Question Number 1

Encode your name (including spaces) in the AES state matrix as shown in class.

- If your name has more than 14 characters (including spaces), use only the first 12 characters.
- Pad the rest of the state to make it 16 bytes.
- For padding use (and mention in the answer) any scheme from https://en.wikipedia.org/wiki/Padding_(cryptography).
- Next apply the `ShiftRows` operation on the state.
- Next apply the `SubBytes` operation.
- Show the state matrix after every operation.

Solution.

Step 1: Encode the Name

The name used is `"Karan Sunil Kumbhar"`. As it contains 19 characters, we take only the first 12 characters:

Name: `"KARAN SUNIL "`

Step 2: Zero Padding to 16 Bytes

Zero padding is applied to make the length of the string 16 bytes. The padded string will be:

Padded String: `"KARAN SUNIL K00000000"`

In hexadecimal, this looks like:

State 1 :

0x4B	0x4E	0x4E	0x00
0x41	0x20	0x49	0x00
0x52	0x53	0x4C	0x00
0x41	0x55	0x20	0x00

Step 3: Apply ShiftRows Operation

The **ShiftRows** operation involves cyclically shifting the rows of the matrix:

State 2 :

0x4B	0x4E	0x4E	0x00
0x20	0x49	0x00	0x41
0x4C	0x00	0x52	0x53
0x00	0x41	0x55	0x20

Step 4: Apply SubBytes Operation

The **SubBytes** operation involves substituting each byte in the state matrix using the AES S-Box. Here are a few substitutions:

- 0x4B → 0xB3
- 0x41 → 0x83
- 0x52 → 0x00
- 0x4E → 0x2F
- 0x20 → 0xB7
- 0x53 → 0xED
- 0x55 → 0xFC
- 0x49 → 0x3B
- 0x4C → 0x29
- 0x00 → 0x63

After applying **SubBytes**, the state matrix becomes:

State 3 :

0xB3	0x2F	0x2F	0x63
0xB7	0x3B	0x63	0x83
0x29	0x63	0x00	0xED
0x63	0x83	0xFC	0xB7

After encoding the name, padding, and applying the AES operations (ShiftRows and SubBytes), the final state matrix is shown above.