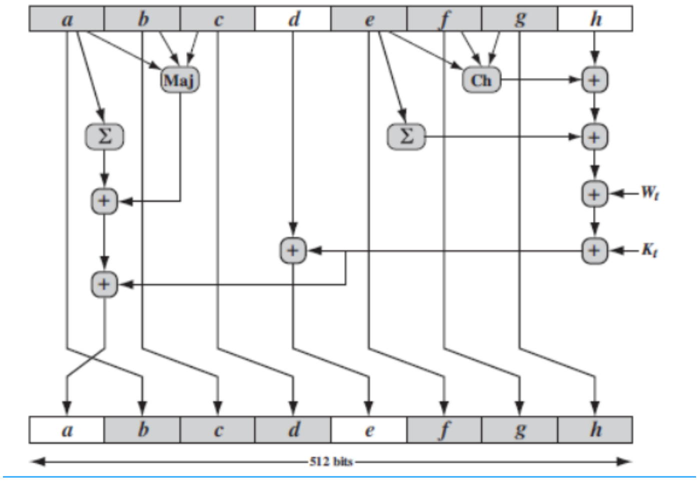
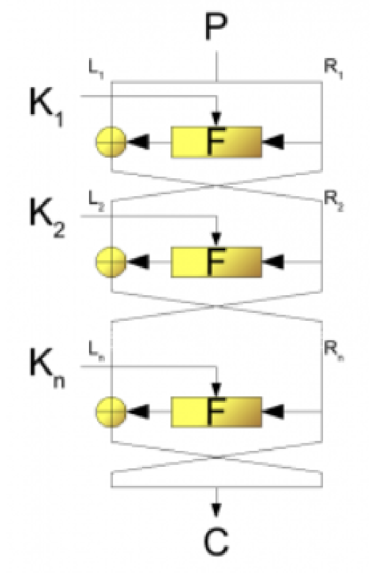
University of Mumbai
Examination June 2021

Examinations Commencing from 1st June 2021

Program: **Computer Engineering**
Curriculum Scheme: Rev2016
Examination: TE Semester VIII
Course Code:**CSC604** and Course Name: **Cryptography and System Security**

Time: 2 hour Max. Marks: 80

Q1.	**Choose the correct option for following questions. All the Questions are compulsory and carry equal marks**
1.	Use Caesar’s Cipher to decipher the following: HQFUBSWHG WHAW
Option A:	ABANDONED LOCK
Option B:	ENCRYPTED TEXT
Option C:	ABANDONED TEXT
Option D:	ENCRYPTED LOCK
2.	On Encrypting “cryptography” using Vignere Cipher System using the keyword “LUCKY” we get cipher text
Option A:	nlazeiibljji
Option B:	nlazeiibljii
Option C:	olaaeiibljki
Option D:	mlaaeiibljki
3.	The DES Algorithm Cipher System consists of ____________rounds (iterations) each with a round key.
Option A:	12
Option B:	18
Option C:	9
Option D:	16
4.	The DES algorithm has a key length of
Option A:	128 Bits
Option B:	32 Bits
Option C:	64 Bits
Option D:	16 Bits
5.	AES uses a ____________ bit block size and a key size of __________ bits.
Option A:	128; 128 or 256
Option B:	64; 128 or 192
Option C:	256; 128, 192, or 256
Option D:	128; 128, 192, or 256
6.	What does the following figure represent?

	 a b c d e f g h Maj Ch Σ Σ + W_t K_t a b c d e f g h 512 bits
Option A:	Compression function
Option B:	Message digest generation using SHA
Option C:	Elementary SHA operation for single round
Option D:	Processing of a single 1024 bit block
7.	The 4×4 byte matrices in the AES algorithm are called
Option A:	States
Option B:	Words
Option C:	Transitions
Option D:	Permutations
8.	This is an example of  P L_1 R_1 K_1 F L_2 R_2 K_2 F L_n R_n K_n F C
Option A:	SP Networks
Option B:	Feistel Cipher
Option C:	Hash Algorithm
Option D:	Hill Cipher
9.	SHA-1 produces a hash value of
Option A:	256 bits
Option B:	160 bits
Option C:	180 bits

Option D:	128 bits
10.	The Kerberos protocol protects against which of the following attacks
Option A:	Dictionary attack
Option B:	Man in the middle attack
Option C:	Replay attack
Option D:	Denial of service attack
11.	A _____________ is a biological feature or a characteristic of a person that uniquely identifies him/her over his/her lifetime.
Option A:	Digital image of a person's fingerprint stored on an electronic passport.
Option B:	PIN enabled chip card for electronic payment.
Option C:	Use of login name + password
Option D:	Driver's license + national ID card
12.	Which of the following authentication protocols is the most widely used today?
Option A:	possession (what you have)
Option B:	knowledge (what you know)
Option C:	combination of possession and knowledge
Option D:	biometrics (something unique about the user)
13.	Which protocol consists of only 1 bit?
Option A:	Alert Protocol
Option B:	Handshake Protocol
Option C:	Upper-Layer Protocol
Option D:	Change Cipher Spec Protocol
14.	Closed ports respond to a(n) _____ with an RST packet.
Option A:	XMAS scan
Option B:	SYN scan
Option C:	Connect scan
Option D:	ACK scan
15.	Firewalls, antivirus and anti spyware installed on every machine that monitors all incoming and outgoing traffic for suspicious activities
Option A:	Host intrusion detection system (HIDS)
Option B:	Distributed intrusion detection system (DIDS)
Option C:	Intrusion detection system (IDS)
Option D:	Network intrusion detection system (NIDS)
16.	What protocol can be used by a host on a network to find the MAC address of another device based on an IP address?
Option A:	DNS
Option B:	ARP
Option C:	TCP
Option D:	UDP
17.	A type of crime in which your private information is stolen and used for criminal activity is
Option A:	money laundering

Option B:	clickbait
Option C:	identity theft
Option D:	phishing
18.	In which of the following exploits does an attacker insert malicious coding into a link that appears to be from a trustworthy source?
Option A:	cross-site scripting
Option B:	command injection
Option C:	path traversal attack
Option D:	buffer overflow
19.	_____________ attack is the exploitation of the web-session & its mechanism that is usually managed with a session token.
Option A:	Session Hacking
Option B:	Session Hijacking
Option C:	Session Cracking
Option D:	Session Compromising
20.	In _______________ attack, the attacker doesn't actively take over another user to perform the attack.
Option A:	phishing
Option B:	spoofing
Option C:	hijacking
Option D:	vishing

Q2. **(20 Marks Each)**	**Solve any Four out of Six** **5 marks each** ***Please delete the instruction shown in front of every sub question***
A	What are the key Goals of Security?
B	Explain with examples mono and poly alphabetic substitution ciphers.
C	Compare Port Scanning and Packet Sniffing
D	What is Buffer overflow attack? Is it intentional or unintentional. Justify.
E	Write short notes on Intrusion Detection Systems.
F	Differentiate between MD5 and SHA-1.

Q3. **(20 Marks Each)**	**Solve any Two Questions out of Three** **10 marks each** ***Please delete the instruction shown in front of every sub question***
A	Explain the mechanism behind Triple DES with 2 Keys. What were the drawbacks of Double DES which have been addressed in Triple DES?
B	Explain the architecture of Needham Schroeder Authentication Protocol in detail.
C	Suppose that two parties A and B wish to set up a common secret key (D-H key) between themselves using the Diffie Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. What is the Diffie Hellman Shared Key ?