HW3 Problem-1

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#>`
- Submit the `md5` digest of the pdf file using `openssl` in `hex`.

Formally CCA-Security

- Give a formal definition of CCA-Security
- Recall the ones given for KPA, CPA in class

HW3 Problem-2

Hill Cipher

- Encrypt first 4 letters of your name with the Hill cipher using the following key in $\mathbb{Z}_{26}$:

$$K = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$$

- Now, show the steps to calculate K^{-1}
- What are the necessary conditions for K to be invertible?
- Now show the decryption.

Problem-3

Theorem (Perfect Secrecy)

Suppose $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *is a cryptosystem where* $|\mathcal{K}| = |\mathcal{P}| = |\mathcal{C}|$, *then the cryptosystem provides perfect secrecy if and only if every key is used with equal probability* $1/|\mathcal{K}|$, *and for every* $x \in \mathcal{P}$ *and* $y \in \mathcal{C}$ *there is a unique* K *such that* $e_K(x) = y$.

- *Prove it.*
- *You are allowed to refer Stinson.*

Problem-4

Perfect Secrecy?

- Show why the One Time Pad (OTP) is insecure if the key is used more than once.

Hill Vs Permutation

- What is the relation between the Hill cipher and the permutation cipher. Illustrate with an example.