Question 1: Security Engineering Basics & Usability [20 points]

(a) **[2 points]** Explain the Principle of Psychological Acceptability.

(b) **[2 points]** A cloud storage provider enforces mandatory encryption for all client files to protect against insider threats. However, the encryption process makes file uploads and downloads significantly slower, frustrating users who need quick access. Explain what security goals are in contention here.

(c) **[6 points]** Answer the following questions related to Fundamental Security Design Principles.

i) Explain the Fundamental Security Design Principle of **Open Design** and how it relates to the **Kerckhoffs's Principle**. **(2 points)**

ii) Explain why it is important for a system's security to follow the principle of Open Design. **(2 points)**

iii) Give one example where Kerckhoffs's Principle is applied in practice. Explain your answer. **(2 points)**

(d) **[4 points]** Humans are susceptible to cognitive biases that can affect decision-making and security behaviour. Identify one cognitive bias, explain the bias, and describe a realistic scenario where an attacker could exploit it to compromise security.

(e) **[4 points]** A company enforces the following password policy for its employees:

- Passwords must be exactly **8 characters long**.
- Characters can be **uppercase letters (A–Z), lowercase letters (a–z), and digits (0–9)**.
- No other symbols are allowed.

i) Calculate the **entropy** (in bits) of a password under this policy. **(2 points)**

ii) If an attacker can try **1 billion (10^9) passwords per second**, estimate the **worst-case time to brute-force** a randomly chosen password. Give your answer approximately in hours. **(2 points)**

(f) **[2 points]** Explain the concept of user conditioning in the context of security.

Question 2: Access Control [20 points]

(a) **[10 points]** Table 1 and Table 2 show mappings between users and clearances, and between objects and required clearnaces, respectively. The clearance levels increase as Public $<$ Sensitive $<$ Confidential $<$ Secret $<$ Top Secret. Only these mappings are defined; no other rule sets exist.

User	Clearance
Alice	Public
Bob	Sensitive
Carol	Confidential
David	Secret
Fiona	Top Secret

Table 1: User Clearance Levels

Object	Required Clearance
meeting_notes.txt	Public
budget_report.txt	Sensitive
project_design.docx	Confidential
incident_log.txt	Secret
strategic_overview.pdf	Top Secret

Table 2: Object Clearance Requirements

Refer to Table 1, and Table 2 and state if the following statements are **True** or **False**. Justify your answer.

i. In a Bell-LaPadula model, Bob can read the file `project_design.docx`. (**2 points)**

ii. In a Biba model, Carol can edit `budget_report.txt`. (**2 points)**

iii. In a Bell-LaPadula model, Fiona can copy content from `strategic_overview.pdf` into `incident_log.txt`. (**2 points)**

iv. In a Biba model, Alice can write to `meeting_notes.txt`. (**2 points)**

v. In a Bell-LaPadula model, David can read `incident_log.txt`. (**2 points)**

(b) **[6 points]** Table 3 shows the current permissions on two files and two directories in a Linux system.

Name	Type	Owner	Group	Permissions
deploy.sh	File	carol	admins	-rwxr-xr--
report.pdf	File	dave	staff	-rw-r-----
temp/	Dir	root	staff	drwxrwxrwt
shared/	Dir	root	staff	drwxrws---

Table 3: Current permissions on files and directories in the Linux system.

i. Convert the permissions for the following entries into octal form **(2 points)**
   - deploy.sh
   - report.pdf

ii. Explain what the sticky bit on the temp/ directory does. **(2 points)**

iii. Explain what the setgid bit on the shared/ directory does. **(2 points)**

(c) **[4 points]** Explain the confused deputy problem in the context of web browsers.

Question 3: Public Key Cryptography [20 points]

You have given the public key of an RSA key pair (e, n) = (3, 51) in the usual notation. Based on this information, answer the following questions. Use your calculators to do the modular computations (i.e., no need to do the exponentiation by squaring or the extended Euclidian algorithm).

(a) **[4 points]** Calculate the private key of the given public key, i.e., (d, n). Show your steps.

(b) **[2 points]** Encrypt the plaintext 8 using the public key and obtain the cipher text. Show your steps.

(c) **[2 points]** Demonstrate that you can obtain the plaintext back by decrypting using the private key. Show your steps.

(d) **[6 points]** Demonstrate the malleability property of RSA using the integer 3. Use the same the cipher text you obtained in b) for the plaintext 8. Explain your calculations.

(e) **[6 points]** Encrypt the plaintext 59 using the given RSA public key. You will find that the resulting ciphertext is the same as in part (b). This suggests that two different plaintexts produce the same ciphertext, raising ambiguity in decryption. Explain why this happens.

Question 4: Web security and Software Security [20 points]

(a) **[5 points]** A news website allows users to post comments under each article. A user reports that when they view the comments section of a popular article, a script automatically executes in their browser and redirects them to a phishing site.

i. Identify the **exact type of attack** happening in this scenario. Briefly justify your answer. **(3 marks)**

ii. Suggest a remediation strategy to prevent this attack. **(2 marks)**

(b) **[4 points]** Briefly explain what Cross-Origin Resource Sharing (CORS) is and why it matters in web security.

(c) **[4 points]** Explain how a Cross-Site Request Forgery (CSRF) attack works. Include the attacker's goal and the mechanism of exploitation.

(d) **[4 points]** A software team integrates a third-party library from an unverified GitHub repository into their project. Later, it is discovered that the library contained hidden malicious code that exfiltrated sensitive data.

i. Identify the type of attack happening here. **(2 marks)**

ii. Suggest a mitigation strategy to reduce the risk of such attacks in practice. **(2 marks)**

(e) **[3 points]** Explain how stack canaries help mitigate buffer overflow attacks.

Question 5: Network Security [20 points]

(a) Consider the below firewall table. It shows the rules of a firewall residing between the internet and a company network having the IP subnet, 203.0.113.0/24.

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	*	*	*	*	*	*	Est.	Accept
B	inet	external	203.0.113.10	TCP	> 1023	80	New	Accept
C	lan	203.0.113.0/24	external	TCP	> 1023	80	New	Accept
D	lan	203.0.113.0/24	external	UDP	> 1023	53	New	Accept
E	lan	203.0.113.0/24	external	TCP	> 1023	22	New	Accept
F	lan	203.0.113.0/24	external	TCP	> 1023	443	New	Accept
G	*	*	*	*	*	*	*	Drop

For each of the below questions, first state whether the statement is TRUE or FALSE and then explain your answer.

i. **[2 points]** The web server of the company accepts HTTPS connections coming from outside.

ii. **[2 points]** Company employees are not allowed to make outgoing SSH connections.

iii. **[2 points]** To further improve the performance of the firewall, Rule G can be moved to the top of the table.

iv. **[2 points]** An attacker can conduct an IP spoofing attack from inside of the company and conduct a DDoS attack against an external server.

v. **[2 points]** This is a stateful firewall table.

(b) **[4 points]** What role does an X.509 certificate play in Transport Layer Security (TLS), and how does it help prevent person-in-the-middle attacks?

(c) **[4 points]** What is forward secrecy in Transport Layer Security (TLS), and how is it achieved?

(d) **[2 points]** Explain the difference between Transport and Tunnel modes in IPSec.

Additional space Use this space if you need additional room for your answers. If you use it, make sure to reference it in the original answer space; otherwise, this space will not be marked.

Additional space Use this space if you need additional room for your answers. If you use it, make sure to reference it in the original answer space; otherwise, this space will not be marked.