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.*

Solution:

We solve the problem in a similar vein to analysing the 9 and 3 divisibility cases:

$a_1a_2a_3a_4a_5 = a_1 \times 10^4 + a_2 \times 10^3 + a_3 \times 10^2 + a_3 \times 10^1 + a_4$

Applying modulo 11, we get:

$a_1 \times 10^4 + a_2 \times 10^3 + a_3 \times 10^2 + a_3 \times 10^1 + a_4 \mod 11$

$\equiv a_1 \times (-1)^4 + a_2 \times (-1)^3 + a_3 \times (-1)^2 + a_3 \times (-1)^1 + a_4 \mod 11$

$= a_1 - a_2 + a_3 - a_4 + a_5 \mod 11$

$\therefore a_1a_2a_3a_4a_5 \equiv a_1 - a_2 + a_3 - a_4 + a_5 \mod 11$

Similarly, $b_1b_2b_3b_4b_5 \equiv b_1 - b_2 + b_3 - b_4 + b_5 \mod 11$

Thus the product p is $(a_1 - a_2 + a_3 - a_4 + a_5) \times (b_1 - b_2 + b_3 - b_4 + b_5) \mod 11$

Applying to 44678 and 28993, we get $(4 - 4 + 6 - 7 + 8) \times (2 - 8 + 9 - 9 + 3) \mod 11 \equiv 1 \mod 11$

§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.

Solution:

Sadly, Deena has chosen the affine pair poorly.

This is because multiple unencrypted letters map to the same encrypted letter. In this case letter 26 (Z) and letter 13 (M) map to the same encrypted letter 13 (M).

The reasoning for this lies in the equation of the affine cipher: $an + b \mod 26$.
Notice that if a contains any factors of 26, multiple values of n (in particular $n = 26$ and $n = 26/d$ where $d = gcd(a, 26)$) return the same value modulo 26.

Thus, a must not contain any factors of 26 i.e. a must be coprime to 26.

§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.

Solution:

We can infer that 1729 is the product of three prime numbers 7,13,19.
We can use Fermat's little theorem to solve the problem.

$$a^{p-1} \ = \ 1 \, mod \, (p)$$

On substituting a=25 and p=7 we get, $\boxed{(25)^6 \ = \ 1 \, mod(7)} \implies (25)^{252} \ = \ 1 \, mod(7)$
$\implies (25)^{252} \ - \ 1$ is divisible by 7
Similarly substituting p=13 and p=19 would give the result as $(25)^{252} \ - \ 1$ is divisible by 13 and 19.
As the number $(25)^{252} \ - \ 1$ is divisible by three prime numbers 7 , 13 and 19. It must be divisible by the product of the primes 1729.
So $\boxed{(25)^{252} \ - \ 1 \ = \ 0 \mod(1729) \implies (25)^{252} \ + \ 3 \ = \ 4 \mod(1729)}$

§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.*

Solution:

12537 in base 7 is 51360 ($= a_0$).

The rightmost digit in base 7 represents the remainder when divided by 7. Further we can also see that the number excluding the rightmost digit represents $\left\lfloor \frac{a_m}{7} \right\rfloor$.

k is 4 in this case since the number has 5 digits in base 7 so $7^4 \leq n < 7^5$. Thus the remainder (in this case 0) becomes the leftmost digit (since it is multiplied by 7^4) and all the other digits shift one place to the right (since they are divided by 7).

Thus $a_1 = 5136$ (leading 0s are neglected). k now changes to 3 as a_1 has 4 digits $a_2 = 6513$, $a_3 = 3651$, $a_4 = 1365$ (the number rotates as all digits move towards the right)

$a_5 = a_1$ and the sequence repeats from here onwards. The minimum in this sequence is a_4 as it is numerically smallest in base 7. Converting a_4 back to base 10, we get:

$a_4 = 1{\times}7^3 + 3{\times}7^2 + 6{\times}7 + 5 = 343 + 147 + 42 + 5 = 537$

§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?*

Solution:

The first thing you are expected to map is `HC -> IS`.

This gives you `TSTWDCHC HC = _____SIS IS`.

By now, you should've noticed it's a one-to-one map.

This leads to `TSTWDCHC HC = ANALYSIS IS`.

`BUGEVGSKD TSTWDCHC HC YFOGUBVW -> ______N_Y ANALYSIS IS _______L`.

From the question, we figure that the first word is `FREQUENCY`.

Multiple appearances of frequent :D -> frequency analysis.

So now `BUGEVGSKD -> FREQUENCY`.

`BUGEVGSKD TSTWDCHC HC YFOGUBVW -> FREQUENCY ANALYSIS IS _______L.`

Substitute known letters:

`BUGEVGSKD TSTWDCHC HC YFOGUBVW -> FREQUENCY ANALYSIS IS ___ERFUL.`

By eliminating the unused letters, or making sense out of the sentence:

`BUGEVGSKD TSTWDCHC HC YFOGUBVW -> FREQUENCY ANALYSIS IS POWERFUL.`

§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`

Solution:

Acrostic Poem: The first letter of each new line, spells out a message.
Here, the message is, `ROTTEN = ROT10`
`DYESJYR` $\xrightarrow{\texttt{ROT10}}$ `NIOCTIB` *(bitcoin in reverse)*
Both `BITCOIN` and `NIOCTIB` are accepted as the right answer.
Partial marks were awarded to people that submitted `ROTTEN` as their answer.

§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.

Solution:

The Vigenère cipher was once considered unbreakable due to its polyalphabetic nature, but it is vulnerable to frequency analysis, especially if the keyword is short or if the plaintext is long. Modern cryptographic methods have rendered it mostly obsolete, but it remains a classic example

of early cryptographic techniques.

Example of Vigenere Cipher (with key being 'KEY'):

Plaintext	H	E	L	L	O
Keyword	K	E	Y	K	E
Ciphertext	R	I	J	V	S

In the cipher we have, eve is repeated twice, which implies that, its a common word, that is put through the same key. This common word, is **the**.
We use this to find the key

Plaintext	T	H	E
Cipher	E	V	E
Keyword	L	O	A

But here comes the tricky part. If the key is only 3 letters long, (i.e. LOA) our plaintext will be,

Cipher	E	V	E		P	P	M		I	X		S	W	D	I	P	B		I	S		E	V	E
Keyword	L	O	A		L	O	A		L	O		A	L	O	A	L	O		A	L		O	A	L
Plaintext	T	H	E		E	B	M		X	J		S	L	P	I	E	N		I	H		Q	V	T

From this we figure that the key has to be longer than 3 for it to overlap with, EVE twice, and give us THE both times. The keys length has to be 4 or 8 or 16 (for the key to overlap perfectly at both 'eve's). But we know it has to be 4 due to practical reasons.

Cipher	E	V	E		P	P	M		I	X		S	W	D	I	P	B		I	S		E	V	E
Keyword	L	O	A		$\_$	L	O		A	$\_$		L	O	A	$\_$	L	O		A	$\_$		L	O	A
Plaintext	T	H	E		$\_$	E	Y		I	$\_$		H	I	D	$\_$	E	N		I	$\_$		T	H	E

Filling in the _s we figure the plaintext and key

Cipher	E	V	E		P	P	M		I	X		S	W	D	I	P	B		I	S		E	V	E
Keyword	L	O	A		F	L	O		A	F		L	O	A	F	L	O		A	F		L	O	A
Plaintext	T	H	E		K	E	Y		I	S		H	I	D	D	E	N		I	N		T	H	E

Therefore, the key is `LOAF` and the plaintext is `the key is hidden in the phrase`

Partial marks were given to those who partially got the answer (like figuring eve->the).

§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`

Solution:

```
EAA EAA SAS EEE -> IITM
A -> 0; E -> 1; S -> 2
100 100 202 111 -> IITM
```

Clue: *"What's my base"*

```
Base3 -> Base10
100 100 202 111 -> 9 9 20 13
9 9 20 13 -> IITM
EEA EAA ASA AES SAE SEA SSA -> 110 100 020 012 201 210 220
110 100 020 012 201 210 220 -> 12 9 6 5 19 21 24
12 9 6 5 19 21 24 -> LIFESUX
```

The plaintext is **LIFESUX**

Happy Solving!

Answer Sheet

§1

Answer for the given numbers: _____

§2

§3

§4

Miminum: _____

§5

§6

§7

§8