Techsoc Freshie Roadmap 2

Asymmetric Encryption

Mathematics Club x Cybersecurity Club

Instructions

- This problem set consists of 8 different questions. You have 60 minutes to attempt this contest.
- The first 4 questions are math based while the remaining 4 are more cyber-security oriented.
- Each question carries 10 marks. Marks will be subjectively awarded for descriptive questions.
- You will have 60 minutes to attempt these questions.
- Please write your answers on the provided answer sheet only.

---

§1 Can't trust them calculators

Achintya is given two 5 digit numbers $a_1a_2a_3a_4a_5$ and $b_1b_2b_3b_4b_5$. However, he does not trust the answer given by his calculator. Thankfully, he knows what the remainder is when each number is divided by 11. Achintya can divide numbers by 11 only if they are less than 100. Can you suggest a method (an expression involving a_i and b_i, $i = 1, 2, 3, 4, 5$) to find the remainder when the product is divided by 11? Apply your method to the numbers 44678 and 28993 and report your answer in the answer sheet.

Hint: *Can you come up with a divisibility test for 11? Try to explain why your test makes sense using Modular Arithmetic.*

§2 Code-Breaking (Building?)

Deena tries to encrypt a message using the affine cipher. He decides to use the pair (18,13). The affine pair (a, b) refers to the equation $n_{new} = an + b \mod 26$. Encrypting "*Math club is the best club in CFI*", he gets

`ZRVN BHNJ FD VNL JLDV BHNJ FR BDF`

Do you think this is a good encryption? If yes, encrypt the message "*CFI OP*". If not, fix Deena's encryption. Brownie points if you can point out a necessary condition for the affine cipher to work.

§3 JEE PTSD

Pratyaksh finds a note in his room one day with a heart on it. Intrigued, he opens the note. A cursive handwriting says, 'Can you solve this for me?' and a problem enclosed. Help a bro out.

Find the remainder of $(25)^{252} + 3$ *when divided by* 1729.

§4 Modular Exploration?

Deena challenges Atharva one day. Atharva chooses a number $n = 12537$. Deena then gives the following expression to Atharva:

$$f(n) = 7^k \times (n \mod 7) + \left\lfloor \frac{n}{7} \right\rfloor$$

where k is an integer such that $7^k \leq n < 7^{k+1}$ and $\lfloor\ \rfloor$ represents the greatest integer/floor function.

Deena decides to define a sequence of numbers a_m such that $a_{m+1} = f(a_m)$ with a_0 being Atharva's chosen number i.e. $a_0 = n = 12537$. Deena then explains that Atharva's task is to find the minimum of this sequence.

Hint: *Deena loves the number 7 (because* thala*) and believes that all numbers should be written in base 7 instead of base 10.*

§5 I think I'm frequent

Decode the hidden message by uncovering the most common visitors of the alphabetic realm. Their frequent appearances will guide you to the truth.

`BUGEVGSKD TSTWDCHC HC YFOGUBVW`

Hint: *What are the common words in English?*

§6 How the turn tables

Riddles in ciphers, secrets we hold,
Onward we march, both brave and bold,
To protect our data, stories unfold.

Trust in the code, with every byte,
Enduring the battles, day and night,
Navigating life, in shadows and light.

Decode: `DYESJYR`

§7 Vigenere

Problem Statement

You have intercepted a secret message that was encrypted using the Vigenère cipher. The ciphertext is:

`eve ppm ix swdipb is eve usfaxp`

The Vigenère cipher is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a key.

Once you identify the key, use it to decrypt the ciphertext.

§8 What's my base?

Base64 encoding converts binary data into ASCII text using a set of 64 characters: `A-Z`, `a-z`, `0-9`, `+`, and `/`.

- Facilitates transmission over text-based protocols like email and HTTP.
- Ensures data integrity when communicating binary data as text.

Encoding Scheme:

- Convert binary data into 6-bit groups.
- Map each 6-bit group to the corresponding Base64 character.
- Add padding (`=`) if necessary to form groups of four characters.

Decoding Scheme:

- Convert each Base64 character back to its 6-bit binary representation.
- Concatenate the 6-bit groups to reconstruct the original binary data.
- Remove padding (`=`) and decode the binary data to its original form.

Question:

Given that `EAA EAA SAS EEE` *translates to* `IITM`, *decode the following message:*

`EEA EAA ASA AES SAE SEA SSA`

Happy Solving!

Answer Sheet

§1

Answer for the given numbers: _____

§2

§3

§4

Miminum: _____

§5

§6

§7

§8