CS4021D Number Theory and Cryptography (S5 and S7 B Tech)

Assignment I: SageMath Implementation of Basic Cryptographic Systems & its Cryptanalysis

The assignment has to be done individually. Please go through the Sagemath (**https://www.sagemath.org/ https://sagecell.sagemath.org/ https://cocalc.com/**) tool and get yourself familiarize with the tool. You are suppose to use Sagemath for implementation of Assignment I.

The aim of this assignment is for you to get yourself more familiar with SageMath tool used by Cyber Security Researchers in developing Cryptographic algorithms, its implementations and Cryptanalysis. Your focus in this assignment is to get familiar with SageMath and implement the basic cryptographic algorithms using CoCalc (SageMathCloud). You should get a clear understanding on the implementation of basic cryptographic algorithms listed below using SageMath tool.

What you have to do?
You have to implement the following algorithms using SageMath tool

1. Affine cipher;
2. Hill cipher;
3. Shift cipher;
4. Substitution cipher;
5. Transposition cipher;
6. Vigenere cipher;

This should be followed by cryptanalysis of all the above classical cyphers algorithm from 1 - 6.

Extra Credits would be given for the person who implements an UNDOCUMENTED attack in the cryptosystem using SAGEMATH tool

You have to submit your code with proper documentation & output screenshots to me via the submission link before **11/10/2023 10:00 PM**, after which you won't be allowed to attend the evaluation. The evaluation would be done individually. Individual demonstration/modifications/viva as part of evaluation has to be completed before **19/10/2023 05:00 PM**. Please note that the slots has to blocked well in advance, so that last minute crowd for evaluations won't be there. Also note that each of you would be given a Max of 15 Min for demonstration/modification/viva.

The filename format should be RollNo_FirstName_QuestionNumber.sage. All code files have to be compressed into a single file with the file name RollNo_FirstName.rar and have to be submitted here.

Submission of any plagiarised/copied contents will lead to awarding of F grade for this subject and will be forwarded for further actions.

Clarifications in the questions, if any has to be brought to me by 28/09/2023, after which no clarifications would be entertained.