. $16 \times 4 \bmod 4 =$
9. $8^3 \bmod 6 =$
10. $7^2 \bmod 4 =$

Question 3: (1 point each – 10 points)

Give the letter corresponding to the correct answer.

1. A mathematical formula that is easy to work forward but very hard to work backward is called
 - a. *Backdoor*
 - b. *Euler's Totient Function*
 - c. *Trapdoor*
 - d. *Logic Bomb*

2. There are infinitely many prime numbers.
 - a. *False*
 - b. *True*

3. 7 is relatively prime to 11
 - a. *True*
 - b. *False*

4. Generally, asymmetric encryption algorithms are much faster to execute on a computer than symmetric ones.
 - a. *True*
 - b. *False*

5. Which of the following is a primitive root of 11?
 - a. *3*
 - b. *5*
 - c. *7*
 - d. *9*

6. The list of all the primitive roots of 7 is?
 - a. *2, 3, 4, 5, 6*
 - b. *2, 3, 5, 6*
 - c. *2, 3, 5*
 - d. *3, 5*

7. Which of the following is the discrete logarithm of 5 mod 13 if the primitive root 2 is used as the base?
 - a. *3*
 - b. *6*
 - c. *9*
 - d. *12*

8. $(\phi(11) + \phi(7)) \bmod \phi(5) =$
 - a. *0*
 - b. *1*
 - c. *2*
 - d. *3*

9. The first public-key scheme which was capable of signatures as well as encryption was
 - a. *DES*
 - b. *RSA*
 - c. *Diffie-Hellman*
 - d. *Merkle Knapsack*

10. The modular inverse of 7 mod 13 is
 - a. *3*
 - b. *5*
 - c. *2*
 - d. *12*