B. Knapsack
C. RSA
D. Diffie-Hellman

Correct Answer: A

QUESTION 1659

Elliptic curves, which are applied to public key cryptography, employ modular exponentiation that characterizes the:

A. Knapsack problem.
B. Elliptic curve modular addition.
C. Elliptic curve discrete logarithm problem.
D. Prime factors of very large numbers.

Correct Answer: C

QUESTION 1660

Which of the following items BEST describes the standards addressed by Title II, Administrative Simplification, of the Health Insurance Portability and Accountability Act (US Kennedy-Kassebaum Health Insurance and Portability Accountability Act -HIPAA-Public Law 104-19)?

A. Transaction Standards, to include Code Sets; Security and Electronic Signatures and Privacy.
B. Security and Electronic Signatures and Privacy.
C. Transaction Standards, to include Code Sets; Unique Health Identifiers; Security and Electronic Signatures and Privacy.
D. Unique Health Identifiers; Security and Electronic Signatures and Privacy.

Correct Answer: C

QUESTION 1661

Which protocol is used to resolve a known IP address to an unknown MAC address?

A. ICMP
B. RARP
C. ARP
D. TFTP

Correct Answer: C

QUESTION 1662

Which of the following BEST describes a block cipher?

A. An asymmetric key algorithm that operates on a variable-length block of plaintext and transforms it into a fixed-length block of ciphertext.
B. A symmetric key algorithm that operates on a fixed-length block of plaintext and transforms it
into a fixed-length block of ciphertext.
C. An asymmetric key algorithm that operates on a fixed-length block of plaintext and transforms it into a fixed-length block of ciphertext.
D. A symmetric key algorithm that operates on a variable-length block of plaintext and transforms
it into a fixed-length block of ciphertext.

Correct Answer: B

QUESTION 1663
In the discretionary portion of the Bell-LaPadula mode that is based on the access matrix, how the access rights are defined and evaluated is called:

A. Validation
B. Identification
C. Authorization
D. Authentication

Correct Answer: C

QUESTION 1664
Which of the following processes establish the minimum national standards for certifying and accrediting national security systems?

A. DITSCAP
B. NIACAP
C. CIAP
D. Defense audit

Correct Answer: B

QUESTION 1665
The primary goal of the TLS Protocol is to provide:

A. Privacy and data integrity between two communicating applications.
B. Authentication and data integrity between two communicating applications.

C. Privacy and authentication between two communicating applications.
D. Privacy, authentication and data integrity between two communicating applications.

Correct Answer: A

QUESTION 1666
The Rijndael cipher employs a round transformation that is itself comprised of three layers of transformations. Which of the following is NOT one of these layers?

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

Correct Answer: A

QUESTION 1667
Context-dependent control uses which of the following to make decisions?

A. Subject or object attributes or environmental characteristics
B. Data
C. Formal models
D. Operating system characteristics

Correct Answer: A

QUESTION 1668
The Number Field Sieve (NFS) is a:

A. General purpose factoring algorithm that can be used to factor large numbers.
B. General purpose algorithm used for brute force attacks on secret key cryptosystems.
C. General purpose hash algorithm.
D. General purpose algorithm to calculate discreet logarithms.

Correct Answer: A

QUESTION 1669
The following compilation represents what facet of cryptanalysis?

A 8.2
B 1.5
C 2.8
D 4.3
E 12.7
F 2.2
G 2.0
H 6.1
I 7.0
J 0.2
K 0.8
L 4.0
M 2.4
N 6.7
O 7.5
P 1.9
Q 0.1
R 6.0
S 6.3
T 9.1
U 2.8
V 1.0
W 2.4
X 0.2
Y 2.0
Z 0.1

A. Frequency analysis
B. Cilly analysis
C. Cartouche analysis
D. Period analysis

Correct Answer: A

QUESTION 1670
In Part 3 of the Common Criteria, Security Assurance Requirements, seven predefined Packages of assurance components that make up the CC scale for rating confidence in the security of IT products and systems are called:

A. Protection Assurance Levels (PALs).
B. Security Target Assurance Levels (STALs).
C. Assurance Levels (ALs).
D. Evaluation Assurance Levels (EALs).

Correct Answer: D

QUESTION 1671
The principles of Notice, Choice, Access, Security, and Enforcement refer to which of the following?

A. Non-repudiation
B. Privacy
C. Authorization
D. Authentication

Correct Answer: B

QUESTION 1672
Which statement below is correct regarding VLANs?

A. A closed VLAN configuration is the least secure VLAN configuration.
B. A VLAN is less secure when implemented in conjunction with private port switching.
C. A VLAN is a network segmented physically, not logically.
D. A VLAN restricts flooding to only those ports included in the VLAN.

Correct Answer: D

QUESTION 1673
The protocol of the Wireless Application Protocol (WAP), which performs functions similar to SSL in the TCP/IP protocol, is called the:

A. Wireless Transport Layer Security Protocol (WTLS).
B. Wireless Transaction Protocol (WTP).
C. Wireless Session Protocol (WSP).
D. Wireless Application Environment (WAE).

Correct Answer: A

QUESTION 1674
The property that states, Reading or writing is permitted at a particular level of sensitivity, but not to either higher or lower levels of sensitivity is called the: