Instructions: You must **not** communicate with anyone else using electronic media. Use the Python programming environment to attempt this assessment. We suggest you use the `sympy` library for this test. You are required to upload your solutions as a Python file (.ipynb) on Moodle under the assignment section once you have completed the exam. The file should be named using your **UID**, for example, UID1234567.ipynb. You will be allowed a maximum of <u>five</u> attempts to upload your submissions and the latest submission will be considered as your final answer. Ensure the file contains all the necessary code as well as all written explanations. Your code must contain all steps leading to the final answer, including calculations, functions, and any other relevant details. Merely copying answers provided by an online AI service, like gpt or Gemini, may not fetch you any credit. In case of concerns, the instructor reserves the right to interview you while evaluating your submissions to authenticate your proposed solutions.

[Max. time = 2 hours | Max. score = 10]

NOTE: You should **<u>not</u>** use any readily available python based cryptography library package in your program or your solution to decode the ciphertext. You must solve the problem by developing the suggested model - no other method will be accepted.

===

Expressing ❤ दिल की बात ❤ secretly using linear algebra

<u>Question</u>: Prof. Sen wishes to communicate a top secret message to his students who are studying computational linear algebra. He does not wish the Dean of Plaksha or anybody else to know about this top secret message. So he encrypts his message using a *matrix key* (call this matrix A of size 100×55) and broadcasts it to his students as a ciphertext `gzvorps$qmr!#fhbhyzo` of length 20 characters. He also shares the matrix key with the students. Additionally, students have access to a dictionary that contains a 5-bit representation of every character (26 lowercase English alphabets and 6 special characters namely @#$&*!). Eg., the character w is encoded in a 5-bit binary representation as 10110. These are available to you in a python notebook with the filename `student_file.ipynb` on Moodle. **Your objective is to use your expertise in linear algebra to decode the ciphertext and print the message text.** In order to achieve this goal, you are required to perform the following sub-tasks and answer the following questions.

1. Convert the ciphertext to a proper binary string and store it as a vector of length $5 \times 20 = 100$. Print this vector as $\mathbf{y}$. **[0.5]**
2. The cipher-string y is generated as follows: $\mathbf{y} = A\mathbf{x}$, where $\mathbf{x}$ is the bit-string corresponding to the message text. What is the character string length of the message text? **[0.5]**

Prof. Sen has included a second layer of security in this crypto-machine and therefore, he has intentionally chosen the matrix-key A as a *non-square* matrix. Had A been a square matrix, the message-string could be easily generated by inverting the key and multiplying it to the cipher-string y, $\mathbf{x} = A^{-1}y$. Since, A is non-square, the key cannot be inverted easily to generate the message-string. But he expects his students to apply their knowledge of linear algebra to figure out a mathematically (and computationally) sound way to decode the cipher-string. Students readily identify that the linear equation $\mathbf{y} = A\mathbf{x}$ can be interpreted as a linear transformation $T(\mathbf{x})$, where A is the matrix representation of T. Here $T : V \rightarrow W$, where V and W are suitable vector spaces.

3. Suggest appropriate vector spaces for V and W along with their respective fields F_V and F_W so that the computer hardware of the crypto-machine they are using can tackle the encoding-decoding process. Clearly write down the mathematical definition of V, W, F_V, and F_W in your python notebook. **[2]**

4 Define clearly (and write it down in your python notebook submission file) the addition and multiplication rules for V, W, F_V, and F_W. Justify your answer with clear mathematical explanation. **[1]**

5 Suggest and write down the bases $\mathbf{b}_i$ and $\mathbf{b'}_j$ for all i, j for the vector spaces V and W. **[0.5]**

6 What is the $dim(V)$ and the $dim(W)$? Find $T(\mathbf{b}_{17})$. **[1]**

In order to decode the ciphertext, the following mathematical operations must be performed. $A_L\mathbf{y} = A_L A\mathbf{x} = \mathbf{x}$. This is true if $A_L A = I$, where I is an identity matrix of appropriate size.

7. Design the matrix A_L that will allow you to correctly decode the ciphertext and generate $\mathbf{x}$. **[1.5]**
8. Generate the message-string $\mathbf{x}$ and use the dictionary to express and print the message-text as a string of characters. **[1]**
9. What is the necessary and essential property of the matrix key A for this crypto-architecture to be an effective and functionally useful decoder? Will any matrix key of size 100×55, with 0s and 1s as entries, serve as an effective decoder? **[1]**
10. Repeat the decoding procedure with a new cipher that uses only one special character in the dictionary. In this case, re-design the matrix key A_L based on the new matrix key (A_{new}) provided to you in Moodle to extract the message text from the new ciphertext `uvdundjharndifbwavla`. Explain if this is a better cipher? **[1]**

□