**Chapter 10:** **Other Public-Key Cryptosystems**

**TRUE OR FALSE**

T F 1. The Diffie-Hellman key exchange is a simple public-key

algorithm.

T F 2. The security of ElGamal is based on the difficulty of

computing discrete logarithms.

T F 3. For purposes of ECC, elliptic curve arithmetic involves

the use of an elliptic curve equation defined over an

infinite field.

T F 4. The Diffie-Hellman algorithm depends on the difficulty of

computing discrete logarithms for its effectiveness.

T F 5. There is not a computational advantage to using ECC

with a shorter key length than a comparably secure TSA.

T F 6. Most of the products and standards that use public-key

cryptography for encryption and digital signatures use RSA.

T F 7. ECC is fundamentally easier to explain than either RSA or

Diffie-Hellman.

T F 8. A number of public-key ciphers are based on the use of

an abelian group.

T F 9. Elliptic curves are ellipses.

T F 10. For determining the security of various elliptic curve

ciphers it is of some interest to know the number of

points in a finite abelian group defined over an elliptic

curve.

T F 11. The form of cubic equation appropriate for

cryptographic applications for elliptic curves is

somewhat different for GF(2m) than for Zp.

T F 12. An encryption/decryption system requires that point

Pm be encrypted as a plaintext.

T F 13. The security of ECC depends on how difficult it is to

determine k given kP and P.

T F 14. A considerably larger key size can be used for ECC

compared to RSA.

T F 15. Since a symmetric block cipher produces an apparently

random output it can serve as the basis of a

pseudorandom number generator.

**MULTIPLE CHOICE**

1. The \_\_\_\_\_\_\_\_\_\_\_\_ protocol enables two users to establish a secret key using a public-key scheme based on discrete logarithms.

A. Micali-Schnorr B. Elgamal-Fraiser

C. Diffie-Hellman D. Miller-Rabin

1. \_\_\_\_\_\_\_\_\_\_ can be used to develop a variety of elliptic curve cryptography schemes.

A. Elliptic curve arithmetic B. Binary curve

C. Prime curve D. Cubic equation

1. The key exchange protocol is vulnerable to a \_\_\_\_\_\_\_\_\_\_ attack because it does not authenticate the participants.

A. one-way function B. time complexity

C. chosen ciphertext D. man-in-the-middle

1. The \_\_\_\_\_\_\_\_\_\_ cryptosystem is used in some form in a number of standards including DSS and S/MIME.

A. Rabin B. Rijnedel

C. Hillman D. ElGamal

1. A(n) \_\_\_\_\_\_\_\_\_\_ is defined by an equation in two variables with coefficients.

A. abelian group B. binary curve

C. cubic equation D. elliptic curve

1. \_\_\_\_\_\_\_\_\_\_ are best for software applications.

A. Binary curves B. Prime curves

C. Bit operations D. Abelian groups

1. An encryption/decryption system requires a point G and an elliptic group \_\_\_\_\_\_\_\_\_ as parameters.

A. Eb(a,q) B. Ea(q,b)

C. En(a,b) D. Eq(a,b)

1. For cryptography the variables and coefficients are restricted to elements in a \_\_\_\_\_\_\_\_\_\_ field.

A. primitive B. infinite

C. public D. finite

1. If three points on an elliptic curve lie on a straight line their sum is \_\_\_\_\_\_\_\_\_\_ .

A. 0 B. 1

C. 6 D. 3

1. \_\_\_\_\_\_\_\_\_\_\_\_ makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field.

A. Prime curve B. Elliptic curve cryptography(ECC)

C. abelian group D. Micali-Schnorr

1. For a \_\_\_\_\_\_\_\_\_\_\_ defined over GF(2m), the variables and coefficients all take on values in GF(2m) and in calculations are performed over GF(2m).

A. cubic equation B. prime curve

C. binary curve D. abelian group

1. If a secret key is to be used as a \_\_\_\_\_\_\_\_\_ for conventional encryption a single number must be generated.

A. discrete logarithm B. prime curve

C. session key D. primitive root

1. The Diffie-Hellman key exchange formula for calculation of a secret key by User A is:

A. K = nB x PA B. K = nA x PB

C. K = nP x BA D. K = nA x PA

1. Included in the definition of an elliptic curve is a single element denoted O and called the point at infinity or the \_\_\_\_\_\_\_\_\_\_ .

A. prime point B. zero point

C. abelian point D. elliptic point

1. The \_\_\_\_\_\_\_\_\_\_ key exchange involves multiplying pairs of nonzero integers modulo a prime number q. Keys are generated by exponentiation over the group with exponentiation defined as repeated multiplication.

A. Diffie-Hellman B. Rabin-Miller

C. Micali-Schnorr D. ElGamal

**SHORT ANSWER**

1. Elliptic curve arithmetic can be used to develop a variety of elliptic curve cryptography schemes, including key exchange, encryption, and \_\_\_\_\_\_\_\_\_\_\_ .
2. The purpose of the \_\_\_\_\_\_\_\_\_\_\_ algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages.
3. The key exchange protocol vulnerability can be overcome with the use of digital signatures and \_\_\_\_\_\_\_\_\_\_ certificates.
4. The principal attraction of \_\_\_\_\_\_\_\_\_\_, compared to RSA, is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead.
5. A(n) \_\_\_\_\_\_\_\_\_\_\_ G is a set of elements with a binary operation, denoted by \*, that associates to each ordered pair (a,b) of elements in G an element ( a\*b) in G.
6. Two families of elliptic curves are used in cryptographic applications: prime curves over Zp and \_\_\_\_\_\_\_\_\_\_ over GF(2m).
7. We use a cubic equation in which the variables and coefficients all take on values in the set of integers from 0 through p - 1 and in which calculations are performed modulo p for a \_\_\_\_\_\_\_\_\_\_ over Zp.
8. A \_\_\_\_\_\_\_\_\_\_ GF(2m) consists of 2m elements together with addition and multiplication operations that can be defined over polynomials.
9. The addition operation in elliptic curve cryptography is the counterpart of modular multiplication in RSA, and multiple addition is the counterpart of \_\_\_\_\_\_\_\_\_\_ .
10. To form a cryptographic system using \_\_\_\_\_\_\_\_\_\_ we need to

find a "hard-problem" corresponding to factoring the product of two primes or taking the discrete logarithm.

1. Eq(a,b) is an elliptic curve with parameters a, b, and q, where

\_\_\_\_\_\_\_\_\_ is a prime or an integer of the form 2m.

1. The fastest known technique for taking the elliptic curve

logarithm is known as the \_\_\_\_\_\_\_\_\_ method.

1. Asymmetric algorithms are typically much slower than

symmetric algorithms so they are not used to generate open-ended \_\_\_\_\_\_\_\_\_\_ generator bit streams.

1. The \_\_\_\_\_\_\_\_\_\_ pseudorandom number generator is

recommended in the ANSI standard X9.82 (Random Number Generation) and in the ISO standard 18031 (Random Bit Generation).

1. The PRNG variable \_\_\_\_\_\_\_\_\_\_\_ is defined in NIST SP 800-90 as

a number associated with the amount of work required to break a cryptographic algorithm or system.