EE720: Home Assignment 1 and Problems on Introduction

January 14, 2016

This is a first short assignment. Will be evaluated on 0 to 10 scale. Its weightage out of 20% in the total shall be decided depending on the second or possibly third assignment. This assignment is to be completed individually. Deadline to submit this assignment is **February 20, 2016**. Submission of the report should be done in soft copy to any one TA whose names will be announced on moodle. Format of title page of submission:

- Title: Name of the cipher you have designed
- Your roll number and name.

Home Assignment Problem

Develop a toy cipher for encrypting English text using only alphabets A to Z, space and punctuation marks are neglected, with following specifications

1. Key length in alphabets should be 8 to 16 characters long for block cipher. Plaintext is limited to 500 alphabets.
2. Algorithm should be simple enough to do hand encryption once the user is given a template or a table of alphabets. Similarly decryption should be easy enough with same set up.
3. Optionally, you may choose to develop a method for choosing a 100 alphabet length key stream which is uniformly randomly distributed at each alphabet and develop a Vernam key pad cipher.
4. Algorithm for encryption and decryption should be implementable by hand without any programming expertise or availability of laptop or a tablet. Any user with the above set up material on paper should be able to carry out encryption and decryption.

5. If any calculations are required to be carried out for encryption or decryption these should be possible on a hand calculator.

6. Use only 25 English alphabets by taking i and j as same letters.

7. Give justification of extent of security your algorithm provides.

8. Modification of existing algorithms should be avoided. But if you use existing algorithm then variations on the algorithm must be incorporated and security should be justified.

Problems on Introductory ideas

1. Develop a method of generating 12 digit random number. (Read Von Newmann's method of random number generation).

2. Develop methods for generating random sequences of alphabets in sets of alphabets $\{0, 1\}$, $\{0, 1, 2\}$ and $\{0, 1, 2, 3\}$ of a specified length.

3. If $\mathcal{A}$ is the alphabet set with cardinality $|\mathcal{A}| = m$, what is the cardinality of $\mathcal{A}^n$?

4. If $F : X \to Y$ is a one way function (OWF) where $X = Y = \mathcal{A}^n$ justify how you can produce a random stream of characters in $\mathcal{A}$ using F?

5. If F is the OWF as in the previous problem, construct and justify a trapdoor OWF $G : X \times X \to X$.

6. Construct and justify a MAC using a OWF.