

Cybersecurity and Cryptography Lab

Ciphers

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

original letter + 3 - 5 = ciphered letter.

G JMTC APWNRMEPYNFW!

Code for Caesar Cipher integer encryption key = 3 - 5, or -2.

Format

The first line contains an integer, `n`, which is the length of the unencrypted string.

The second line contains the unencrypted string, `s`.

The third line contains the integer encryption key, `k`, which is the number of letters to rotate.

```
main()
{
    var n = parseInt(readLine());
    var s = readLine();
    var k = parseInt(readLine());
    var result = '';

    for (var i=0; i<s.length; i++) {
        var char = s[i].charCodeAt();
        var ch = s[i];

        if ((char >= 'A'.charCodeAt() && char <= 'Z'.charCodeAt())) {
            char += k;

            while (char > 'Z'.charCodeAt()) {
                char = 'A'.charCodeAt() + (char - 'Z'.charCodeAt() - 1);
            }

            ch = String.fromCharCode(char);
        }
    }
}
```

```

    }
    else if (char >= 'a'.charCodeAt() && char <= 'z'.charCodeAt()) {
        char += k;

        while (char > 'z'.charCodeAt()) {
            char = 'a'.charCodeAt() + (char - 'z'.charCodeAt() - 1);
        }

        ch = String.fromCharCode(char);
    }

    result += ch;
}

console.log(result);
}
(ldco2016/caesar-cipher.js)

```

ldco2016/caesar-cipher.js. (2017). Github.
<https://gist.github.com/ldco2016/918647ab90c5b6478d83c06e51af6833>

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. Hacking user accounts for passwords happens all too often. USA Today concludes their article 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/>