Cybersecurity and Cryptography Lab

Ciphers

My cipher uses the alphabet (wrapped around) and a mathematical equation.

Original letter + 3 – 5 = Ciphered letter.

G JMTC APWNRMEPYNFW!

Code for Caesar Cipher (offset value = -2)

```
/*
        The Caesar Cipher technique is one of the earliest and simplest method of
        encryption technique. It’s simply a type of substitution cipher, i.e., each letter
        of a given text is replaced by a letter some fixed number of positions down the
        alphabet. For example with a shift of 1, A would be replaced by B, B would become
        C, and so on. The method is apparently named after Julius Caesar, who apparently
        used it to communicate with his officials.
        Thus to cipher a given text we need an integer value, known as shift which
        indicates the number of position each letter of the text has been moved down.
        The encryption can be represented using modular arithmetic by first transforming
        the letters into numbers, according to the scheme, A = 0, B = 1, Z = 25. Encryption
        of a letter by a shift n can be described mathematically as...
        */

        function caesarCipher (string, key) {
          key = key % 26;
          var alphabetsArr = 'abcdefghijklmnopqrstuvwxyz'.split('');
          var lowerCaseString = string.toLowerCase();
          var newString = '';
          var charCount = lowerCaseString.length;

          for(i = 0; i < charCount; i++) {
            var currentLetter = lowerCaseString[i];
            if(currentLetter === ' ') {
              newString += currentLetter;
              continue;
            }
            var charIndex = alphabetsArr.indexOf(currentLetter);
            var newIndex = charIndex + key;
```

```
    if (newIndex > 25) newIndex = newIndex - 26;
    if (newIndex < 0) newIndex =  26 + newIndex;

    if (string[i] === lowerCaseString[i].toUpperCase()) {
      newString += alphabetsArr[newIndex].toUpperCase();
    } else {
      newString += alphabetsArr[newIndex];
    }
  }
  return newString;
}

// Running solution
console.log(caesarCipher('Lorem Ipsum is simply dummy text of the printing and
typesetting industry', -2)); (uiarjev).
```

uiarjeev. (January 21, 2020). Algorithm-Caesar-Cipher-in-javascript. https://github.com/uirajeev/Algorithm-Caesar-Cipher-in-javascript/blob/master/index.js

Cybersecurity Research

In 2016, 360 million user accounts on the social media site *MySpace* were compromised. Hackers obtained users' usernames, passwords, and email addresses. For some accounts a second email was obtained by the hackers, bringing the total number of passwords to 427 million that were available for sale. It's estimated that one-half to three-quarters of Internet users just use one password for most or all of their online accounts. According to an article that appeared in *USA Today*, "Criminal cyber attack rings are very organized about how they use the data the steal or buy on the cyber underground. "They've got smart programs that can try variations of these passwords that

will work and then they've got rooms of people typing in these passwords, kind of a password call center"" (Weise).

In response, *MySpace* notified all affected users and invalidated their passwords. They also closely monitored user accounts for suspicious activity. Unfortunately, hacking user accounts to steal passwords happens all too often. USA Today concludes their report by saying, "Several caches of old passwords and IDs from other online platforms have appeared for sale recently. Two weeks ago LinkedIn reset passwords for as many as 117 million users whose IDs had been stolen in a 2012 breach after they went up for sale online" (Weise).

Weise, E. (May 31, 2016). *360 million Myspace accounts breached.* USA Today. https://www.usatoday.com/story/tech/2016/05/31/360-million-myspace-accounts-breached/85183200/