September 1 2024

RAM Math Circle - Chennai
Session 1

Session format:

- 60 minutes: Simple ciphers
- 30 minutes: Geometry with paper folding

1 Cryptology

We worked with the English alphabet and encoding given by

A	B	C	D	E	F	...	X	Y	Z
0	1	2	3	4	5	...	23	24	25

1. Introduction to the shift cipher; warm up with some examples:
   (a) Encrypt the plaintext 'Good morning' with the key 5.
   (b) Encrypt the plaintext 'It is a lovely sunny day' with the key -7.
   (c) Decrypt the ciphertext 'VO DOHA H ILHBAPMBS TVYUPUN'
2. Discussion on the need for cryptography
   - to prevent tampering of messages (security)
   - privacy
   - secrecy
3. How to break a shift cipher: for this one needs to figure out the key. Several students suggested methods. Of these we discussed two in some detail:
   - Guessing (or brute force) - this involves trying all possible shifts and choosing the one for which the decrypted message makes sense. In the worst case, we need to try 25 different shifts in this method.
   - Smart guessing
     - If there are spaces in the message, one can start by looking at shorter words (one-letter, 2-letter words, 3-letter words etc.) - if any are present - in the ciphertext. Since there are very few of these in the English language, one can try these possibilities and try to guess the key.
     - If there are no spaces in the message then one can try deciphering the first few letters to see if the decrypted part makes sense in the English language. If it does, we proceed with decryption and declare that the key is found.
4. What strategies can be used to deter attempts of breaking the shift cipher? Students suggested following strategies, and some of them warrant more discussion.
   - Using different shifts for different parts of the message
   - Using more than one rounds of shifting (think about why this may not really work)
   - Padding the message at various places with gibberish
   - layered encryption (using more than one encryption methods)
   - Breaking the original message into chunks and shuffling the chunks (i.e. using permutations)

2 Folding an equilateral triangle in a square

1. Think about how we can fold an equilateral triangle in a square.
2. Write down the steps you employed in part (1) and your reasoning (or proof) for why your triangle is equilateral.

3 Work for home and food for thought

1. Decrypt the ciphertext written on the board at the beginning of the session: ‘N MTUJ DTZ BNQQ MFAJ KZS’
2. Write a feedback/review for the first session encrypted by a shift cipher.
3. How/where will the largest equilateral triangle in a square be located? How can we obtain such a triangle by folding?
4. Read about end-to-end encryption on Wikipedia. No need to go into details, a light reading is sufficient.