Instructions

- Use Latex (Submit only pdf file, Mention Name, Roll No. in title)
- Private submission on Piazza (Ask TA for help with submission)
- Select appropriate folder (e.g. hw2)
- Subject of post: `<HW#>_<Roll#>`

Fiestal SPN

- State five Fiestal & five SPN block ciphers with following details
  - Name
  - Block-length
  - Supported Key-sizes
  - Any other additional info (in one line only)

Random Sbox

- Generate a 4-bit random Sbox in your favourite programming language
- State it in the main assignment
- Submit the code file separately with comments briefly stating your approach
- Follow file naming convention
- It is expected that your Sbox-es will be unique

DDT Your Sbox

- Use the random Sbox you generated for the following
  - Write a code to generate its DDT
  - Use your favorite programming language.
  - Submit code in a separate file
  - Show DDT in answer script
  - What is the maximum differential probability of your Sbox? Mention the transition(s) that lead to that.

Sbox — As a Boolean function

- Use the Sbox generated by you in Problem-2
- Find its corresponding Boolean function
- There will be four functions each representing one output bit