**COMPUTER NETWORKS : 03-60-467-01**

**University of Windsor**

**School of Computer Science**

This document contains focused statements that may be used to study for the required midterm examination. The examination covers Chapters 1-9 of the textbook.

The actual Midterm examination will be structured so that all questions are either Multiple Choice or True-False. For each Multiple Choice question, you must choose only one response which **best answers** the question. For True-False questions you must choose only one option (True or False). There may be up to five (5) response options for some questions.

The statements provided below should be used to launch a search and explore strategy. Determine if the statement is TRUE or FALSE. If false then you must determine how to modify the statement so as to make it true – it could be a single word or brief phrase that is the problem, but you will need to use the textbook and discuss with other students.

|  |  |  |
| --- | --- | --- |
| 1. | The OSI security architecture provides a systematic framework for defining security attacks, mechanisms, and services. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 2. | Security attacks are classified as either passive or aggressive. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 3. | Authentication protocols and encryption algorithms are examples of security mechanisms. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 4. | The more critical a component or service, the higher the level of required availability. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 5. | Security services include access control, data confidentiality and data integrity, but do not include authentication. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 6. | The field of network and Internet security consists of measures to deter, prevent, detect and correct security violations that involve the transmission of information. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 7. | Patient allergy information is an example of an asset with a high requirement for integrity. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 8. | The OSI security architecture was not developed as an international standard, therefore causing an obstacle for computer and communication vendors when developing security features. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 9. | Data origin authentication does not provide protection against the modification of data units. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 10. | The emphasis in dealing with active attacks is on prevention rather than detection. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 11. | The connection-oriented integrity service addresses both message stream modification and denial of service. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 12. | All the techniques for providing security have two components: a security- related transformation on the information to be sent and some secret information shared by the two principals. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 13. | Information access threats intercept or modify data on behalf of users who should not have access to that data. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 14. | The data integrity service inserts bits into gaps in a data stream to frustrate traffic analysis attempts. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 15. | Symmetric encryption is used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys, and passwords. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 16. | \_\_\_\_\_\_\_\_\_\_ is the most common method used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures. | |
| A) | Symmetric encryption |
| B) | Data integrity algorithms |
| C) | Asymmetric encryption |
| D) | Authentication protocols |

|  |  |  |
| --- | --- | --- |
| 17. | A common technique for masking contents of messages or other information traffic so that opponents can not extract the information from the message is \_\_\_\_\_\_\_\_\_\_ . | |
| A) | integrity |
| B) | encryption |
| C) | analysis |
| D) | masquerade |

|  |  |  |
| --- | --- | --- |
| 18. | \_\_\_\_\_\_\_\_\_\_ involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect. | |
| A) | Disruption |
| B) | Replay |
| C) | Service denial |
| D) | Masquerade |

|  |  |  |
| --- | --- | --- |
| 19. | The three concepts that form what is often referred to as the CIA triad are \_\_\_\_\_\_\_\_ . These three concepts embody the fundamental security objectives for both data and for information and computing services. | |
| A) | confidentiality, integrity and availability |
| B) | communication, integrity and authentication |
| C) | confidentiality, integrity, access control |
| D) | communication, information and authenticity |

|  |  |  |
| --- | --- | --- |
| 20. | A loss of \_\_\_\_\_\_\_\_\_\_ is the unauthorized disclosure of information. | |
| A) | authenticity |
| B) | confidentiality |
| C) | reliability |
| D) | integrity |

|  |  |  |
| --- | --- | --- |
| 21. | Verifying that users are who they say they are and that each input arriving at the system came from a trusted source is \_\_\_\_\_\_\_\_\_ . | |
| A) | authenticity |
| B) | credibility |
| C) | accountability |
| D) | integrity |

|  |  |  |
| --- | --- | --- |
| 22. | A \_\_\_\_\_\_\_\_\_\_ is any action that compromises the security of information owned by an organization. | |
| A) | security attack |
| B) | security service |
| C) | security alert |
| D) | security mechanism |

|  |  |  |
| --- | --- | --- |
| 23. | A \_\_\_\_\_\_\_\_\_\_ takes place when one entity pretends to be a different entity. | |
| A) | replay |
| B) | masquerade |
| C) | service denial |
| D) | passive attack |

|  |  |  |
| --- | --- | --- |
| 24. | \_\_\_\_\_\_\_\_\_\_ is the protection of transmitted data from passive attacks. | |
| A) | Access control |
| B) | Data control |
| C) | Nonrepudiation |
| D) | Confidentiality |

|  |  |  |
| --- | --- | --- |
| 25. | A(n) \_\_\_\_\_\_\_\_\_\_ service is one that protects a system to ensure its availability and addresses the security concerns raised by denial- of- service attacks. | |
| A) | replay |
| B) | availability |
| C) | masquerade |
| D) | integrity |

|  |  |  |
| --- | --- | --- |
| 26. | \_\_\_\_\_\_\_\_\_\_ threats exploit service flaws in computers to inhibit use by legitimate users. | |
| A) | Information access |
| B) | Reliability |
| C) | Passive |
| D) | Service |

|  |  |  |
| --- | --- | --- |
| 27. | A(n) \_\_\_\_\_\_\_\_\_\_ is a potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm. | |
| A) | threat |
| B) | attack |
| C) | risk |
| D) | attack vector |

|  |  |  |
| --- | --- | --- |
| 28. | The protection of the information that might be derived from observation of traffic flows is \_\_\_\_\_\_\_\_\_ . | |
| A) | connectionless confidentiality |
| B) | connection confidentiality |
| C) | traffic- flow confidentiality |
| D) | selective- field confidentiality |

|  |  |  |
| --- | --- | --- |
| 29. | Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery is a(n) \_\_\_\_\_\_\_\_\_\_\_ . | |
| A) | security audit trail |
| B) | digital signature |
| C) | encipherment |
| D) | authentication exchange |

|  |  |  |
| --- | --- | --- |
| 30. | Symmetric encryption remains by far the most widely used of the two types of encryption. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 31. | Rotor machines are sophisticated precomputer hardware devices that use substitution techniques. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 32. | Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using different keys. It is also known as non-conventional encryption. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 33. | With the use of symmetric encryption, the principal security problem is maintaining the secrecy of the key. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 34. | The process of converting from plaintext to ciphertext is known as deciphering or decryption. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 35. | The encryption/decryption algorithm will produce a different output depending on the specific secret key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 36. | When using symmetric encryption it is very important to keep the algorithm secret. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 37. | On average, half of all possible keys must be tried to achieve success with a brute-force attack. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 38. | Ciphertext generated using a computationally secure encryption scheme is impossible for an opponent to decrypt simply because the required information is not there. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 39. | Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 40. | As with Playfair, the strength of the Hill cipher is that it completely hides single letter frequencies. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 41. | A scheme known as a one-time pad is unbreakable because it produces random output that bears no statistical relationship to the plaintext. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 42. | The one-time pad has unlimited utility and is useful primarily for high-bandwidth channels requiring low security. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 43. | The most widely used cipher is the Data Encryption Standard. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 44. | Steganography renders the message unintelligible to outsiders by various transformations of the text. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 45. | \_\_\_\_\_\_\_\_\_\_ techniques map plaintext elements (characters, bits) into ciphertext elements. | |
| A) | Transposition |
| B) | Substitution |
| C) | Traditional |
| D) | Symmetric |

|  |  |  |
| --- | --- | --- |
| 46. | Joseph Mauborgne proposed an improvement to the Vernam cipher that uses a random key that is as long as the message so that the key does not need to be repeated. The key is used to encrypt and decrypt a single message and then is discarded. Each new message requires a new key of the same length as the new message. This scheme is known as a(n) \_\_\_\_\_\_\_\_\_\_ . | |
| A) | pascaline |
| B) | one-time pad |
| C) | polycipher |
| D) | enigma |

|  |  |  |
| --- | --- | --- |
| 47. | A \_\_\_\_\_\_\_\_\_\_ attack involves trying every possible key until an intelligible translation of the ciphertext is obtained. | |
| A) | brute-force |
| B) | Caesar attack |
| C) | ciphertext only |
| D) | chosen plaintext |

|  |  |  |
| --- | --- | --- |
| 48. | Techniques used for deciphering a message without any knowledge of the enciphering details is \_\_\_\_\_\_\_\_\_\_\_ . | |
| A) | blind deciphering |
| B) | steganography |
| C) | cryptanalysis |
| D) | transposition |

|  |  |  |
| --- | --- | --- |
| 49. | \_\_\_\_\_\_\_\_\_\_ attacks exploit the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used. | |
| A) | Brute-force |
| B) | Cryptanalytic |
| C) | Block cipher |
| D) | Transposition |

|  |  |  |
| --- | --- | --- |
| 50. | The \_\_\_\_\_\_\_\_\_\_ attack is the easiest to defend against because the opponent has the least amount of information to work with. | |
| A) | ciphertext-only |
| B) | chosen ciphertext |
| C) | known plaintext |
| D) | chosen plaintext |

|  |  |  |
| --- | --- | --- |
| 51. | \_\_\_\_\_\_\_\_\_ refer(s) to common two-letter combinations in the English language. | |
| A) | Streaming |
| B) | Transposition |
| C) | Digrams |
| D) | Polyalphabetic cipher |

|  |  |  |
| --- | --- | --- |
| 52. | A way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is \_\_\_\_\_\_\_\_\_\_\_ . | |
| A) | rail fence cipher |
| B) | cryptanalysis |
| C) | polyalphabetic substitution cipher |
| D) | polyanalysis cipher |

|  |  |  |
| --- | --- | --- |
| 53. | A technique referred to as a \_\_\_\_\_\_\_\_\_\_ is a mapping achieved by performing some sort of permutation on the plaintext letters. | |
| A) | transposition cipher |
| B) | polyalphabetic cipher |
| C) | Caesar cipher |
| D) | monoalphabetic cipher |

|  |  |  |
| --- | --- | --- |
| 54. | The methods of \_\_\_\_\_\_\_\_\_\_ conceal the existence of the message in a graphic image. | |
| A) | steganography |
| B) | decryptology |
| C) | cryptology |
| D) | cryptography |

|  |  |  |
| --- | --- | --- |
| 55. | The vast majority of network based symmetric cryptographic applications make use of stream ciphers. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 56. | The Feistel cipher structure, based on Shannon's proposal of 1945, dates back over a quarter of a century and is the structure used by many significant symmetric block ciphers currently in use. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 57. | DES uses a 56-bit block and a 64-bit key. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 57. | DES uses a 64-bit block and a 56-bit key. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 58. | Confusion seeks to make the statistical relationship between the plaintext and ciphertext as complex as possible in order to thwart attempts to deduce the key. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 59. | All other things being equal, smaller block sizes mean greater security. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 60. | Greater complexity in the subkey generation algorithm should lead to greater difficulty of cryptanalysis. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 61. | A prime concern with DES has been its vulnerability to brute-force attack because of its relatively short key length. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 62. | The strict avalanche criterion and the bit independence criterion appear to weaken the effectiveness of the confusion function. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 63. | DES exhibits the classic \_\_\_\_\_\_\_\_\_\_ block cipher structure, which consists of a number of identical rounds of processing. | |
| A) | Feistel |
| B) | SAC |
| C) | Shannon |
| D) | Rendell |

|  |  |  |
| --- | --- | --- |
| 64. | A sequence of plaintext elements is replaced by a \_\_\_\_\_\_\_\_\_\_ of that sequence which means that no elements are added, deleted or replaced in the sequence, but rather the order in which the elements appear in the sequence is changed. | |
| A) | permutation |
| B) | diffusion |
| C) | stream |
| D) | substitution |

|  |  |  |
| --- | --- | --- |
| 65. | A \_\_\_\_\_\_\_\_\_\_ cipher is one that encrypts a digital data stream one bit or one byte at a time. | |
| A) | product |
| B) | block |
| C) | key |
| D) | stream |

|  |  |  |
| --- | --- | --- |
| 66. | The vast majority of network-based symmetric cryptographic applications make use of \_\_\_\_\_\_\_\_ ciphers. | |
| A) | linear |
| B) | block |
| C) | permutation |
| D) | stream |

|  |  |  |
| --- | --- | --- |
| 67. | The greater the number of rounds, the \_\_\_\_\_\_\_\_\_\_ it is to perform cryptanalysis. | |
| A) | easier |
| B) | less difficult |
| C) | equally difficult |
| D) | harder |

|  |  |  |
| --- | --- | --- |
| 68. | Finite fields play a crucial role in several areas of cryptography. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 69. | Unlike ordinary addition, there is not an additive inverse to each integer in modular arithmetic. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 70. | Two integers a and b are said to be congruent modulo n, if (a mod n) = (b mod n). | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 71. | Finite fields of order p can be defined using arithmetic mod p. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 72. | The Advanced Encryption Standard uses infinite fields. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 73. | The rules for ordinary arithmetic involving addition, subtraction, and multiplication carry over into modular arithmetic. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 74. | A field is a set in which we can do addition, subtraction, multiplication and division without leaving the set. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 75. | It is easy to find the multiplicative inverse of an element in g(p) for large values of p by constructing a multiplication table, however for small values of p this approach is not practical. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 76. | Polynomial arithmetic includes the operations of addition, subtraction and multiplication. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 77. | Two integers are \_\_\_\_\_\_\_\_\_\_ if their only common positive integer factor is 1. | |
| A) | relatively prime |
| B) | congruent modulo |
| C) | polynomials |
| D) | residual |

|  |  |  |
| --- | --- | --- |
| 78. | The \_\_\_\_\_\_\_\_\_\_ of two numbers is the largest integer that divides both numbers. | |
| A) | greatest common divisor |
| B) | prime polynomial |
| C) | lowest common divisor |
| D) | integral divisor |

|  |  |  |
| --- | --- | --- |
| 79. | A \_\_\_\_\_\_\_\_\_ is a set of elements on which two arithmetic operations have been defined and which has the properties of ordinary arithmetic, such as closure, associativity, commutativity, distributivity, and having both additive and multiplicative inverses. | |
| A) | modulus |
| B) | ring |
| C) | group |
| D) | field |

|  |  |  |
| --- | --- | --- |
| 80. | A \_\_\_\_\_\_\_\_\_ is a field with a finite number of elements. | |
| A) | finite group |
| B) | finite order |
| C) | finite field |
| D) | finite ring |

|  |  |  |
| --- | --- | --- |
| 81. | The principle requirement of random or pseudorandom number generation is that the generated number stream be unpredictable. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 82. | Random numbers play an important role in the use of encryption for various network security applications. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 83. | There are well-defined tests for determining uniform distribution and independence to validate that a sequence of numbers is random. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 84. | With true random sequences each number is statistically independent of other numbers in the sequence and therefore unpredictable. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 85. | The true random number generator may simply involve conversion of an analog source to a binary output. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 86. | Examples of a pseudorandom function are decryption keys and nonces. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 87. | If the PRF does not generate effectively random 128-bit output values it may be possible for an adversary to narrow the possibilities and successfully use a brute force attack. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 88. | The seed that serves as input to the PRNG must be secure for cryptographic applications. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 89. | Three broad categories of cryptographic algorithms are commonly used to create PRNGs: symmetric block ciphers, asymmetric ciphers, and hash functions and message authentication codes. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 90. | A secret key for symmetric encryption that is generated for use for a short period of time is called a \_\_\_\_\_\_\_\_\_ . | |
| A) | strategic key |
| B) | sequence key |
| C) | session key |
| D) | stream key |

|  |  |  |
| --- | --- | --- |
| 91. | A \_\_\_\_\_\_\_\_\_\_ is used to produce a pseudorandom string of bits of some fixed length. | |
| A) | PRF |
| B) | PRNG |
| C) | OFB PRNG |
| D) | TRNG |

|  |  |  |
| --- | --- | --- |
| 92. | A source that is effectively random is referred to as a(n) \_\_\_\_\_\_\_\_\_\_ . | |
| A) | open source |
| B) | entropy source |
| C) | keystream |
| D) | seed |

|  |  |  |
| --- | --- | --- |
| 93. | The best that can be done to determine if a PRNG generates numbers that have the characteristic of randomness is on the basis of multiple tests. These tests should seek to establish uniformity, scalability, and \_\_\_\_\_\_\_\_\_\_ . | |
| A) | consistency |
| B) | authentication |
| C) | frequency |
| D) | sequencing |

|  |  |  |
| --- | --- | --- |
| 94. | The \_\_\_\_\_\_\_\_\_\_ test is the most basic test of randomness and must be included in any test suite. | |
| A) | frequency |
| B) | runs |
| C) | unpredictability |
| D) | Maurer |

|  |  |  |
| --- | --- | --- |
| 95. | 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. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 96. | All integers have primitive roots. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 97. | An area of ongoing research is the development of efficient algorithms for determining if a randomly chosen large integer is a prime number. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 98. | Discrete logarithms are not fundamental to public-key algorithms. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 99. | The number 37 is prime so therefore all of the positive integers from 1 to 36 are relatively prime to 37. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 100. | The Miller-Rabin test can determine if a number is not prime but cannot determine if a number is prime. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 101. | 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 |

|  |  |  |
| --- | --- | --- |
| 102. | Discrete logarithms are fundamental to the \_\_\_\_\_\_\_\_\_\_\_\_ . | |
| A) | Euler algorithm |
| B) | digital signature algorithm |
| C) | Miller-Rabin algorithm |
| D) | Rijndael algorithm |

|  |  |  |
| --- | --- | --- |
| 103. | Discrete logarithms are fundamental to a number of public-key algorithms including \_\_\_\_\_\_\_\_\_\_ key exchange and the DSA. | |
| A) | Rijndael-Fadiman |
| B) | Miller-Rabin |
| C) | Diffie-Hellman |
| D) | Fermat-Euler |

|  |  |  |
| --- | --- | --- |
| 104. | Asymmetric encryption can be used for confidentiality but not for authentication. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 105. | Public-key encryption is more secure from cryptanalysis than symmetric encryption. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 106. | If the authenticator is encrypted with the sender's private key, it serves as a signature that verifies origin, content, and sequencing. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 107. | A trap-door one-way function is easy to calculate in one direction and infeasible to calculate in the other direction unless certain additional information is known. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 108. | A public-key encryption scheme is not vulnerable to a brute-force attack. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 109. | Before the application of the public-key cryptosystem each participant must generate a pair of keys. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 110. | Timing attacks are ciphertext attacks that are only applicable to RSA. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 111. | The Playfair algorithm is based on the use of a 5 × 5 matrix of letters constructed using a keyword. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 112. | The Playfair algorithm encrypts three letters at a time. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 113. | An encryption scheme is said to be computationally secure if \_\_\_\_\_\_\_\_\_\_ . | |
| A) | the cost of breaking the cipher exceeds the value of the encrypted information |
| B) | the time required to break the cipher exceeds the useful lifetime of the information |
| C) | the amount of time required to break the cipher is greater than the fastest CPUs |
| D) | Both A and B responses are correct. |

|  |  |  |
| --- | --- | --- |
| 114. | The avalanche effect is a property of any encryption algorithm such that a small change in \_\_\_\_\_\_\_\_\_\_\_ produces a significant change in the ciphertext. | |
| A) | the plaintext |
| B) | the key |
| C) | Both A and B responses are correct. |
| D) | None of the responses above are correct. |

|  |  |  |
| --- | --- | --- |
| 115. | A group is a set of elements that is closed under a binary operation and that is associative and that includes an identity element and an inverse element. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 116. | A ring is a set of elements that is closed under two binary operations, addition and subtraction, with the following: the addition operation is a group that is commutative; the multiplication operation is associative and is distributive over the addition operation. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 117. | A field is a ring in which the multiplication operation is commutative, has no zero divisors, and includes an identity element and an inverse element. | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 118. | The multiplicative inverse of 3, modulo 5, is \_\_\_\_\_\_\_\_\_\_ . | |
| A) | 1 |
| B) | 2 |
| C) | 3 |
| D) | 4 |
| E) | None of the responses above is correct. |

|  |  |  |
| --- | --- | --- |
| 119. | The additive inverse of 3, modulo 5, is \_\_\_\_\_\_\_\_\_\_ . | |
| A) | 1 |
| B) | 2 |
| C) | 3 |
| D) | 4 |
| E) | None of the responses above is correct. |

|  |  |  |
| --- | --- | --- |
| 120. | A typical intermediate round in AES encryption consists of the steps: Substitute bytes; \_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_ . | |
| A) | Shift rows and Mix columns |
| B) | Mix rows and Shift columns |
| C) | Shift rows, Mix columns and Add round key |
| D) | Shift rows, Mix columns and Expand key |
| E) | None of the responses above is correct. |

|  |  |  |
| --- | --- | --- |
| 121. | Within GF(2n), a polynomial m(x) is called irreducible if and only if it cannot be expressed a product of two polynomials, both of degree lower than that of m(x). | |
| A) | True |
| B) | False |

|  |  |  |
| --- | --- | --- |
| 122. | In AES, how many bytes in **State** are affected by ShiftRows? | |
| A) | 4 |
| B) | 8 |
| C) | 12 |
| D) | 14 |
| E) | None of the responses above is correct. |

|  |  |  |
| --- | --- | --- |
| 123. | The \_\_\_\_\_\_\_\_\_\_\_ allows for block lengths of 128, 192 or 256 bits. | |
| A) | Rijndael cipher |
| B) | DES algorithm |
| C) | AES algorithm |
| D) | All of these responses are correct. |

|  |  |  |
| --- | --- | --- |
| 124. | To apply a block cipher in a variety of applications, five modes of operation have been defined by NIST, including modes \_\_\_\_\_\_\_\_\_ . | |
| A) | DES and AES |
| B) | CBC and CTR |
| C) | ECB and OFB |
| D) | Both B and C responses are correct. |

|  |  |  |
| --- | --- | --- |
| 125. | A time-varying value that has at most a negligible chance of repeating is called a \_\_\_\_\_\_\_\_\_\_\_ . | |
| A) | temporal key |
| B) | nonce |
| C) | cipher |
| D) | None of these responses is correct. |

|  |  |  |
| --- | --- | --- |
| 126. | The minimum number of distinct keys used in triple encryption is \_\_\_\_\_\_\_\_\_\_\_ . | |
| A) | 1 |
| B) | 2 |
| C) | 3 |
| D) | None of these responses is correct. |

|  |  |  |
| --- | --- | --- |
| 127. | If r and n are relatively prime integers with n > 0. and if φ(n) is the least positive exponent m such that am ≡ 1 mod n, then r is called a \_\_\_\_\_\_\_\_\_ modulo n. | |
| A) | simple factor |
| B) | relative prime |
| C) | primitive root |
| D) | None of these responses is correct. |

|  |  |  |
| --- | --- | --- |
| 128. | A group G is said to be \_\_\_\_\_\_\_\_\_ if it satisfies the condition a\*b = b\*a for all a,b in G. | |
| A) | abelian |
| B) | commutative |
| C) | cyclic |
| D) | infinite |