Đầu tiên vào phần inspect để xem thì ta có được đoạn code như bên dưới

Graphical user interface, text, application, email

Description automatically generated

Ta thực hiện format code js

function xor(x, y) {

    return x ^ y;

}

function powsum1(y) {

    var sum = 0;

    for (var i = 0; i < y; i++) {

        sum += Math.pow(2, i);

    }

    return sum;

}

function powsum2(y) {

    var sum = 0;

    for (var i = 8 - y; i < 8; i++) {

        sum += Math.pow(2, i);

    }

    return sum;

}

function bit1(x, y) {

    y = y % 8;

    ps = powsum1(y);

    ps = (x & ps) << (8 - y);

    return (ps) + (x >> y);

}

function bit2(x, y) {

    y = y % 8;

    ps = powsum2(y);

    ps = (x & ps) >> (8 - y);

    return ((ps) + (x << y)) & 0x00ff;

}

function bit(x, y) {

    return bit2(x, y)

}

function encrypy(salt, key) {

    pwd = "";

    unuse = "";

    for (var i = 0; i < salt.length; i++) {

        c = salt.charCodeAt(i);

        if (i != 0) {

            switch (pwd.charCodeAt(i - 1) % 2) {

                case 0:

                    n = xor(c, key.charCodeAt(i % key.length));

                    break;

                case 1:

                    n = bit(c, key.charCodeAt(i % key.length));

                    break;

            }

        } else {

            n = xor(c, key.charCodeAt(i % key.length));

        }

        pwd += String.fromCharCode(n);

    }

    return pwd;

}

function check(pwd) {

    var checksum = 0;

    for (var i = 0; i < pwd.length; i++) {

        checksum += pwd["charCodeAt"](i)

    }

    if (checksum == 8932) {

        var win = window.open("", "", "width=300, height=20");

        win.document.write(pwd)

    } else {

        alert("Mauvais mot de passe: " + checksum)

    }

}

var salt = "\x71\x11\x24\x59\x8d\x6d\x71\x11\x35\x16\x8c\x6d\x71\x0d\x39\x47\x1f\x36\xf1\x2f\x39\x36\x8e\x3c\x4b\x39\x35\x12\x87\x7c\xa3\x10\x74\x58\x16\xc7\x71\x56\x68\x51\x2c\x8c\x73\x45\x32\x5b\x8c\x2a\xf1\x2f\x3f\x57\x6e\x04\x3d\x16\x75\x67\x16\x4f\x6d\x1c\x6e\x40\x01\x36\x93\x59\x33\x56\x04\x3e\x7b\x3a\x70\x50\x16\x04\x3d\x18\x73\x37\xac\x24\xe1\x56\x62\x5b\x8c\x2a\xf1\x45\x7f\x86\x07\x3e\x63\x47"

var key = prompt("Mot de passe?")

var pwd = encrypy(salt, key)

check(pwd);

Ngoài ra ta sẽ code bằng python để thực hiện lại code nhưng có thể chạy trên máy

def xor(x, y) :

    return x ^ y

def powsum1(y) :

    sum = 0

    for i in range(0, y) :

        sum += pow(2, i)

    return sum

def powsum2(y) :

    sum = 0

    for i in range(8 - y, 8) :

        sum += pow(2, i)

    return sum

def bit1(x, y) :

    y = y % 8

    ps = powsum1(y)

    ps = (x & ps) << (8 - y)

    return ps + (x >> y)

def bit2(x, y) :

    y = y % 8

    ps = powsum2(y)

    ps = (x & ps) >> (8 - y)

    return (ps + (x << y)) & 0x00ff

def bit(x, y) :

    return bit2(x, y)

def encrypt(salt, key) :

    pwd = ''

    key\_len = len(key)

    if key\_len > 0 :

        for i, c in enumerate(salt) :

            x = ord(c)

            y = ord(key[i % key\_len])

            if i > 0 and ord(pwd[i - 1]) % 2 != 0 :

                y = y % 8

                z = bit(x, y)

            else :

                z = xor(x, y)

            pwd += chr(z)

    return pwd

def check(key, pwd) :

    checksum = 0

    for c in pwd :

        checksum += ord(c)

    flag = (checksum == 8932)

    if flag :

        pass

    print('%s(%i): \n\tkey=%s\n\tpwd=%s' % ('Bingo' if flag else 'Fail', checksum, key, pwd))

    return flag

if \_\_name\_\_ == '\_\_main\_\_' :

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| i | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Pwd | \x71 | \x11 | \x24 | \x24 | \x59 | \x8d | \x6d | … |
| Plaintext | < | h | t | m | l | > | < | … |
| Enc | Xor | Xor | Xor | Xor | Bit | Xor | Xor | … |
| Key | **M** | **y** | **P** | **4** | **s** | **S** | M | … |

salt = "\x71\x11\x24\x59\x8d\x6d\x71\x11\x35\x16\x8c\x6d\x71\x0d\x39\x47\x1f\x36\xf1\x2f\x39\x36\x8e\x3c\x4b\x39\x35\x12\x87\x7c\xa3\x10\x74\x58\x16\xc7\x71\x56\x68\x51\x2c\x8c\x73\x45\x32\x5b\x8c\x2a\xf1\x2f\x3f\x57\x6e\x04\x3d\x16\x75\x67\x16\x4f\x6d\x1c\x6e\x40\x01\x36\x93\x59\x33\x56\x04\x3e\x7b\x3a\x70\x50\x16\x04\x3d\x18\x73\x37\xac\x24\xe1\x56\x62\x5b\x8c\x2a\xf1\x45\x7f\x86\x07\x3e\x63\x47"

    key = ""

    pwd = encrypt(salt, key)

    check(key, pwd)

Tiếp theo ta sẽ thực hiện giải tay các giá trị tương ứng và ta có được key

Thực thi code và ta có được kết quả

Text

Description automatically generated