VishwaCTF

CHALLENGE NAME: [18th Century]

DEV: [Soham]

CATEGORY: [Cryptography]

LEVEL: [Hard]

2025

Challenge Description:

A message was encoded critically, encrypted using a method said to have been devised by a mathematician who worked with numbers and their intrinsic progressions. The key to this encryption lies in a unique series of shifts, where each character's fate is determined by a structured yet non-uniform alteration. Can you unlock the secret message?

Encrypted string : fVngv&ex6x+izZg)4ex]Z
Flag format: VishwaCTF{Decrypted String}

Hint: Growth is one way to look at numbers, but consider restriction instead. A function that measures what does not divide might be helpful. Some values shift in ways unseen, their fate determined by what they stand apart from—each step altering a symbol's form.

Solution:

There are no files provided for this challenge; the encrypted string is given in the description itself. This means the solution revolves around the challenge description and its name, "18th Century."
It's crucial to understand the structure of the description and what hints it provides to solve the challenge. To do this, we need to read it carefully. If you have trouble understanding the description, *you can use an AI model for interpretation.*
(with deep thinking or reason)

From the challenge name, "18th Century," it's clear that it relates to something from that era, possibly a mathematician.

Now, let's take a look at the description :-

1. **Line from Description:**
   "A message was encoded critically, encrypted using a method said to have been devised by a mathematician who worked with numbers and their intrinsic progressions."
   Meaning:
   The phrase "mathematician who worked with numbers and their intrinsic progressions" suggests a historical figure known for his contributions to number theory.

2. Line from Description:
   "The key to this encryption lies in a unique series of shifts, where each character's fate is determined by a structured yet non-uniform alteration."
   Meaning:
   - The "unique series of shifts" indicates that each character is altered by a different, predetermined value.
   - Structured yet non-uniform" hints at a mathematically defined sequence rather than a simple constant shift—suggesting the use of a function whose output naturally varies from one input to the next.

Breaking Down the Hint :-

3. Line from Hint:
   "Growth is one way to look at numbers, but consider restriction instead."
   Interpretation:
   Instead of focusing on functions that simply grow (like arithmetic or geometric progressions), this line nudges toward functions that impose limits or "restrictions" on numbers.

4. Line from Hint:
   "A function that measures what does not divide might be helpful."
   Interpretation:
   This directly refers to **Euler's Totient function (ϕ)**, which counts how many numbers up to a given number are coprime to it—essentially measuring the numbers that don't divide it.

5. Line from Hint:
   "Some values shift in ways unseen, their fate determined by what they stand apart from—each step altering a symbol's form."
   Interpretation:
   - This line further emphasizes that each character's transformation is dictated by an underlying numerical property like *position or ASCII values.*

- The phrase "their fate" being determined by "what they stand apart from" suggests that the character's position in a sequence matters. This reinforces the idea of a position-based mathematical shift.

From the above points, it's clear that the mathematician is Leonhard Euler, and the function used is Euler's Totient Function ($\phi(n)$). The challenge suggests that the encryption is based on character positions or ASCII values.

Since the description mentions an "irregular shift," we can guess that each letter was shifted in a way that isn't uniform. Euler's Totient Function gives different values for each position, making the shift pattern unique.

So, the final encryption logic appears to be: $new\_char = char \pm \phi(pos)$

This means each character was shifted by the totient value of its position, either forward (+) or backward (-). In this case, the shift is backward (-): $new\_char = char - \phi(pos)$

Character	Position (n)	ASCII Value	- Totient Value φ(n)	= New ASCII Value	Decrypted Character
f	1	102	1	101	e
V	2	86	1	85	U
n	3	110	2	108	l
g	4	103	2	101	e
v	5	118	4	114	r
&	6	38	2	36	$
e	7	101	6	95	_
x	8	120	4	116	t
6	9	54	6	48	0
x	10	120	4	116	t
+	11	43	10	33	!
i	12	105	4	101	e
z	13	122	12	110	n
Z	14	90	6	84	T
g	15	103	8	95	_
)	16	41	8	33	!
4	17	52	16	36	$
e	18	101	6	95	_
x	19	120	18	102	f
]	20	93	8	85	U
Z	21	90	12	78	N

Flag: VishwaCTF{eUler$_t0t!enT_!$_fUN}

Thank You

My discord: @sohamkolte