Rough

CLO 1: Explain key concepts of information security such as design principles, cryptography, risk management and ethics

Question 1 [20 Marks]

To be answered on the last page

1. During a ransomware outbreak, the IT team finds that backups were intact but inaccessible due to missing decryption keys. Which CIA pillar was primarily impacted?
   A) Confidentiality
   B) Integrity
   C) Availability
   D) Authentication

2. An attacker compromises a database by altering product prices without being detected. Which defense principle could have minimized this risk?
   A) Obscurity
   B) Simplicity
   C) Layering
   D) Auditing

3. A security team enforces multi-factor authentication for administrators. Which risk management strategy is this?
   A) Avoidance
   B) Mitigation
   C) Transference
   D) Acceptance

4. An APT spends weeks studying an organization's LinkedIn profiles before sending spear-phishing emails. Which Cyber Kill Chain phase is this?
   A) Weaponization
   B) Reconnaissance
   C) Delivery
   D) Exploitation

5. A company uses the same antivirus vendor across all endpoints. Which defense principle is being violated?
   A) Layering
   B) Simplicity
   C) Diversity
   D) Limiting

6. An attacker steals login credentials and uses them to access confidential medical data. Which combo of the CIA triad and AAA Security Model is compromised?
   A) Confidentiality & Integrity
   B) Integrity & Availability

C) Confidentiality & Authorization
D) Confidentiality & Authentication

7. A company publicly enforces strict legal action policies, including termination and prosecution, for any insider who attempts to leak trade secrets. Which risk management strategy is being applied?

A) Risk transference
B) Risk avoidance
C) Deterrence
D) Risk mitigation

8. An attacker plants backdoors that remain dormant until triggered months later. Which Kill Chain stage ensures long-term foothold?

A) Reconnaissance
B) Installation
C) Exploitation
D) Actions on Objectives

9. A victim clicks on `mircosoft.com` instead of `microsoft.com`. Which malware delivery mechanism could be paired with this?

A) Drive-by download
B) Polymorphic virus
C) Macro Trojan
D) Spyware injection

10. An attacker calls employees pretending to be IT staff, asking for their OTP. Which two social engineering elements are combined?

A) Pretexting & Fear
B) Quid Pro Quo & Curiosity
C) Phishing & Authority
D) Vishing & Trust

11. A trojan appears as a free software update but secretly installs spyware. Which feature distinguishes it from a worm?

A) Spreads automatically across networks
B) Requires user execution under false pretenses
C) Launches without needing victim trust
D) Leaves no file traces

12. A senior manager receives a fake invoice email crafted using their LinkedIn project details. Which attack is this?

A) Spear Phishing
B) Pretexting
C) Impersonation
D) Whaling

13. A compromised website silently installs malware when visited. Which infection method is being used?
A) Typosquatting
B) Drive-by download
C) Malvertising
D) Pretexting

14. A user dumps company documents in a public bin, later recovered by attackers. Which failed defense principle applies?
A) Layering
B) Simplicity
C) Limiting
D) Obscurity

15. A spyware variant silently exfiltrates clipboard data. Which CIA element is threatened most?
A) Confidentiality
B) Availability
C) Integrity
D) Accountability

16. A polymorphic virus changes its code on each infection cycle. Which malware detection method is most impacted?
A) Signature-based
B) Behavior-based
C) Heuristic
D) Sandboxing

17. A vishing scam convinces employees to install "remote support software." What psychological lever is central here?
A) Greed
B) Authority
C) Fear
D) Trust

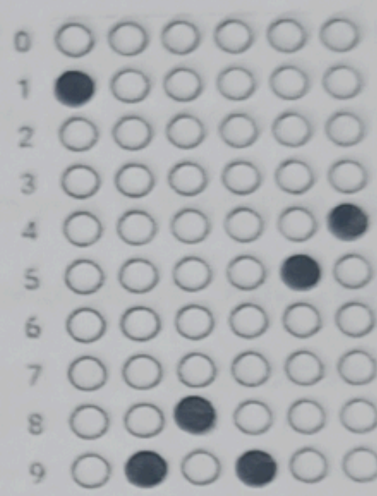
18. An attacker distributes fake job postings with malware-laden PDFs. Which primary entry point is exploited?
A) Curiosity-driven phishing
B) Pretexting with authority
C) Whaling-based deception
D) Dumpster-diving lure

19. In Caesar cipher, shifting the alphabet by 13 is equivalent to:
A) Affine cipher with key (a=1, b=13)
B) Vigenère cipher with key "M"
C) ROT13
D) Columnar cipher

20. An affine cipher uses key (a=5, b=7). Why must "a" satisfy gcd(a, 26)=1?
A) To prevent brute force
B) To ensure invertibility in decryption
C) To maximize key space
D) To hide frequency patterns

Question 1: Multiple Choice Questions [20 Marks]

- Mark your answers to the MCQ's in the following answer sheet by FILLING the correct box. **Tick or Cross WILL NOT BE MARKED.**
- Any answers not provided here will not be marked.
- Multiple filled choices will be marked incorrect.
- In the Roll No column, use 6 digits of your registration number (ignoring alphabet), for example, 22i-8954 will be filled as in the right column.



Roll No: 2 2 0 7 8 9

Information Security
MCQs

	A	B	C	D
1	○	○	●	○
2	○	○	○	●
3	○	●	○	○
4	○	●	○	○
5	○	○	●	○
6	○	○	○	●
7	○	○	●	○
8	○	○	○	●
9	○	○	●	○
10	○	○	●	○
11	○	●	○	○
12	○	○	○	●
13	○	○	●	○
14	○	○	○	●
15	●	○	○	○
16	●	○	○	○
17	○	○	○	●
18	●	○	○	○
19	○	○	●	○
20	○	●	○	○

13

CLO 3: Apply various security and risk management tools for achieving information security and privacy

Question 2 [20 Marks]

At FAST NUCES, life is full of struggles, assignments that even NASA would find difficult, papers that feel like mystery novels, teachers who explain like Einstein, but somehow notes are never available! And the GPA? That's always a dukh bhari kahani!

One day, a witty student named Ali wanted to share this reality in the famous FAST NUCES Facebook group. But then Ali thought:

"If I just post it directly, everyone, even the faculty, will read it. Let me make it fun. I'll encrypt my own name, so people will have to solve the puzzle to know it was me."

Ali decides to hide his name using the Affine Cipher.

$$C = a.P + b \pmod{m},$$ P = Plaintext, C = Ciphertext

with the following rules:

1. The multiplier a must be an integer such that:
   - $5 < a < 10$
2. The shift b must satisfy:
   - $5 < b < 10$, and b is a **prime number**.
3. To handle the spaces and dots (.) some used to remove them in pre-processing and some ignore them altogether. Both techniques have draw back, we want to incorporate the **spaces** and **dots**(.) as well to retain the exact word and sentence boundaries. So consider them as separate characters.

Tasks:

a. Determine the valid values of a and b, satisfying all conditions. **[2 marks]**

a	9 ∵ $5<9<10$ ✓ & $\gcd(28,9)=1$ ✓
b	7 ∵ $5<7<10$ ✓ & 7 is a prime number

b. Encrypt the plaintext **ALI RAZA** with the chosen key (a,b). Show all steps clearly. **[4 marks]**

Encryption Result	<Perform the step by step decryption on the answer sheet provided> ~~HWXXOHIH~~ HWXRUHIH

c. Decrypt your ciphertext back to plaintext. **[3+3 = 6 marks]**

Decryption Key	<Perform all steps to find decryption key on the answer sheet provided> $a^{-1} = 25$
Decryption Result	<Perform the step by step decryption on the answer sheet provided> ALI RAZA

d. Encrypt the same Plaintext **ALI RAZA** with Vigenere cipher, using key=**DO YOU**. **[4+4 = 8]**

Encryption Result	<Perform the step by step encryption on the answer sheet provided> DZGWDUAO
Decryption Result	<Perform the step by step decryption on the answer sheet provided> ALI RAZA

CLO 4: Identify appropriate techniques to tackle and solve problems of real life in the discipline of information security

Question 3 [30 Marks]

Case Study: Noisy Bear APT (Kazakhstan Oil & Gas, May 2025)

In April–May 2025, a newly discovered Advanced Persistent Threat (APT) group, codenamed Noisy Bear, launched a campaign against Kazakhstan's largest oil and gas company, *KazMunaiGas*. The organization played a critical role in national energy exports and employed over 50,000 staff across corporate offices, oil fields, and refineries.

What Happened:

Employees across the finance and IT departments received emails seemingly sent from their own finance division, referencing topics such as updated salary schedules and IT policy changes. The emails were sent from a compromised internal email account, making them appear authentic.

Attached to the email was a ZIP file named Salary_Schedule_Q2.zip. Inside the archive:

- A decoy document (salary update notice).
- A malicious Windows shortcut (.LNK) file, disguised with a similar name.

When employees clicked the shortcut, hidden PowerShell commands were silently executed. These commands:

- Disabled Windows Defender and logging.
- Pulled down a malicious DLL for persistence.
- Established a covert Command & Control (C2) channel over HTTPS, blending into normal traffic.
- Exfiltrated sensitive documents, including contract details with foreign partners.

Impact:

- Confidential salary and HR records were leaked.
- Several internal project documents were exfiltrated to external servers.
- Attackers gained lateral movement privileges, mapping the corporate Active Directory.
- Although no immediate financial theft was reported, the breach posed geopolitical risks since leaked contracts involved international energy deals.

Actions Taken by KazMunaiGas:

1. Isolated affected workstations, reset compromised accounts, and blocked C2 domains.
2. Conducted a forensic investigation, deployed updated EDR (Endpoint Detection & Response) tools, and patched email filtering rules.
3. Launched urgent phishing-awareness training for employees, particularly focused on "internal-looking" emails.
4. Shared Indicators of Compromise (IOCs) with Kazakhstan's national CERT and energy-sector partners.
5. Released a press statement assuring no operational disruption to energy supply chains.

Tasks:

Q a. In the context of the Noisy Bear APT (KazMunaiGas, 2025) case study, analyze the attack by mapping it to the Cyber Kill Chain. **[7+7+7+7=28 marks]**

14

Kill Chain Stage	Targeted Asset	Malware / Social Engineering Exploit	Attack Vector	How Penetration Occurred
Reconnaissance	.Employees	Tailgaiting	Gathered info about salary updates	
Weaponization	Internal domains & its	Phishing, spoofing		Get compromised domains & its
Delivery	Employees	Phishing	Phishing email	Phishing emails disguised as Quarter report
Exploitation	Deshtop access	Trojan	.LNK file disguised in the zip	
Installation	Deshtop access	Rootkit,	Disable Win Defender DLL	
Command & Control	.	Used DLL for persistence, Logic Bom	Established C&C over HTTPs	
Actions on Objectives	Employee records, salaries etc	Logic Bomb	exfiltrate info	

CLO 3: Discuss legal, ethical, and professional issues in information security

b. In the context of the Noisy Bear APT case, identify one international legal implication of a state-sponsored cyberattack on a foreign energy company. **[1 mark]**

It could be considered as an act of war, since energy infrastruce is part of nation's sovereignity.

c. From an ethical standpoint, what makes spear-phishing employees in the Noisy Bear case more concerning than simply exploiting technical vulnerabilities? **[1 mark]**

Continuous phishing threat can erode trust, causing a lot of false ~~trues~~ positives.

Vigenère Cipher Reference Table

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Best of Luck ☺

IS S-1 F25 _2025-09-23_key

Q No	Correct
Information Security - MCQs	
1	C
2	D
3	B
4	B
5	C
6	C
7	C
8	B
9	A
10	D
11	B
12	D
13	B
14	C
15	A
16	A
17	B
18	A
19	C
20	B

Affine Cipher – Solution Key for Plaintext “ALI RAZA”								
Parameter / Step	**Affine (a=5, b=7, m=26)**	**Affine (a=7, b=7, m=26)**	**Affine (a=9, b=7, m=26)**	**Affine (a=6, b=7, m=27)**	**Affine (a=6, b=7, m=28)**	**Affine (a=7, b=7, m=28)**	**Affine (a=9, b=7, m=28)** (space=26, dot=27)	**Affine (a=9, b=7, m=28)** (dot=26, space=27)
a	5	7	9	6	6	7	9	9
b	7	7	7	7	7	7	7	7
a^{-1} (mod m)	21	15	3	–	–	–	25	25
Ciphertext	HBEWHAH	HGLWHAH	HCBEHYH	HTBBBHWH	HR.XZHRH	HAHVOHOH	HWXRUHIH	HWX.UHIH
$\gcd(a, m)$	1	1	1	3	2	7	1	1

Vigenère Cipher – Solution Key for Plaintext “ALI RAZA”									
Alphabet (m)	**26 (A–Z)**	**27 (A–Z + space)**	**27 (A–Z + dot)**	**28 (A–Z + space + dot)**	**28 (A–Z + space + dot)**	**28 (A–Z + space + dot)**	**28 (A–Z + space + dot)**	**28 (A–Z + dot(26) + space(27))**	**28 (A–Z + space(26) + dot(27))**
Key	DOYOU	DO YOUDO	DOYOU.	DO YOU.	DO YOU.D	DOYOUDOY	DO YOUDO	DO YOUDO	DO YOUD
Ciphertext	DZGFUCO	DZHXEUBO	DZFEUYD	DZGWDUYD	DZGWDUYD	DZEMJDLY	DZGWDUAO	DZHXDUAO	DZGNORD
Decrypted text	ALIRAZA	ALI RAZA	ALIRAZA	ALI RAZA	ALI RAZA	ALI RAZA	ALI RAZA	ALI RAZA	ALIRAZA

Question No 03:

(a) Mapping the Noisy Bear Attack to the Cyber Kill Chain (28 marks)

Kill Chain Stage	Targeted Asset	Malware / Social Engineering Exploit	Attack Vector	How Penetration Occurred
Reconnaissance	Finance & IT employees, email accounts	Gathering employee roles, org chart, internal email patterns	OSINT, compromised internal account	Attackers identified high-value targets and valid internal accounts
Weaponization	HR / salary communications	Malicious ZIP with decoy salary doc + .LNK + PowerShell script	ZIP archive attachment	Malware disguised as legitimate HR document
Delivery	Employees' inboxes	Spear phishing / impersonation of finance division	Phishing email from compromised internal account	Employees received convincing internal-looking emails
Exploitation	End-user workstations	PowerShell commands disabling Windows Defender, downloading DLL	Clicking .LNK shortcut	Execution triggered hidden malware commands
Installation	Workstations	Malicious DLL installed for persistence	Executed via PowerShell script	DLL installed silently, enabling repeated access
Command & Control	Network traffic / infected hosts	C2 channel over HTTPS	Network traffic blending with normal activity	Malware communicated with external servers covertly
Actions on Objectives	Salary records, HR files, project documents, AD info	Data exfiltration tools, lateral movement scripts	Network exfiltration / internal file access	Sensitive documents stolen, lateral movement

				mapped Active Directory

(b) International Legal Implication (1 mark)
It breaks international law by interfering with another country's critical systems, violating national sovereignty.

(c) Ethical Concern (1 mark)
It is worse because it tricks people instead of systems, using deception to exploit human trust.