QUESTION 763

Which of the following is a symmetric encryption algorithm?

A. RSA
B. Elliptic Curve
C. RC5
D. ElGamal

Correct Answer: C

QUESTION 764

How many bits is the effective length of the key of the Data Encryption Standard Algorithm?

A. 16
B. 32
C. 56
D. 64

Correct Answer: C

QUESTION 765

Compared to RSA, which of the following is true of elliptic curve cryptography?

A. It has been mathematically proved to be the more secure.
B. It has been mathematically proved to be less secure.
C. It is believed to require longer keys for equivalent security.
D. It is believed to require shorter keys for equivalent security.

Correct Answer: D

QUESTION 766

Which of the following is not a one-way algorithm?

A. MD2
B. RC2
C. SHA-1
D. DSA

Correct Answer: B

QUESTION 767

A public key algorithm that does both encryption and digital signature is which of the following?

A. RSA
B. DES
C. IDEA
D. DSS

Correct Answer: A

QUESTION 768

Which of the following encryption algorithms does not deal with discrete logarithms?

A. ElGamal
B. Diffie-Hellman
C. RSA
D. Elliptic Curve

Correct Answer: C

QUESTION 769

The RSA algorithm is an example of what type of cryptography?

A. Asymmetric key
B. Symmetric key
C. Secret Key
D. Private Key

Correct Answer: A

QUESTION 770

How many rounds are used by DES?

A. 16
B. 32
C. 64
D. 48

Correct Answer: A

QUESTION 771

Which of the following is the most secure form of triple-DES encryption?

A. DES-EDE3
B. DES-EDE1
C. DES-EEE4
D. DES-EDE2

Correct Answer: A

QUESTION 772

Which of the following algorithms does *NOT* provide hashing?

A. SHA-1
B. MD2
C. RC4
D. MD5

Correct Answer: C

QUESTION 773

Which of the following is unlike the other three?

A. ElGamal
B. Teardrop
C. Buffer Overflow
D. Smurf

Correct Answer: A

QUESTION 774

Which of the following is not an encryption algorithm?

A. Skipjack
B. SHA-1
C. Twofish
D. DEA

Correct Answer: B

QUESTION 775

Which one of the following is an asymmetric algorithm?

A. Data Encryption Algorithm.
B. Data Encryption Standard
C. Enigma
D. Knapsack

Correct Answer: D

QUESTION 776

Which of the following is *NOT* a symmetric key algorithm?

A. Blowfish
B. Digital Signature Standard (DSS)
C. Triple DES (3DES)
D. RC5

Correct Answer: B

QUESTION 777

Which of the following layers is not used by the Rijndael algorithm?

A. Non-linear layer
B. Transposition layer
C. Key addition layer
D. The linear mixing layer

Correct Answer: B

QUESTION 778

What is the basis for the Rivest-Shamir-Adleman (RSA) algorithm scheme?

A. Permutations
B. Work factor
C. Factorability
D. Reversibility

Correct Answer: C

QUESTION 779

Which of the following encryption algorithms does not deal with discrete logarithms?

A. ElGamal
B. Diffie-Hellman
C. RSA
D. Elliptic Curve

Correct Answer: C

QUESTION 780

The RSA Algorithm uses which mathematical concept as the basis of its encryption?

A. Geometry
B. Irrational numbers
C. PI (3.14159...)
D. Large prime numbers

Correct Answer: D

QUESTION 781

PGP provides which of the following? (Choose three)

A. Confidentiality
B. Accountability
C. Accessibility
D. Integrity
E. Interest
F. Non-repudiation
G. Authenticity

Correct Answer: ADG

QUESTION 782

PGP uses which of the following to encrypt data?

A. An asymmetric scheme
B. A symmetric scheme
C. A symmetric key distribution system
D. An asymmetric key distribution