

University of Mumbai
Examination 2020

Program: BE Electronics and Telecommunication Engineering

Curriculum Scheme: Revised 2016

Examination: Third Year Semester V

Course Code and Course Name: ECCDLO-5014 Data Compression & Encryption

Time: 1 hour

Max. Marks: 50

=====

Q1.	What are the characteristics of anomaly based IDS?
Option A:	It models the normal usage of network as a noise characterization
Option B:	It doesn't detect novel attacks
Option C:	Anything distinct from the noise is not assumed to be intrusion activity
Option D:	It detects based on signature
Q2.	What is the key size allowed in PGP?
Option A:	1024-1056
Option B:	1024-4056
Option C:	1024-4096
Option D:	1024-2048
Q3.	What are the characteristics of signature based IDS?
Option A:	Most are based on simple pattern matching algorithms
Option B:	It is programmed to interpret a certain series of packets
Option C:	It models the normal usage of network as a noise characterization
Option D:	Anything distinct from the noise is assumed to be intrusion activity
Q4.	What are characteristics of Network based IDS?
Option A:	They look for attack signatures in network traffic
Option B:	Filter decides which traffic will not be discarded or passed
Option C:	It is programmed to interpret a certain series of packet
Option D:	It models the normal usage of network as a noise characterization
Q5.	Which is of the following uses Sliding window technique
Option A:	Lz77
Option B:	Lzw
Option C:	arithmetic coding
Option D:	Lz78
Q6.	Extended Huffman code is best suited for
Option A:	for logarithmic scale
Option B:	for skewed probabilities
Option C:	Increasing probabilities

University of Mumbai
Examination 2020

Option D:	Decreasing probabilities
Q7.	Code efficiency is
Option A:	avg information per message /avg codeword length
Option B:	avg information per message - avg codeword length
Option C:	avg information per message +avg codeword length
Option D:	avg codeword length /avg information per message
Q8.	Prob a1= 0.2,prob a2=0.2 , prob a3=0.25 , prob a4=0.05 , prob a5=0.15, prob a6=0.15 find entropy
Option A:	3
Option B:	3.25
Option C:	2
Option D:	2.25
Q9.	compression ratio is.....
Option A:	Uncompressed size /compressed size
Option B:	compressed size/ Uncompressed size
Option C:	compression gain/compression factor
Option D:	compression factor/ compression gain
Q10.	compression factor is.....
Option A:	Uncompressed size /compressed size
Option B:	compressed size/ Uncompressed size
Option C:	compression gain/compression factor
Option D:	compression factor/ compression gain
Q11.	Without losing quality, JPEG-2000 can achieve compression ratios of
Option A:	20:1
Option B:	2000:1
Option C:	200:1
Option D:	2:1
Q12.	The full form of JPG or JPEG is
Option A:	Joint Photographic Expert Group
Option B:	Joint Photographic Excel Group
Option C:	Joint Performance Expert Group
Option D:	Joint Performance Excel Group
Q13.	Adaptive DPCM is used to
Option A:	Increase bandwidth
Option B:	Decrease bandwidth
Option C:	Increase SNR
Option D:	Decrease SNR

University of Mumbai
Examination 2020

Q14.	In public key cryptosystem _____ keys are used for encryption and decryption.
Option A:	Same
Option B:	Different
Option C:	Encryption Keys
Option D:	Decryption Keys
Q15.	Private key algorithm is used for _____ encryption and public key algorithm is used for _____ encryption.
Option A:	Messages, session key
Option B:	Session key, messages
Option C:	Can be used for both
Option D:	Cant be used for both
Q16.	An asymmetric-key ciphers uses
Option A:	1 key
Option B:	2 key
Option C:	3 key
Option D:	4 key
Q17.	In Asymmetric-Key Cryptography, the two keys, e and d, have a special relationship to
Option A:	Others
Option B:	Data
Option C:	Keys
Option D:	Each other
Q18.	MPEG stands for
Option A:	Motion Picture Express Group
Option B:	Motion Picture Expert Group
Option C:	Motion Picture Export Group
Option D:	Multiplexing Picture Expert Group
Q19.	What does AVI stand for
Option A:	Audio for voice on internet
Option B:	Audio voice interleaved
Option C:	Audio video interleaved
Option D:	Adapted video for internet
Q20.	Which of the following two file formats has a smaller file size:
Option A:	MP3
Option B:	WAV
Option C:	MP4
Option D:	AVI
Q21.	The Caesar cipher is a _____ cipher that has a key of 3.

University of Mumbai
Examination 2020

Option A:	Transposition
Option B:	Additive
Option C:	Shift
Option D:	AES
Q22.	A _____ is a keyless substitution cipher with N inputs an M outputs that uses a formula to define the relationship between the input stream and the output stream
Option A:	S-box
Option B:	P-box
Option C:	T-box
Option D:	A-box
Q23.	DES is a _____ method adopted by the U.S. government.
Option A:	symmetric-key
Option B:	asymmetric-key
Option C:	either symmetric-key or asymmetric-key
Option D:	both symmetric-key and asymmetric-key
Q24.	DES has an initial and final permutation block and
Option A:	14
Option B:	15
Option C:	16
Option D:	17
Q25.	DES uses a key generator to generate sixteen _____ round keys
Option A:	32-bit
Option B:	48-bit
Option C:	54-bit
Option D:	42-bit