

Computer and Network Security Fall Semester 2002

Quiz No. 4

October 1, 2002

Time Allowed: 15 Minutes

Name: **SOLUTION**

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.

Key Generation

$$n = p \times q = 3 \times 11 = 33$$

$$z = (p-1) \times (q-1) = 2 \times 10 = 20$$

$$e = d^{-1} \text{ mod } z$$

$$e = 7^{-1} \text{ mod } 20$$

$$e = 3$$

$$\boxed{\text{Public Key} = \{3, 33\}}$$

Encryption

Plaintext	Numeric	P^e	$P^e \text{ mod } n$	Ciphertext
A	1	1	1	A
B	2	8	8	H
A	1	1	1	A
C	3	27	27	+
U	21	9261	21	U
S	19	6859	28	-

$$\boxed{\text{Ciphertext} = \text{AHA+U-}}$$

Question 2: (1 point each – 10 points)

Solve the following:

1. $\phi(15) = 8$
2. $\phi(23) = 22$
3. $\phi(41) = 40$
4. $\phi(11) + \phi(13) = 22$
5. $\phi(7) * \phi(14) = 36$
6. $8 + 18 \text{ mod } 6 = 2$
7. $23 + 29 \text{ mod } 7 = 3$
8. $16 \times 4 \text{ mod } 4 = 0$
9. $8^3 \text{ mod } 6 = 2$
10. $7^2 \text{ mod } 4 = 1$

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 5?
a. *1* b. *2* c. *4* d. *6*
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*