2022Q4 ENCRYPTION

QUESTIONS

Computers, storage devices, and networks use encryption to protect data and safeguard against security breaches. Here at One Energy, we use computers every day to complete tasks involving data storage and transfer which enable us to communicate with the turbines and our customers. Data such as wind speed and power production is transmitted from the turbines to computers in the office to monitor the weather and status of the turbines. Encryption helps keep this important information safe.

Encryption is defined as the conversion of data or information into an encoded version that can only be read by authorized users. The simplest form of encryption, called Caesar's Cipher, is a form of substitution cipher. A substitution cipher encrypts a message by replacing the units of text with ciphertext. Encoding sentences using Caesar's Cipher simply shifts each letter up or down the alphabet by a given amount. The number of shifts is then used as the key to decode the message.

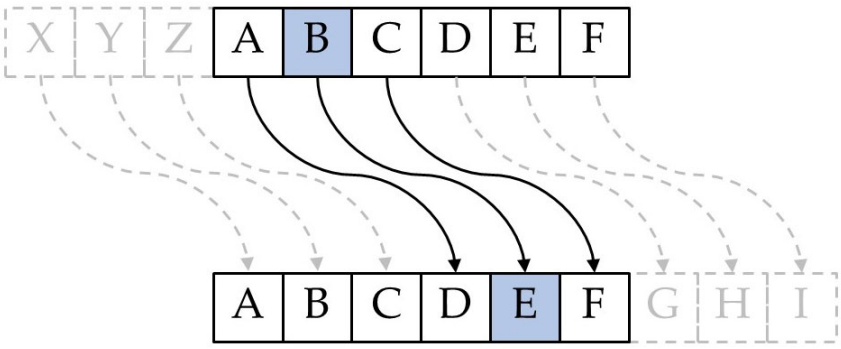

Fig. 1. Conversion of text units to ciphertext.

Another representation of Caesar's Cipher can be found using modular arithmetic. This method transforms letters into numbers and performs calculations based on the equation below. The calculation is based on the modulo operator (mod), which returns the remainder after dividing by the modulus. To calculate 5 modulus 3, divide 5 by 3 and round the answer down to a whole number, 1. Multiply this number by the divisor, 3, and subtract the result from the initial number, 5, to get the answer: 2. When encrypting messages using the alphabet, the modulus is 26.

$$New\ Letter = (x + n)\ mod(26)$$

Where "x" is the letter to be encoded and "n" is the amount the letter will be shifted by.

Check out this example that encodes the letters "ABC" using modular arithmetic and a left shift of 3:

First, convert the letters to numbers.

A = 0, B = 1, C = 2

Next, use the formula to determine the encoded value by using the modulo of 26. Note that the modulo operator returns the original number when it is less than the modulus.

$$New\ Letter = (0 + 3)\ mod(26) = 3\ mod(26)$$

Finally, convert the encoded number back into its alphabetic value and repeat for the remaining letters.

$$New\ Letter = 3 = D$$

Encoded message: "DEF"

Level 1: Given that the message was encoded using a right shift of 7, decipher the following message:

DPUK MVY PUKBZAYF

Level 2: Using modular arithmetic and a right shift of 4, encode the following word:

WIND

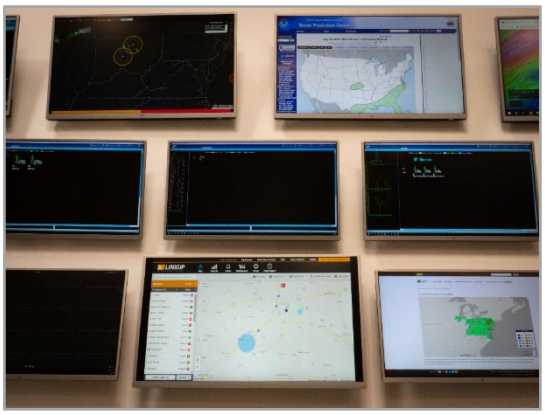

Fig. 2. One Energy's weather wall tracks local weather patterns and communicates to the turbines to track their status.