**Chapter 8:** **More Number theory**

**TRUE OR FALSE**

T F 1. Prime numbers play a very small role in cryptography.

T F 2. One of the useful features of the Chinese remainder theorem is that

it provides a way to manipulate potentially very large numbers

mod *M* in terms of tuples of smaller numbers.

T F 3. An important requirement in a number of cryptographic

algorithms is the ability to choose a large prime number.

T F 4. All integers have primitive roots.

T F 5. An area of ongoing research is the development of efficient

algorithms for determining if a randomly chosen large integer is a

prime number.

T F 6. The first assertion of the CRT, concerning arithmetic operations,

follows from the rules for modular arithmetic.

T F 7. Discrete logarithms are not fundamental to public-key algorithms.

T F 8. The number 37 is prime so therefore all of the positive integers

from 1 to 36 are relatively prime to 37.

T F 9. Discrete logarithms are analogous to ordinary logarithms but are

defined using modular arithmetic.

T F 10. The Chinese Remainder Theorem is believed to have been

discovered by the Chinese mathematician Agrawal in 100 A.D.

T F 11. The primitive roots for the prime number 19 are 2, 3, 10, 13, 14

and 15.

T F 12. With ordinary positive real numbers the logarithm function is the

inverse of exponentiation.

T F 13. A prime number can have a remainder when divided by positive

or negative values of itself.

T F 14. The Miller-Rabin test can determine if a number is not prime but

cannot determine if a number is prime.

T F 15. The logarithm of a number is defined to be the power to which

some positive base (except 1) must be raised in order to equal the

number.

**MULTIPLE CHOICE**

1. A \_\_\_\_\_\_\_\_\_ number can only be divided by +/- values of itself and 1 and cannot have a remainder.

A. prime B. composite

C. indexed D. positive

1. An important quantity in number theory referred to as \_\_\_\_\_\_\_\_\_\_ , is defined as the number of positive integers less than *n* and relatively prime to *n*.

A. CRT B. Miller-Rabin

C. Euler’s totient function D. Fermat’s theorem

1. Miller's test will return \_\_\_\_\_\_\_\_\_\_ if it fails to detect that *n* is not prime.

A. rejected B. inconclusive

C. composite D. discrete

1. Prime numbers play a \_\_\_\_\_\_\_\_\_ role in number theory.

A. minor B. nonessential

C. critical D. abbreviated

1. If *p* is prime and *a* is a positive integer, then *ap* = *a*(mod *p*) is an alternative form of \_\_\_\_\_\_\_\_\_ theorem.

A. Rijndael’s B. Vignere’s

C. Euler’s D. Fermat’s

1. Two numbers are relatively prime if they have \_\_\_\_\_\_\_\_\_ prime factors in common.

A. some B. zero

C. multiple D. all

1. The \_\_\_\_\_\_\_\_\_ algorithm is typically used to test a large number for primality.

A. Rijndael B. Fermat

C. Miller-Rabin D. Euler

1. The procedure TEST takes a candidate integer *n* as input and returns the result \_\_\_\_\_\_\_\_\_\_ if *n* is definitely not a prime.

A. discrete B. composite

C. inconclusive D. primitive

1. Two numbers are relatively prime if they have \_\_\_\_\_\_\_\_ prime factors in common.

A. zero B. two

C. several D. one

1. Discrete logarithms are fundamental to the \_\_\_\_\_\_\_\_\_\_\_\_ .

A. Euler algorithm B. digital signature algorithm

C. Miller-Rabin algorithm D. Rijndael algorithm

1. The procedure TEST takes a candidate integer *n* as input and returns the result \_\_\_\_\_\_\_\_\_\_ if *n* may or may not be a prime.

A. discrete B. composite

C. inconclusive D. primitive

1. If a number is the highest possible exponent to which a number can belong, it is referred to as a \_\_\_\_\_\_\_\_\_ of *n*.

A. primitive root B. composite

C. discrete logarithm D. bijection

1. For any integer *b* and a primitive root *a*  of prime number *p* we can find a unique exponent *i* . This exponent *i* is referred to as the \_\_\_\_\_\_\_\_\_\_\_ .

A. order B. discrete logarithm

C. bijection D. primitive root

1. Discrete logarithms are fundamental to a number of public-key algorithms including \_\_\_\_\_\_\_\_\_\_ key exchange and the DSA.

A. Diffie-Hellman B. Rijndael-Fadiman

C. Fermat-Euler D. Miller-Rabin

1. A one-to-one correspondence is called \_\_\_\_\_\_\_\_\_\_ .

A. a bijection B. an inclusive

C. a composite D. an index

**SHORT ANSWER**

1. A \_\_\_\_\_\_\_\_\_\_ number is an integer that can only be divided by positive and negative values of itself and 1 without having a remainder.
2. Two theorems that play important roles in public-key cryptography are Fermat's theorem and \_\_\_\_\_\_\_\_\_\_ theorem.
3. Discrete logarithms are analogous to ordinary logarithms but are defined using \_\_\_\_\_\_\_\_\_\_ arithmetic.
4. \_\_\_\_\_\_\_\_\_\_ theorem states the following: If *p* is prime and *a* is a positive integer not divisible by *p*, then *ap-1* = 1(mod *p*).
5. Two numbers are \_\_\_\_\_\_\_\_\_\_ if their greatest common divisor is 1.
6. The number of positive integers less than n and relatively prime to n is referred to as \_\_\_\_\_\_\_\_\_\_ function.
7. The \_\_\_\_\_\_\_\_\_\_ theorem states that it is possible to reconstruct integers in a certain range from their residues modulo a set of pairwise relatively prime moduli.
8. The mapping of the CRT equation is a one-to-one correspondence called a \_\_\_\_\_\_\_\_\_ between *Zm* and the Cartesian product *Zm1*  X *Zm2* X . . . X *Zmk.*
9. Discrete logarithms are fundamental to the digital signature algorithm and the \_\_\_\_\_\_\_\_\_ algorithm.
10. The \_\_\_\_\_\_\_\_\_ of a number is defined to be the power to which some positive base (except 1) must be raised in order to equal the number.
11. To determine whether an odd integer *n* is prime with a reasonable degree of confidence repeatedly invoke TEST (n) using randomly chosen values for *a*. If, at any point, TEST returns \_\_\_\_\_\_\_\_\_ then *n* is determined to be nonprime.
12. Two numbers are relatively prime if their greatest common divisor is \_\_\_\_\_\_\_\_\_ .
13. An integer *p* > 1 is a \_\_\_\_\_\_\_\_\_\_ number if and only if its only divisors are + 1 and + 1.
14. The \_\_\_\_\_\_\_\_\_ of integers *a* and *b*, expressed (gcd a, b), is an integer *c* that divides both *a* and *b* without remainder and that any divisor of *a* and *b* is a divisor of *c*.
15. Although it does not appear to be as efficient as the Miller-Rabin algorithm, in 2002 a relatively simple deterministic algorithm that efficiently determines whether a given large number is a prime was developed. This algorithm is known as the \_\_\_\_\_\_\_\_\_ algorithm.