Rotation/ROT

ROT is short for rotation and has many different forms and amounts of rotations, but the idea is the same. Take a letter, say A, and move ahead that many letters in the English alphabet. For example, if ROT5 is being used, A becomes F since F is 5 letters after A. ROT6 would be G. PLEASE NOTE: we are only talking about substitutions using the english alphabet, this cipher can be used to numbers 0 - 9, letters A - Z uppercase or lowercase, and a combination of both 0 - 9 A - Z.

To learn more about ROT visit this wikipedia page: ROT13 - Wikipedia

To solve: Use ROT13 on the input L0h_Pnag_533_Z3

Hints:

Since ROT13 doesn't change the position of the input characters, the output flag should be in the form of _ _ _ _ _ _ _ _ _ _ _ _ _ _

Use this link for more help ROT13 decoder: Decrypt and convert ROT13 to text - cryptii

RSA

RSA is a common encryption scheme that is widely used today. It works based on the fact that there is no efficient way to find the prime factors of an arbitrary composite number. The scheme is described in the resources

Description of the Scheme: https://en.wikipedia.org/wiki/RSA_(cryptosystem)
RSA implementation: https://www.devglan.com/online-tools/rsa-encryption-decryption
Issues with RSA implementation: https://blog.trailofbits.com/2019/07/08/fuck-rsa/
Toolkit for common exploits in RSA: https://github.com/RsaCtfTool/RsaCtfTool

Factordb: factordb.com

OTP:

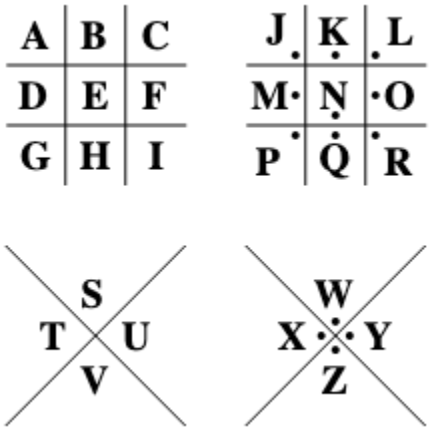
A one-time pad is an encryption technique where each plaintext character is XORed with a corresponding random key character only used once, providing perfect secrecy when the key is truly random and as long as the plaintext, ensuring no patterns exist for cryptanalysis. Also assuming the pad is only used one time and never shared

Use this website to turn pad into all caps key:
https://www.rapidtables.com/convert/number/binary-to-ascii.html

Use this website to decode ciphertext with key and the result should be the key
https://www.boxentriq.com/code-breaking/one-time-pad

Pigpen

This is a substitution cipher, where each symbol corresponds to a letter.



a	b	c	d	e	f	g	h	i	j
									
k	l	m	n	o	p	q	r	s	t
									
u	v	w	x	y	z				
									

Caesar

To learn more about the Caesar cipher, visit https://en.wikipedia.org/wiki/Caesar_cipher
The way a Caesar cipher works is by rotating all of the letters by a certain number of steps. For example, a value of 3 on the code ‘abcd’ would be ‘defg’.

Solving

The thing about Caesar ciphers is that they can be brute-forced pretty easily. After all, there are only 25 total ways to encode a given message, all of which can be figured out pretty easily. However, the number used in this puzzle does have a connection to the real-life Julius Caesar.

Substitution

For more information about substitution ciphers, see
https://en.wikipedia.org/wiki/Substitution_cipher

A substitution works by manually assigning which letter is which. If we said that A=J, B=E, C=T, then “ABC” would be “JET”.

Solving

It might seem like it’s nearly impossible to figure out which letter is which, but the most common way when the mapping isn’t known is to use something like frequency analysis. For this challenge, you are more than welcome to try to do that, but you might have better luck taking a look at this tweet (Xeet?) from Neil DeGrass Tyson
https://twitter.com/neiltyson/status/259486092766625793?lang=en

Vigenere

For more information about the Vigenere cipher, see
https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher
The Vigenere cipher works by taking a message, and using the letters in a key phrase to cycle that many characters forward. For example, the message “ABC” can be encoded with the key phrase “AAA” to become “BCD”, or be encoded with the key phrase “ABC” to become “BDF”.

Solving

In order to figure out the cipher, you need to figure out how what the key phrase is. In this case, the phrase isn’t actually a word, but a famous number associated with the date of this meeting.

Bacon (Baconian) Cipher

So for a bacon cipher each letter in the alphabet is tied to a length 5 code of “a” and “b”. Each “a” and “b” can be then converted into binary where “a” is 0 and “b” is 1. Then, once you convert the “a” and “b” to binary, you can then correlate each number to a letter in the alphabet. I added a table below to give a few examples

Code	Binary	Number in base 10	Letter
aaaaa	00000	0	A
aaaab	00001	1	B
aaaba	00010	2	C
aaabb	00011	3	D

Pretty simple right? The twist is that there are 2 pairs of letters (I,J) and (U,V) with the same code. Based on the context of the clue, you can determine which letter to use in the pair.
The table only shows the first 4 letters of the alphabet so the binary would go all the way until it hits 10111 (or 23 in base 10 because we start at 0 and because there are two pairs with the same code value it subtracts 2 from the total number of letters).

Not in Use

Color wheel
[Color wheel - color theory and calculator | Canva Colors]

Morse Code

Morse code is a language that uses sequences of Dots and Dashes to represent different letters and numbers (and more in some circumstances). The spaces between dots and dashes within the same letter is one, space between each individual letter is three, and the space between words is seven. For example . _ is A since there is only one space between the dot and dash. AA is . _ . _ since there are three spaces between the end of the first A and the dot of the second A. AA A is represented as . _ . _ . _ . _ . _ since there is a space between AA and A, so there is seven spaces.

Read more about morse code here: Morse code - Wikipedia

Hint: Morse Code Translator | Morse Code World