001. -------------refers to unauthorized access to or interception of data. **D**

A repudiation B replaying
C modification D Snooping

002. Find the solution of x^2 16 mod 23. **A**

A x = 4 and 19 B x = 6 and 17
C x = 11 and 12 D x = 7 and 16

003. The --------of data can be threatened by several kinds of attacks: modification, masquerading,replaying, and repudiation. **B**

A Availability B integrity
C Authenticity D Confidentiality

004. The linear combination of gcd(252,198)=18 is---------- **C**

A 252*5-198*4 B 252*4-198*2
C 252*4-198*5 D 252*2-198*5

005. In computer security, _______ means that the information contained in a computer system can only be read by authorized persons. **A**

A Confidentiality B Integrity
C Availability D Authenticity

006. -5 mod -3 = **C**

A 3 B 2
C 1 D 5

007. In computer security, _______ means that active computer systems can only be modified by authorized persons. **B**

A Confidentiality B Integrity
C Availability D Authenticity

008. The two types of attacks threaten the ----------of information: snoopingand traffic analysis. **C**

A Integrity B Availability
C confidentiality D Authenticity

009. ------- is an attack threatening availability **B**

A Repudiation B Denial of Service
C Replaying D Masquerading

010. The solution of linear congruence 4x5(mod 9) is ------------ **B**

A 6(mod 9) B 8(mod 9)
C 9(mod 9) D 10(mod 9)

011. In -----------, the attackers goal is just to obtain information **C**

A Slow attack B Active attack
C passive attack D sleep attack

012. The value of 5^{2003} mod 7 is--------- **A**

A 3 B 4
C 8 D 9

013. In ------, the sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message. **A**

A repudiation B replaying
C modification D Snooping

014. The inverse of 7 modulo 26 is----- **C**

A 12 B 14
C 15 D 20

015. -------------happens when the attacker impersonates somebody else. **D**

A Replaying B Snooping
C Traffic Analysis D Masquerading

016. The inverse of 3 modulo 7 is -------- **B**

A -1 B -2
C -3 D -4

017. Attacks that threaten the integrity and availability are --------------- **B**

A Slow attack B Active attack
C passive attack D sleep attack

018. Expand ITU-T: **D**

A International Telecom Union-Telecom Standardization Section
B International Telecom Union-Telecom Standardization Sector
C International Telecommunication Union-Telecommunication Standardization Section
D International Telecommunication Union-Telecommunication Standardization Sector

019. ---------is designed to protect data from disclosure attack **C**

A Data Integrity B nonrepudiation
C Data Confidentiality D Access Control

020. ---------- is designed to protect data from modification, insertion, deletion, andreplaying by an adversary **A**

A Data Integrity B nonrepudiation
C Data Confidentiality D Access Control

021. An --------attack may change the data or harm the system **A**

A active B passive
C slow D fast

022. A binary operation takes ------- inputs and creates -------- output **C**

A 1, 2 B 2, 2
C 2, 1 D 2, 0

023. Attacks that threaten confidentiality: snooping and traffic analysis, are ------------attacks **D**

A fast B slow
C active D passive

024. ab(modn) if and only if n|(ab) . **B**

A n|(a) . B n|(ab) .
C n|(a+b) . D n|(a*b) .

025. if a | 1, then a = ±------------- **A**

A 1 B 0
C 2 D a

026. Find the greatest common divisor of 2740 and 1760. **D**

A 25 B 5
C 10 D 20

027. A linear Diophantine equation of two variables is---------------. **C**

A xy+a=y B xy = c
C ax + by = c D x+y=xy

028. The result of the modulo operation with modulus n is always an integer between 0 and---------- **B**

A n B n 1
C n+1 D n/2

029. -------is designed to prevent snooping and traffic analysis attack **C**

A Data Integrity B nonrepudiation
C Data Confidentiality D Access Control

030. In ----------with proof of delivery, the sender of data can later prove that data were delivered to the intended recipient **B**

A Data Integrity B nonrepudiation
C Data Confidentiality D Access Control

031. In ---------with proof of the origin, the receiver of the data can later prove the identity of the sender if denied **B**

A Data Integrity B nonrepudiation
C Data Confidentiality D Access Control

032. gcd (36, 10)= **D**

A 6 B 4
C 1 D 2

033. In Zn, two numbers a and b are the multiplicative inverse of each other if **A**

A a + b 1 (mod n) B a + b 0 (mod n)
C a + b -1 (mod n) D a + b k (mod n)

034. The multiplicative Inverse of 1234 mod 4321 is --------- **A**

A 3239 B 3213
C 3242 D 3225

035. (1,723,345 + 2,124,945) mod 11=-------- **C**

A 8 B 10
C 6 D 9

036. What is 11 mod 7 and -11 mod 7? **D**

A 4 and 5 B 4 and 4
C 5 and 3 D 4 and -4

037. What is the result of the following operation? Subtract 11 from 7 in Z13 **C**

A 6 B 0
C 9 D 17

038. In Zn, two numbers a and b are additive inverses of each other if **B**

A a + b 1 (mod n) B a + b 0 (mod n)
C a + b -1 (mod n) D a + b k (mod n)

039. What is the result of the following operation? Add 7 to 14 in Z15 **A**

A 6 B 10
C 9 D 17

040. What is the result of the following operation? Multiply 11 by 7 in Z20 **D**

A 6 B 10
C 9 D 17

041. ----------- means selecting and continuously changing different available routes between the sender and the receiver to prevent the opponent from eavesdropping on a particular route. **B**

A Notarization B Routing control
C Traffic padding D Access control

042. -----------uses methods to prove that a user has access right to the data or resources owned by a system. **D**

A Notarization B Routing control
C Traffic padding D Access control

043. --------- refers to selecting a third trusted party to control the communication between two entities. **A**

A Notarization B digital signature
C authentication D enciphering

044. In -----------exchange, two entities exchange some messages to prove their identity to each other **C**

A Notarization B digital signature
C authentication D enciphering

045. -5 mod -3 = **C**

A 3 B 2
C 1 D 5

046. ----------- means inserting some bogus data into the data traffic to thwart the adversarys attempt to use the traffic analysis. **C**

A Notarization B Routing control
C Traffic padding D Access control

047. GCD(a,b) = GCD(b,a mod b) **A**

A true B false
C infinity D cantt defined

048. 7x 6 mod 5. Then the value of x is----------- **B**

A 2 B 3
C 4 D 5

049. Find the multiplicative inverse of 11 in Z26 **B**

A	-7	B	19
C	-2	D	26

050. A residue matrix has a multiplicative inverse if gcd (det(A), n) = ------------ **C**

A	0	B	Doesnt exist
C	1	D	-1

051. DES follows **C**

A	Hash Algorithm	B	Caesars Cipher
C	Feistel Cipher Structure	D	SP Networks

052. For the group S_n of all permutations of n distinct symbols, what is the number of elements in S_n? **D**

A	n	B	n-1
C	2n	D	n!

053. The integer a in Zn has a multiplicative inverse if and only if gcd (n, a) ---------- **A**

A	1 (mod n)	B	-1 (mod n)
C	0 (mod n)	D	k (mod n)

054. The extended Euclidean algorithm finds the multiplicative inverses of b in Zn when n and b are given and gcd (n, b) = ----------- **C**

A	0	B	b
C	1	D	-1

055. A -----------is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature. **B**

A	Notarization	B	digital signature
C	authentication	D	enciphering

056. cryptography and steganography are used for ------------- **D**

A	Notarization	B	digital signature
C	authentication	D	enciphering

057. In the DES algorithm the round key is __ bit and the Round Input is ______bits. **A**

A	48, 32	B	64,32
C	56, 24	D	32, 32

058. How many numbers cannot be used in GF(p) in 2^n where n=4? **C**

A	2	B	3
C	5	D	1

059. In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via _____________ **A**

A	Scaling of the existing bits	B	Duplication of the existing bits
C	Addition of zeros	D	Addition of ones

060. On multiplying $(x^5+ x^2+ x)$ by $(x^7+ x^4+ x^3+ x^2+ x)$ in $GF(2^8)$ with irreducible polynomial $(x^8+ x^4+ x^3+ x + 1)$ we get------------- **D**

A	$x^{12}+x^7+x^2$	B	$x^5+x^3+x^3$
C	$x^5+x^3+x^2+x$	D	$x^5+x^3+x^2+x+1$

061. The DES algorithm has a key length of ----- **C**

A	128 Bits	B	32 Bits
C	64 Bits	D	16 Bits

062. The GCD of $x^3+ x + 1$ and $x^2+ x + 1$ over GF(2) is--------- **A**

A	1	B	x + 1
C	x^2	D	$x^2+ 1$

063. The DES Algorithm Cipher System consists of ____________rounds (iterations) each with a round key **D**

A	12	B	18
C	9	D	16

064. On multiplying $(x^6+x^4+x^2+x+1)$ by (x^7+x+1) in $GF(2^8)$ with irreducible polynomial $(x^8+$ **B**

$x^4 + x^3 + x + 1$) we get-----

A $x^7+x^6+x^3+x^2+1$ B x^7+x^6+1

C $x^6+x^5+x^2+x+1$ D x^7+x^6+x+1

065. How many keys does the Triple DES algorithm use? **C**

A 2 B 3

C 2 or 3 D 3 or 4

066. How many rounds does the AES-192 perform? **B**

A 10 B 12

C 14 D 16

067. What is the size of the key in the SDES algorithm? **D**

A 24 bits B 16 bits

C 20 bits D 10 bits

068. How many rounds does the AES-256 perform? **C**

A 10 B 12

C 14 D 16

069. The number of unique substitution boxes in DES after the 48 bit XOR operation are--- **A**

A 8 B 4

C 6 D 12

070. AES uses a ____________ bit block size and a key size of __________ bits. **D**

A 128; 128 or 256 B 64; 128 or 192

C 256; 128, 192, or 256 D 128; 128, 192, or 256

071. In DES, the Initial Permutation table/matrix is of size--------- **C**

A 16x8 B 12x8

C 8x8 D 4x8

072. The GCD of $x^3 - x + 1$ and $x^2 + 1$ over GF(3) is------ **A**

A 1 B x

C x + 1 D $x^2 + 1$

073. Which of the 4 operations are false for each round in the AES algorithm i) Substitute Bytes ii) Shift Columns iii) Mix Rows iv) XOR Round Key **B**

A i) only B ii) iii) and iv)

C ii) and iii) D only iv)

074. The combination of the set and the operations that are applied to the elements of the set is calledan/a ------- **A**

A algebraic structure B group

C commutative group D abelian group

075. In AES the 4x4 bytes matrix key is transformed into a keys of size _________ **D**

A 32 words B 64 words

C 54 words D 44 words

076. A ------- is a set of elements with a binary operation that satisfies four axioms. **B**

A algebraic structure B group

C commutative group D abelian group

077. The 4x4 byte matrices in the AES algorithm are called----- **A**

A States B Words

C Transitions D Permutations

078. The DES function has _______ components. **C**

A 2 B 3

C 4 D 5

079. What is the expanded key size of AES-192? **C**

A 44 words B 60 words

C 52 words D 36 words

080. ________ DES was designed to increase the size of the DES key. **B**

A Double B Triple

C Quadruple D zero

081. A ring involves --------operations **C**

A one | B three
C two | D four

082. Which of the following is a faulty S-AES step function? **B**

A Add round key | B Byte substitution
C Shift rows | D Mix Columns

083. What is the block size in the Simplified AES algorithm? **B**

A 8 bits | B 40 bits
C 16 bits | D 36 bits

084. How many computation rounds does the simplified AES consists of? **B**

A 5 | B 2
C 8 | D 10

085. If a subgroup of a group can be generated using the power of an element, the subgroup is called the -----------subgroup. **A**

A cyclic | B finite
C infinite | D closed

086. On comparing AES with DES, which of the following functions from DES does not have an equivalent AES function? **C**

A permutation p | B f function
C swapping of halves | D xor of subkey with function f

087. ----------theorem relates the order of a group to the order of its subgroup **D**

A Euclidian | B tailor
C fermat | D Lagranges

088. Which function can be used in AES multiplication? **B**

A $m(x)=x^7+x^4+x^3$ | B $m(x)=x^8+x^4+x^3+x+1$
C $m(x)=x^8+x^3+x^2+x+1$ | D $m(x)=x^8+x^5+x^3+x$

089. Multiplication of polynomials in GF(2n) can be achieved using --------andexclusive-or operations. **D**

A AND | B rotate
C shift-right | D shift-left

090. Polynomials representing --------bit words use two fields: GF(2) and GF(2n). **C**

A 2n | B 2
C n | D 8

091. A Galois field, GF(p^n), is a finite field with --------elements. **D**

A pn | B n
C p | D p^n

092. How many step functions do Round 1 and 2 each have in S-AES? **A**

A 4 and 3 | B Both 4
C 1 and 4 | D 3 and 4

093. Addition/subtraction in GF(2) is the same as the -------operation **B**

A OR | B XOR
C AND | D NOR

094. How many round keys are generated in the AES algorithm? **A**

A 11 | B 10
C 8 | D 12

095. DES uses a key generator to generate sixteen _______ round keys. **B**

A 32-bit | B 48-bit
C 54-bit | D 42-bit

096. A ------------- is invertible, but compression and expansion P-boxes are not. **C**

A P-Box | B Compression P-Box
C Straight P-Box | D Expansion P-boxes

097. A(n) _____ is a keyless substitution cipher with N inputs and M outputs that uses a formula to define the relationship between the input stream and the output stream. **A**

A S-box B P-box
C T-box D B-box

098. Which one of the following is not a possible key length for the Advanced Encryption Standard Rijndael cipher? **A**
A 56 bits B 128 bits
C 192 bits D 256 bits

099. A ---------- parallels the traditional transposition cipher for characters **B**
A S-Box B P-Box
C T-Box D N-Box

100. The Advanced Encryption Standard (AES), has three different configurations with respect to the number of rounds and----------- **C**
A data size B round size
C key size D encryption size

101. ----------are used when we need to permute bits and the same time increase the number of bits for the next stage **D**
A P-Box B Compression P-Box
C Straight P-Box D Expansion P-boxes

102. To provide security, AES uses ----------- types of transformations **D**
A 2 B 3
C 5 D 4

103. (231)= **D**
A 230 B 60
C 80 D 120

104. In a nonsynchronous stream cipher, the key depends on either the plaintext or ciphertext **C**
A synchronous B modern
C nonsynchronous D general

105. ------------hides the relationship between the ciphertext and the plaintext. **D**
A Key generator B Confusion
C Key schedule D Diffusion

106. ---------hides the relationship between the ciphertext and the key. **B**
A Key generator B Confusion
C Key schedule D Diffusion

107. In a --------------stream cipher the key is independent of the plaintext or ciphertext **A**
A synchronous B modern
C asynchronous D general

108. In a ----------------stream cipher, each r-bit word in the plaintext stream is enciphered using an r-bit word in the key stream to create the corresponding r-bit word in the ciphertext stream. **B**
A synchronous B modern
C asynchronous D general

109. The inverse of 49 mod 37 is -- **D**
A 31 B 23
C 22 D 34

110. Find the primitive roots of G=<Z11*, x>? **D**
A {2, 6, 8} B {2, 5, 8}
C {3, 4, 7, 8} D {2, 6, 7, 8}

111. Find the number of primitive roots of G=<Z11*, x>? **C**
A 5 B 6
C 4 D 10

112. Find the order of group G= <Z20*, x> **D**
A 6 B 9
C 10 D 8

113. Find x for the CRT when x= 2 mod 3; x= 3 mod 5; x = 2 mod 7 **C**

A 33   B 22
C 23   D 31

114. Which among the following values: 17, 20, 38, and 50, does not have primitive roots in the group G = <Zn*, x>? **B**
A 17   B 20
C 38   D 50

115. Consider a function: f(n) = number of elements in the set {a: 0 <= a < n and gcd(a,n) = 1}. What is this function? **B**
A Primitive   B Totient
C Primality   D Primitive, totient, primality

116. -----------theoremstates that ifpis aprime number, then for anyintegera, the numbera^{p}-ais an integer multiple ofp **D**
A Euclidean   B Eulers
C Chinese remainder   D Fermat &#39s little

117. x- 4x - 16 = 0 (mod 29) **B**
A x = 6, 24 (mod 29)   B x = 9, 24 (mod 29)
C x = 9, 22 (mod 29)   D x = 6, 22 (mod 29)

118. 17 x^{2} 10 (mod 29) **C**
A x = 3, 22 (mod 29)   B x = 7, 28 (mod 29)
C x = 2, 27 (mod 29)   D x = 4, 28 (mod 29)

119. Six teachers begin courses on Monday Tuesday Wednesday Thursday Friday and Saturday, respectively, and announce their intentions of lecturing at intervals of 2,3,4,1,6 and 5 days respectively. Sunday lectures are forbidden. When first will all the teachers feel compelled to omit a lecture? Use CRT. **B**
A 354   B 371
C 432   D 213

120. The number of primes of the form |n ^{2} 6n + 5| where n is an integer is----- **C**
A 0   B 1
C 2   D 3

121. How many primitive roots are there for 25? **D**
A 4   B 5
C 7   D 8

122. whenmandnare coprime, (m*n) = ------------- **A**
A (m)*(n)   B (m)+(n)
C (m)/(n)   D (m)**(n)

123. The inverse of 37 mod 49 is - **C**
A 23   B 12
C 4   D 6

124. Does the set of residue classes (mod 3) form a group with respect to modular addition? **A**
A Yes   B No
C Cant Say   D Insufficient Data

125. Using Differential Crypt-analysis, the minimum computations required to decipher the DES algorithm is--- **D**
A 256   B 243
C 255   D 247

126. Find the set of quadratic residues in the set - Z11* = { 1, 2, 3, 4, 5, 6, 7, 8, 9, 10} **D**
A QR set = {1, 2, 4, 5, 9} of Z11*   B QR set = {1, 3, 6, 5, 9} of Z11*
C QR set = {1, 3, 4, 9,10} of Z11*   D QR set = {1, 3, 4, 5, 9} of Z11*

127. x^{7} 17 (mod 29) **B**
A x = 8, 9, 12, 13, 15, 24, 28 (mod 29)   B x = 8, 10, 12, 15, 18, 26, 27 (mod 29)
C x = 8, 10, 12, 15, 17, 24, 27 (mod 29)   D x = 8, 9, 13, 15, 17, 24, 28 (mod 29)

128. Consider the following system of two equations (congruences):x 12 mod 29x 7 mod 15According to Chinese Remainder Theorem (CRT), which of the following is true **B**

about x?

A x has no solution in (mod 29 15)
B x has exactly one solution in (mod 29 15)
C x has more than one solution in (mod 29 15)
D x has four solutions in (mod 29 15) because there are two equations

129. How many primitive roots are there for 19? **D**

A 4
B 5
C 3
D 6

130. The GCD of x5+x4+x3 - x2 - x + 1 and x3 + x2 + x + 1 over GF(3) is--- **C**

A 1
B x
C x + 1
D $x^2 + 1$

131. What is the Discrete logarithm to the base 13 (mod 19) for a =13? **B**

A 14
B 1
C 8
D 17

132. Find a number x between 0 and 28 with x^{85} congruent to 6 mod 29. **C**

A 22
B 12
C 6
D 18

133. What is the Discrete logarithm to the base 10 (mod 19) for a =7? **A**

A 12
B 14
C 8
D 11

134. Find the solution of x^2 16 mod 23 **B**

A x = 6 and 17
B x = 4 and 19
C x = 11 and 12
D x = 7 and 16

135. 3^{201}mod 11 = **A**

A 3
B 5
C 6
D 10

136. Primitive Polynomial is also called a ____ i) Perfect Polynomial ii) Prime Polynomial iii) Irreducible Polynomial iv) Imperfect Polynomial **A**

A ii) and iii)
B only iii)
C iv) and ii)
D only i)

137. (41)= **A**

A 40
B 18
C 20
D 22

138. The ---------- theorem is used to solve a set of congruent equations with one variable but different moduli that are relatively prime **C**

A Euclidean
B Eulers
C Chinese remainder
D Fermat &#39s little

139. If the multiplicative inverse of 53 modulo 21 exists, then which of the following is true? **B**

A GCD(53,21)=29
B GCD(53,21)=1
C GCD(53,21)=53
D GCD(53,21)=12

140. A composite is a positive integer with at least ----------divisors **C**

A four
B three
C two
D zero

141. What is the Discrete logarithm to the base 15 (mod 19) for a =9? **D**

A 3
B 7
C 12
D 4

142. How many primitive roots are there for 25? **D**

A 4
B 5
C 7
D 8

143. Find a number x between 0 and 28 with x^{85}congruent to 6 mod 35. **A**

A 6
B 32
C 8
D 28

144. If n is a prime, mod n = $\pm$---------- **B**

A 0 B 1
C p D n

145. Find the order of the group G = <Z12*, x>? **A**
A 4 B 5
C 6 D 2

146. How many primitive roots does Z<19> have? **D**
A 5 B 8
C 7 D 6

147. (27)= **D**
A 6 B 12
C 26 D 18

148. -------------- function finds the number of integers that are both smaller than n and relatively prime to n. **B**
A Euclidean B Eulers totient
C Chinese remainder D Fermat &#39s little

149. 7^3mod 19 = **B**
A 18 B 1
C 14 D 12

150. The modulus in the Fermat theorem is a ------------ **C**
A odd B even
C prime D integer