| 일반 소스 공유 | >

RSA Encryption

OtakoidTony 챗봇 고수 1:1 채팅
2019.11.23. 20:03 조회 74


```
stringToUnicode = function(str) {
    if (!str) return false; // Escaping if not exist
    var unicode = '';
    test = new Array;
    var ascii = '';
    for (var i = 0, l = str.length; i < l; i++) {
        ascii = str[i].charCodeAt(0).toString(10);
        test.push(ascii);
    };
    return test;
}

function encrypt(str, e, N){
    var encArray = stringToUnicode(str);
    var i;
    for (i in encArray){
        encArray[i]=Math.pow(parseInt(encArray[i]), e)%N;
    }
    return encArray;
}

function decrypt(arr, d, N){
    var i;
    for (i in arr){
        arr[i]=String.fromCharCode(Math.pow(arr[i], d)%N);
    }
    return arr;
}

function get_private_key(e, tot) {
    var v = 1;
    var d = e;
    var u = (e == 1);
    var t = 1 - u;
    if (t == 1) {
        var c = tot % e;
        u = Math.floor(tot / e);
        while (c != 1 && t == 1) {
            var q = Math.floor(d / c);
            d = d % c;
            v = v + q * u;
            t = (d != 1);
            if (t == 1) {
                q = Math.floor(c / d);
                c = c % d;
                u = u + q * v;
            }
        }
        u = v * (1 - t) + t * (tot - u);
    }
    return u;
}

function gcd(x, y) { // https://www.w3resource.com/javascript-exercises/javascript-math-exercis
    if ((typeof x !== 'number') || (typeof y !== 'number'))
        return false;
```

```
    x = Math.abs(x);
    y = Math.abs(y);
    while (y) {
        var t = y;
        y = x % y;
        x = t;
    }
    return x;
}

function isPrime(n, k) {
    // Corner cases
    if (n <= 1 || n == 4) return false;
    if (n <= 3) return true;
    var a = 0;
    while (k > 0) {
        // Pick a randomly in the range [2, n - 2]
        a = 2 + Math.floor(Math.random() * (n - 4));
        // Fermat's little theorem
        if (Math.pow(a, n - 1) % n != 1) {
            return Math.pow(a, n - 1) % n;
        }
        k = k - 1;
    }
    return true;
}

function totient(p, q) {
    return (p - 1) * (q - 1);
}

/*
RSA 알고리즘 개념 및 구현(python)
https://wkdtjsgur100.github.io/RSA-algorithm/
*/
function get_public_key(totient) {
    var e = 2;
    while (e < totient && gcd(e, totient) != 1) {
        e += 1;
    }
    return e;
}

function randomItem(a) {
    return a[Math.floor(Math.random() * a.length)];
}

const primes = [107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191,
             227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 31
             349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 44
             467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 58
             613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 71
             751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 85
             887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997, 1009, 1
             1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097, 1103, 1109, 1117
             1163, 1171, 1181, 1187, 1193, 1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249, 1259
             1291, 1297, 1301, 1303, 1307, 1319, 1321, 1327, 1361, 1367, 1373, 1381, 1399, 1409
             1439, 1447, 1451, 1453, 1459, 1471, 1481, 1483, 1487, 1489, 1493, 1499, 1511, 1523
             1559, 1567, 1571, 1579, 1583, 1597, 1601, 1607, 1609, 1613, 1619, 1621, 1627, 1637
             1693, 1697, 1699, 1709, 1721, 1723, 1733, 1741, 1747, 1753, 1759, 1777, 1783, 1787
             1831, 1847, 1861, 1867, 1871, 1873, 1877, 1879, 1889, 1901, 1907, 1913, 1931, 1933
             1987, 1993, 1997, 1999, 2003, 2011, 2017, 2027, 2029, 2039, 2053, 2063, 2069, 2081
             2111, 2113, 2129, 2131, 2137, 2141, 2143, 2153, 2161, 2179, 2203, 2207, 2213, 2221
             2267, 2269, 2273, 2281, 2287, 2293, 2297, 2309, 2311, 2333, 2339, 2341, 2347, 2351
             2383, 2389, 2393, 2399, 2411, 2417, 2423, 2437, 2441, 2447, 2459, 2467, 2473, 2477
             2543, 2549, 2551, 2557, 2579, 2591, 2593, 2609, 2617, 2621, 2633, 2647, 2657, 2659
             2687, 2689, 2693, 2699, 2707, 2711, 2713, 2719, 2729, 2731, 2741, 2749, 2753, 2767
             2801, 2803, 2819, 2833, 2837, 2843, 2851, 2857, 2861, 2879, 2887, 2897, 2903, 2909
             2957, 2963, 2969, 2971, 2999, 3001, 3011, 3019, 3023, 3037, 3041, 3049, 3061, 3067
```

```
3119, 3121, 3137, 3163, 3167, 3169, 3181, 3187, 3191, 3203, 3209, 3217, 3221, 3229
3271, 3299, 3301, 3307, 3313, 3319, 3323, 3329, 3331, 3343, 3347, 3359, 3361, 3371
3413, 3433, 3449, 3457, 3461, 3463, 3467, 3469, 3491, 3499, 3511, 3517, 3527, 3529
3557, 3559, 3571, 3581, 3583, 3593, 3607, 3613, 3617, 3623, 3631, 3637, 3643, 3659
3697, 3701, 3709, 3719, 3727, 3733, 3739, 3761, 3767, 3769, 3779, 3793, 3797, 3803
3851, 3853, 3863, 3877, 3881, 3889, 3907, 3911, 3917, 3919, 3923, 3929, 3931, 3943
4003, 4007, 4013, 4019, 4021, 4027, 4049, 4051, 4057, 4073, 4079, 4091, 4093, 4099
4139, 4153, 4157, 4159, 4177, 4201, 4211, 4217, 4219, 4229, 4231, 4241, 4243, 4253
4283, 4289, 4297, 4327, 4337, 4339, 4349, 4357, 4363, 4373, 4391, 4397, 4409, 4421
4457, 4463, 4481, 4483, 4493, 4507, 4513, 4517, 4519, 4523, 4547, 4549, 4561, 4567
4621, 4637, 4639, 4643, 4649, 4651, 4657, 4663, 4673, 4679, 4691, 4703, 4721, 4723
4783, 4787, 4789, 4793, 4799, 4801, 4813, 4817, 4831, 4861, 4871, 4877, 4889, 4903
4937, 4943, 4951, 4957, 4967, 4969, 4973, 4987, 4993, 4999, 5003, 5009, 5011, 5021
5077, 5081, 5087, 5099, 5101, 5107, 5113, 5119, 5147, 5153, 5167, 5171, 5179, 5189
5233, 5237, 5261, 5273, 5279, 5281, 5297, 5303, 5309, 5323, 5333, 5347, 5351, 5381
5413, 5417, 5419, 5431, 5437, 5441, 5443, 5449, 5471, 5477, 5479, 5483, 5501, 5503
5531, 5557, 5563, 5569, 5573, 5581, 5591, 5623, 5639, 5641, 5647, 5651, 5653, 5657
5693, 5701, 5711, 5717, 5737, 5741, 5743, 5749, 5779, 5783, 5791, 5801, 5807, 5813
5849, 5851, 5857, 5861, 5867, 5869, 5879, 5881, 5897, 5903, 5923, 5927, 5939, 5953
6029, 6037, 6043, 6047, 6053, 6067, 6073, 6079, 6089, 6091, 6101, 6113, 6121, 6131
6173, 6197, 6199, 6203, 6211, 6217, 6221, 6229, 6247, 6257, 6263, 6269, 6271, 6277
6317, 6323, 6329, 6337, 6343, 6353, 6359, 6361, 6367, 6373, 6379, 6389, 6397, 6421
6473, 6481, 6491, 6521, 6529, 6547, 6551, 6553, 6563, 6569, 6571, 6577, 6581, 6599
6659, 6661, 6673, 6679, 6689, 6691, 6701, 6703, 6709, 6719, 6733, 6737, 6761, 6763
6803, 6823, 6827, 6829, 6833, 6841, 6857, 6863, 6869, 6871, 6883, 6899, 6907, 6911
6961, 6967, 6971, 6977, 6983, 6991, 6997, 7001, 7013, 7019, 7027, 7039, 7043, 7057
7121, 7127, 7129, 7151, 7159, 7177, 7187, 7193, 7207, 7211, 7213, 7219, 7229, 7237
7297, 7307, 7309, 7321, 7331, 7333, 7349, 7351, 7369, 7393, 7411, 7417, 7433, 7451
7487, 7489, 7499, 7507, 7517, 7523, 7529, 7537, 7541, 7547, 7549, 7559, 7561, 7573
7603, 7607, 7621, 7639, 7643, 7649, 7669, 7673, 7681, 7687, 7691, 7699, 7703, 7717
7757, 7759, 7789, 7793, 7817, 7823, 7829, 7841, 7853, 7867, 7873, 7877, 7879, 7883
7933, 7937, 7949, 7951, 7963, 7993, 8009, 8011, 8017, 8039, 8053, 8059, 8069, 8081
8111, 8117, 8123, 8147, 8161, 8167, 8171, 8179, 8191, 8209, 8219, 8221, 8231, 8233
8273, 8287, 8291, 8293, 8297, 8311, 8317, 8329, 8353, 8363, 8369, 8377, 8387, 8389
8443, 8447, 8461, 8467, 8501, 8513, 8521, 8527, 8537, 8539, 8543, 8563, 8573, 8581
8627, 8629, 8641, 8647, 8663, 8669, 8677, 8681, 8689, 8693, 8699, 8707, 8713, 8719
8753, 8761, 8779, 8783, 8803, 8807, 8819, 8821, 8831, 8837, 8839, 8849, 8861, 8863
8929, 8933, 8941, 8951, 8963, 8969, 8971, 8999, 9001, 9007, 9011, 9013, 9029, 9041
9091, 9103, 9109, 9127, 9133, 9137, 9151, 9157, 9161, 9173, 9181, 9187, 9199, 9203
9241, 9257, 9277, 9281, 9283, 9293, 9311, 9319, 9323, 9337, 9341, 9343, 9349, 9371
9413, 9419, 9421, 9431, 9433, 9437, 9439, 9461, 9463, 9467, 9473, 9479, 9491, 9497
9547, 9551, 9587, 9601, 9613, 9619, 9623, 9629, 9631, 9643, 9649, 9661, 9677, 9679
9733, 9739, 9743, 9749, 9767, 9769, 9781, 9787, 9791, 9803, 9811, 9817, 9829, 9833
9871, 9883, 9887, 9901, 9907, 9923, 9929, 9931, 9941, 9949, 9967, 9973, 10007, 100
10067, 10069, 10079, 10091, 10093, 10099, 10103, 10111, 10133, 10139, 10141, 10151
10177, 10181, 10193, 10211, 10223, 10243, 10247, 10253, 10259, 10267, 10271, 10273
10313, 10321, 10331, 10333, 10337, 10343, 10357, 10369, 10391, 10399, 10427, 10429
10459, 10463, 10477, 10487, 10499, 10501, 10513, 10529, 10531, 10559, 10567, 10589
10613, 10627, 10631, 10639, 10651, 10657, 10663, 10667, 10687, 10691, 10709, 10711
10739, 10753, 10771, 10781, 10789, 10799, 10831, 10837, 10847, 10853, 10859, 10861
10891, 10903, 10909, 10937, 10939, 10949, 10957, 10973, 10979, 10987, 10993, 11003
11059, 11069, 11071, 11083, 11087, 11093, 11113, 11117, 11119, 11131, 11149, 11159
11177, 11197, 11213, 11239, 11243, 11251, 11257, 11261, 11273, 11279, 11287, 11299
11329, 11351, 11353, 11369, 11383, 11393, 11399, 11411, 11423, 11437, 11443, 11447
11489, 11491, 11497, 11503, 11519, 11527, 11549, 11551, 11579, 11587, 11593, 11597
11657, 11677, 11681, 11689, 11699, 11701, 11717, 11719, 11731, 11743, 11777, 11779
11807, 11813, 11821, 11827, 11831, 11833, 11839, 11863, 11867, 11887, 11897, 11903
11933, 11939, 11941, 11953, 11959, 11969, 11971, 11981, 11987, 12007, 12011, 12037
12071, 12073, 12097, 12101, 12107, 12109, 12113, 12119, 12143, 12149, 12157, 12161
12211, 12227, 12239, 12241, 12251, 12253, 12263, 12269, 12277, 12281, 12289, 12301
12347, 12373, 12377, 12379, 12391, 12401, 12409, 12413, 12421, 12433, 12437, 12451
12487, 12491, 12497, 12503, 12511, 12517, 12527, 12539, 12541, 12547, 12553, 12569
12601, 12611, 12613, 12619, 12637, 12641, 12647, 12653, 12659, 12671, 12689, 12697
12739, 12743, 12757, 12763, 12781, 12791, 12799, 12809, 12821, 12823, 12829, 12841
12899, 12907, 12911, 12917, 12919, 12923, 12941, 12953, 12959, 12967, 12973, 12979
13007, 13009, 13033, 13037, 13043, 13049, 13063, 13093, 13099, 13103, 13109, 13121
13159, 13163, 13171, 13177, 13183, 13187, 13217, 13219, 13229, 13241, 13249, 13259
13309, 13313, 13327, 13331, 13337, 13339, 13367, 13381, 13397, 13399, 13411, 13417
13457, 13463, 13469, 13477, 13487, 13499, 13513, 13523, 13537, 13553, 13567, 13577
```

```
            13619, 13627, 13633, 13649, 13669, 13679, 13681, 13687, 13691, 13693, 13697, 1370
            13729, 13751, 13757, 13759, 13763, 13781, 13789, 13799, 13807, 13829, 13831, 1384
            13879, 13883, 13901, 13903, 13907, 13913, 13921, 13931, 13933, 13963, 13967, 1399
            14029, 14033, 14051, 14057, 14071, 14081, 14083, 14087, 14107, 14143, 14149, 1415
            14197, 14207, 14221, 14243, 14249, 14251, 14281, 14293, 14303, 14321, 14323, 1432
            14387, 14389, 14401, 14407, 14411, 14419, 14423, 14431, 14437, 14447, 14449, 1446
            14519, 14533, 14537, 14543, 14549, 14551, 14557, 14561, 14563, 14591, 14593, 1462
            14639, 14653, 14657, 14669, 14683, 14699, 14713, 14717, 14723, 14731, 14737, 1474
            14767, 14771, 14779, 14783, 14797, 14813, 14821, 14827, 14831, 14843, 14851, 1486
            14891, 14897, 14923, 14929, 14939, 14947, 14951, 14957, 14969, 14983, 15013, 1501
            15073, 15077, 15083, 15091, 15101, 15107, 15121, 15131, 15137, 15139, 15149, 1516
            15199, 15217, 15227, 15233, 15241, 15259, 15263, 15269, 15271, 15277, 15287, 1528
            15319, 15329, 15331, 15349, 15359, 15361, 15373, 15377, 15383, 15391, 15401, 1541
            15451, 15461, 15467, 15473, 15493, 15497, 15511, 15527, 15541, 15551, 15559, 1556
            15607, 15619, 15629, 15641, 15643, 15647, 15649, 15661, 15667, 15671, 15679, 1568
            15737, 15739, 15749, 15761, 15767, 15773, 15787, 15791, 15797, 15803, 15809, 1581
            15881, 15887, 15889, 15901, 15907, 15913, 15919, 15923, 15937, 15959, 15971, 1597
            16033, 16057, 16061, 16063, 16067, 16069, 16073, 16087, 16091, 16097, 16103, 1611
            16183, 16187, 16189, 16193, 16217, 16223, 16229, 16231, 16249, 16253, 16267, 1627
            16339, 16349, 16361, 16363, 16369, 16381, 16411, 16417, 16421, 16427, 16433, 1644
            16481, 16487, 16493, 16519, 16529, 16547, 16553, 16561, 16567, 16573, 16603, 1660
            16649, 16651, 16657, 16661, 16673, 16691, 16693, 16699, 16703, 16729, 16741, 1674
            16811, 16823, 16829, 16831, 16843, 16871, 16879, 16883, 16889, 16901, 16903, 1692
            16943, 16963, 16979, 16981, 16987, 16993, 17011, 17021, 17027, 17029, 17033, 1704
            17093, 17099, 17107, 17117, 17123, 17137, 17159, 17167, 17183, 17189, 17191, 1720
            17239, 17257, 17291, 17293, 17299, 17317, 17321, 17327, 17333, 17341, 17351, 1735

function response(room, msg, sender, isGroupChat, replier, ImageDB, packageName, threadId) {
    if(msg=="Bot!GetKeypair"){
        var usingPrimes = primes;
        var p = randomItem(usingPrimes);
        usingPrimes.splice(usingPrimes.indexOf(p), 1);
        var q = randomItem(usingPrimes);
        var tot = totient(p, q);
        var n = p * q;
        var publicKey = get_public_key(tot);
        var privateKey= get_private_key(publicKey, tot);
        replier.reply("[Public Key]\n"+"n="+n.toString()+" "+"Encrypt Key: "+publicKey.toString
        replier.reply("[Private Key]\n"+"n="+n.toString()+" "+"Decrypt Key: "+privateKey.toStri
    }
}
```

OtakoidTony님의 게시글 더보기 >

좋아요 **1** 댓글 **3** 공유 | 신고

댓글 등록순 최신순

댓글알림

srfu

자바는 착해서 API쓰면 됩니다

2019.11.23. 21:04 답글쓰기

odosk

ㄹㅇ

2019.11.24. 04:18 답글쓰기

Bunked

감사합니다 잘 이용하겠습니다

2020.01.07. 00:41 답글쓰기

Hibot

댓글을 남겨보세요

등록

글쓰기 답글 목록 ▲ TOP

'| 일반 소스 공유 |' 게시판 글

이 게시판 새글 구독하기

파이썬 인공신경망과 자바스크립트 인공신경망 [12]	OtakoidTony	2019.11.23.
내가 처음으로 봇에 추가했던 기능. [12]	OtakoidTony	2019.11.23.
RSA Encryption [3]	OtakoidTony	2019.11.23.
클래시로얄 전적 Jsoup [4]	doami2005	2019.11.23.
배그전적 [5]	흐미	2019.11.23.

1 2 3 전체보기

이 카페 인기글

틱택토 (카카오링크 적용)

도미 doami2005
♡1 💬2

반가워요.

천방지축하연
♡0 💬4

타 메신저 사용시 무한반복

NaN
♡0 💬1

글자의 개수가 넘어가면 자르기 질문

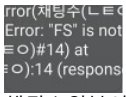
흑까마귀
♡0 💬5

[치***, 한**] 님 강제 탈퇴

AlphaDo
♡1 💬2

오픈이발 괴롭히기(메봇R)

ERROR
♡0 💬7



채팅순위봇이 갑자기 안되네요..ㅠ

eval 질문

Kiri
♡0 💬5

카톡방 나가기

hajuhee01
♡0 💬15

1 2 3 4 5