Computer Security - Assignment 2

Security Models (18 points)

Consider a secure information system that enforces **three policies simultaneously**: **Bell–LaPadula (BLP)** for confidentiality, **Biba** for integrity, **Chinese Wall** for conflict-of-interest control.

Confidentiality levels (highest to lowest):

TS > S > C > U

Integrity levels (highest to lowest):

H > M > L

There are three conflict classes:

Class	Companies
Banking	AlphaBank, BetaBank
Energy	SunOil, GreenFuel
Tech	NovaTech, QuantumSoft

There are following subjects:

Subject	Confidentiality	Integrity	Access History
Alice	Secret (S)	High (H)	Accessed AlphaBank data
Bob	Top Secret (TS)	Medium (M)	None
Carol	Confidential (C)	High (H)	Accessed SunOil data
Dave	Secret (S)	Low (L)	Accessed NovaTech data

There are following objects:

Object	Company	Confidentiality	Integrity
O1	AlphaBank	Secret (S)	Medium (M)
O2	BetaBank	Confidential (C)	High (H)
O3	SunOil	Top Secret (TS)	Low (L)
O4	GreenFuel	Secret (S)	Medium (M)
O5	NovaTech	Confidential (C)	High (H)
O6	QuantumSoft	Secret (S)	Low (L)

Please fill out the following table: (Result: Denied or Allowed, Reason: if denied, which models are violated)

Question	Result	Reason
Alice attempts to **read O1**.		
Alice attempts to **read O2**.		
Bob attempts to **write to O3**.		
Carol attempts to **read O4**.		
Dave attempts to **write to O5**.		
Bob attempts to **read O6**.		

Classical Ciphers (12 points)

Question 1: Permutation Cipher

Consider a **block permutation cipher** with block size 5.

The permutation key is:

i	1	2	3	4	5
π(i)	3	5	1	4	2

Encrypt the following plaintext using this permutation cipher:

PLAIN

Question 2: Vigenère Cipher

Encrypt the following plaintext using the **Vigenère cipher**.

- Plaintext:

SECURE

- Key:

KEY

Assume:

- Ignore spaces
- Repeat the key as needed

Questions about Number Sizes (Do not use Calculator or AI models) (40 points)

One of the most cost-effective ways to access significant general-purpose computing power is to rent time on a large system from a cloud provider, like Amazon AWS. In this problem, you'll use powers-of-two estimation to estimate how much it would cost to break keys using massive GPUs available through AWS.

An NVIDIA H100 tensor core GPU can test roughly **16 billion AES keys per second**.
How many keys (as a power of two) can an H100 test in one hour?

You can rent time on an Amazon **p5.48xlarge** instance, which includes **8 NVIDIA H100 GPUs**, for about **$24 per hour**.

1. How much would it cost to test **2^{60} keys**?
   Give this as an understandable dollar amount (not a power of two).
2. How much would it cost, on average, to break a **72-bit key**?
3. How much would it cost, on average, to break a **128-bit key**?
   Do you think this much money exists in the world?
4. As described in the textbook, if you are looking at English text, the number of n-bit strings that are valid English text is approximately
   $2^{0.18n}$.

   Consider what would happen if someone used an English phrase for the AES key.

   a) How many **128-bit sequences** are valid English phrases (approximately)?
   b) Assuming you had a way to efficiently generate all such phrases, how much would it cost to test all of these on the p5.48xlarge AWS instance?

Crypto Lab -- Secret-Key Encryption (30 points)

This is your **first experiment on SEED Labs**, so you may need to spend some extra time exploring how to conduct the lab in the virtual environment you have already set up.

The lab platform is available at:
https://seedsecuritylabs.org/Labs_20.04/Crypto/Crypto_Encryption/

Please follow these steps carefully:

1. First, click the **blue PDF button next to "TASK"** to view the detailed lab guide. This guide is very comprehensive and should be followed exactly.
2. Download the **setup files** under each task and import them into your VM using the **shared folder**. **Do not unzip the files inside the shared folder**, as this may trigger your host machine's firewall.
3. You may not be familiar with concepts such as **Docker** and **Containers** yet. Please **carefully read the [Docker manual]**(https://github.com/seed-labs/seed-labs/blob/master/manuals/docker/SEEDManual-Container.md) and then run Docker in your VM to support the lab environment.
4. You are only required to complete **Tasks 1–5**. Submit your work to **Canvas** by uploading a **detailed lab report with screenshots**, describing what you have done and what you have observed. You should also provide explanations for any observations that you find **interesting or surprising**.

*(Please merge this report with the answers to the other part of assignment and submit them as a **single PDF file**.)*