

RSA Program :

```
def gcd(a, b): # calculates GCD of a and d
    while b != 0:
        c = a % b
        a = b
        b = c
    return a

def modinv(a, m): # calculates modulo inverse of a for
mod m    for x in range(1, m):
    if (a * x) % m == 1:
        return x
    return None

def coprimes(a): # calculates all possible co-prime numbers
with a    l = []
    for x in range(2, a):
        if gcd(a, x) == 1 and modinv(x, phi) != None:
l.append(x)
    for x in l:
        if x == modinv(x, phi):
l.remove(x)
    return l

def encrypt_block(m): # encrypts a single block
    c = m ** e % n
    return c

def decrypt_block(c): # decrypts a single block
    m = c ** d % n
    return m

def encrypt_string(s): # applies encryption
    return ''.join([chr(encrypt_block(ord(x))) for x in list(s)])

def decrypt_string(s): # applies decryption
    return ''.join([chr(decrypt_block(ord(x))) for x in list(s)])

if __name__ == "__main__":
    p = int(input('Enter prime p: '))
    q = int(input('Enter prime q: '))

    print("Choosen primes:\np=" + str(p) + ", q=" + str(q) + "\n")

    n = p * q
    print("n = p * q = " + str(n) + "\n")

    phi = (p - 1) * (q - 1)
    print("Euler's function (totient) [phi(n)]: " + str(phi) + "\n")

    print("Choose an e from a below coprimes array:\n")
    print(str(coprimes(phi)) + "\n")
```

```

e = int(input())

d = modinv(e, phi) # calculates the decryption key d

print("\nYour public key is a pair of numbers (e=" + str(e) + ", n="
+ str(n) + ").\n")
print("Your private key is a pair of numbers (d=" + str(d) + ", n=" +
str(n) + ").\n")

s = input("Enter a message to encrypt: ")
print("\nPlain message: " + s + "\n")
enc = encrypt_string(s)
print("Encrypted message: ", enc, "\n")
dec = decrypt_string(enc)
print("Decrypted message: " + dec + "\n")

```

Output:

```

PS E:\LP2> python -u "e:\LP2\RSA.py"
Enter prime p: 53
Enter prime q: 59
Chosen primes:
p=53, q=59

n = p * q = 3127

Euler's function (totient) [phi(n)]: 3016

Choose an e from a below coprimes array:

[3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25, 27, 31, 33, 35, 37, 41, 43, 45, 47, 49, 51, 53, 55, 57,
59, 61, 63, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 89, 93, 95, 97, 99, 101, 103, 105, 107, 109,
111, 113, 115, 117, 121, 123, 125, 127, 129, 131, 133, 135, 137, 139, 141, 147, 149, 151, 153, 15
5, 157, 159, 161, 163, 165, 167, 171, 173, 175, 177, 179, 181, 183, 185, 187, 189, 191, 193, 197,
199, 201, 205, 207, 209, 211, 213, 215, 217, 219, 223, 225, 227, 229, 231, 235, 237, 239, 241, 2
43, 245, 249, 251, 253, 255, 257, 259, 263, 265, 267, 269, 271, 275, 277, 279, 281, 283, 285, 287
, 289, 291, 293, 295, 297, 301, 303, 305, 307, 309, 311, 313, 315, 317, 321, 323, 327, 329, 331,
333, 335, 337, 339, 341, 343, 345, 347, 349, 353, 355, 357, 359, 361, 363, 365, 367, 369, 371, 37
3, 375, 379, 381, 383, 385, 387, 389, 391, 393, 395, 397, 399, 401, 405, 407, 409, 411, 413, 415,
417, 419, 421, 423, 425, 427, 431, 433, 437, 439, 441, 443, 445, 447, 449, 451, 453, 457, 459, 4
61, 463, 465, 467, 469, 471, 473, 475, 477, 479, 483, 485, 487, 489, 491, 495, 497, 499, 501, 503
, 505, 509, 511, 513, 515, 517, 519, 523, 525, 527, 529, 531, 535, 537, 539, 541, 543, 545, 547,
549, 553, 555, 557, 561, 563, 565, 567, 569, 571, 573, 575, 577, 579, 581, 583, 587, 589, 591, 59
3, 595, 597, 599, 601, 603, 605, 607, 613, 615, 617, 619, 621, 623, 625, 627, 629, 631, 633, 635,
639, 641, 643, 645, 647, 649, 651, 653, 655, 657, 659, 661, 665, 669, 671, 673, 675, 677, 679, 6
81, 683, 685, 687, 691, 693, 695, 697, 699, 701, 703, 705, 707, 709, 711, 713, 717, 719, 721, 723
, 727, 729, 731, 733, 735, 737, 739, 743, 745, 747, 749, 751, 755, 757, 759, 761, 763, 765, 769,
771, 773, 775, 777, 779, 781, 785, 787, 789, 791, 795, 797, 799, 801, 803, 805, 807, 809, 811, 81
3, 815, 817, 821, 823, 825, 827, 829, 831, 833, 835, 837, 839, 843, 847, 849, 851, 853, 855, 857,
859, 861, 863, 865, 867, 869, 873, 875, 877, 879, 881, 883, 885, 887, 889, 891, 893, 895, 901, 9
03, 905, 907, 909, 911, 913, 915, 917, 919, 921, 925, 927, 929, 931, 933, 935, 937, 939, 941, 943
, 945, 947, 951, 953, 955, 959, 961, 963, 965, 967, 969, 971, 973, 977, 979, 981, 983, 985, 989,
991, 993, 995, 997, 999, 1003, 1005, 1007, 1009, 1011, 1013, 1017, 1019, 1021, 1023, 1025, 1029,
1031, 1033, 1035, 1037, 1039, 1041, 1043, 1045, 1047, 1049, 1051, 1055, 1057, 1059, 1061, 1063, 1
065, 1067, 1069, 1071, 1075, 1077, 1081, 1083, 1085, 1087, 1089, 1091, 1093, 1095, 1097, 1099, 11
01, 1103, 1107, 1109, 1111, 1113, 1115, 1117, 1119, 1121, 1123, 1125, 1127, 1129, 1133, 1135, 113
7, 1139, 1141, 1143, 1145, 1147, 1149, 1151, 1153, 1155, 1159, 1161, 1163, 1165, 1167, 1169, 1171
, 1173, 1175, 1177, 1179, 1181, 1185, 1187, 1191, 1193, 1195, 1197, 1199, 1201, 1203, 1205, 1207,
1211, 1213, 1215, 1217, 1219, 1221, 1223, 1225, 1227, 1229, 1231, 1233, 1237, 1239, 1241, 1243,
1245, 1249, 1251, 1253, 1255, 1257, 1259, 1263, 1265, 1267, 1269, 1271, 1273, 1277, 1279, 1281, 1
283, 1285, 1289, 1291, 1293, 1295, 1297, 1299, 1301, 1303, 1307, 1309, 1311, 1315, 1317, 1319, 13
21, 1323, 1325, 1327, 1329, 1331, 1333, 1335, 1337, 1341, 1343, 1345, 1347, 1349, 1351, 1353, 135
5, 1357, 1359, 1361, 1367, 1369, 1371, 1373, 1375, 1377, 1379, 1381, 1383, 1385, 1387, 1389, 1393

```

```
Code - LP2 - Visual Studio Code
File Edit Selection View Go Run Terminal Help
RSApy Code x
1465, 1467, 1471, 1473, 1475, 1477, 1481, 1483, 1485, 1487, 1489, 1491, 1493, 1497, 1499, 1501, 1
503, 1505, 1509, 1511, 1513, 1515, 1517, 1519, 1523, 1525, 1527, 1529, 1531, 1533, 1535, 1539, 15
41, 1543, 1545, 1549, 1551, 1553, 1555, 1557, 1559, 1561, 1563, 1565, 1567, 1569, 1571, 1575, 157
7, 1579, 1581, 1583, 1585, 1587, 1589, 1591, 1593, 1597, 1601, 1603, 1605, 1607, 1609, 1611, 1613
, 1615, 1617, 1619, 1621, 1623, 1627, 1629, 1631, 1633, 1635, 1637, 1639, 1641, 1643, 1645, 1647
, 1649, 1655, 1657, 1659, 1661, 1663, 1665, 1667, 1669, 1671, 1673, 1675, 1679, 1681, 1683, 1685
, 1687, 1689, 1691, 1693, 1695, 1697, 1699, 1701, 1705, 1707, 1709, 1713, 1715, 1717, 1719, 1721, 1
723, 1725, 1727, 1731, 1733, 1735, 1737, 1739, 1743, 1745, 1747, 1749, 1751, 1753, 1757, 1759, 17
61, 1763, 1765, 1767, 1771, 1773, 1775, 1777, 1779, 1783, 1785, 1787, 1789, 1791, 1793, 1795, 179
7, 1799, 1801, 1803, 1805, 1809, 1811, 1813, 1815, 1817, 1819, 1821, 1823, 1825, 1829, 1831, 1835
, 1837, 1839, 1841, 1843, 1845, 1847, 1849, 1851, 1853, 1855, 1857, 1861, 1863, 1865, 1867, 1869
, 1871, 1873, 1875, 1877, 1879, 1881, 1883, 1887, 1889, 1891, 1893, 1895, 1897, 1899, 1901, 1903
, 1905, 1907, 1909, 1913, 1915, 1917, 1919, 1921, 1923, 1925, 1927, 1929, 1931, 1933, 1935, 1939, 1
941, 1945, 1947, 1949, 1951, 1953, 1955, 1957, 1959, 1961, 1965, 1967, 1969, 1971, 1973, 1975, 19
77, 1979, 1981, 1983, 1985, 1987, 1991, 1993, 1995, 1997, 1999, 2003, 2005, 2007, 2009, 2011, 2013,
2017, 2019, 2021, 2023, 2025, 2027, 2031, 2033, 2035, 2037, 2039, 2043, 2045, 2047, 2049, 2051, 2053, 20
55, 2057, 2061, 2063, 2065, 2069, 2071, 2073, 2075, 2077, 2079, 2081, 2083, 2085, 2087, 2089, 2091, 2095
, 2097, 2099, 2101, 2103, 2105, 2107, 2109, 2111, 2113, 2115, 2121, 2123, 2125, 2127, 2129, 2131, 21
33, 2135, 2137, 2139, 2141, 2143, 2147, 2149, 2151, 2153, 2155, 2157, 2159, 2161, 2163, 2165, 2167, 2169
, 2173, 2177, 2179, 2181, 2183, 2185, 2187, 2189, 2191, 2193, 2195, 2199, 2201, 2203, 2205, 2207, 22
09, 2211, 2213, 2215, 2217, 2219, 2221, 2225, 2227, 2229, 2231, 2235, 2237, 2239, 2241, 2243, 2245
, 2247, 2251, 2253, 2255, 2257, 2259, 2263, 2265, 2267, 2269, 2271, 2273, 2277, 2279, 2281, 2283, 2285
, 2287, 2289, 2293, 2295, 2297, 2299, 2303, 2305, 2307, 2309, 2311, 2313, 2315, 2317, 2319, 2321, 2323
, 2325, 2329, 2331, 2333, 2335, 2337, 2339, 2341, 2343, 2345, 2347, 2351, 2353, 2355, 2357, 2359, 2361
, 2363, 2365, 2367, 2369, 2371, 2373, 2375, 2377, 2381, 2383, 2385, 2387, 2389, 2391, 2393, 2395, 2397
, 2399, 2401, 2403, 2405, 2407, 2409, 2411, 2413, 2415, 2417, 2419, 2421, 2423, 2425, 2427, 2429, 2431
, 2433, 2435, 2437, 2439, 2441, 2443, 2445, 2447, 2449, 2451, 2453, 2455, 2457, 2459, 2461, 2463, 2465
, 2467, 2469, 2471, 2473, 2475, 2477, 2479, 2481, 2483, 2485, 2487, 2489, 2491, 2493, 2495, 2497, 2499
, 2501, 2503, 2505, 2507, 2509, 2511, 2513, 2515, 2517, 2519, 2521, 2523, 2525, 2527, 2529, 2531, 2533
, 2535, 2537, 2539, 2541, 2543, 2545, 2547, 2549, 2551, 2553, 2555, 2557, 2559, 2561, 2563, 2565, 2567
, 2569, 2571, 2573, 2575, 2577, 2579, 2581, 2583, 2585, 2587, 2589, 2591, 2593, 2595, 2597, 2599, 2601
, 2603, 2605, 2607, 2609, 2611, 2613, 2615, 2617, 2619, 2621, 2623, 2625, 2627, 2629, 2631, 2633, 2635
, 2637, 2639, 2641, 2643, 2645, 2647, 2649, 2651, 2653, 2655, 2657, 2659, 2661, 2663, 2665, 2667, 2669
, 2671, 2673, 2675, 2677, 2679, 2681, 2683, 2685, 2687, 2689, 2691, 2693, 2695, 2697, 2699, 2701, 2703
, 2705, 2707, 2709, 2711, 2713, 2715, 2717, 2719, 2721, 2723, 2725, 2727, 2729, 2731, 2733, 2735, 2737
, 2739, 2741, 2743, 2745, 2747, 2749, 2751, 2753, 2755, 2757, 2759, 2761, 2763, 2765, 2767, 2769, 2771
, 2773, 2775, 2777, 2779, 2781, 2783, 2785, 2787, 2789, 2791, 2793, 2795, 2797, 2799, 2801, 2803, 2805
, 2807, 2809, 2811, 2813, 2815, 2817, 2819, 2821, 2823, 2825, 2827, 2829, 2831, 2833, 2835, 2837, 2839
, 2841, 2843, 2845, 2847, 2849, 2851, 2853, 2855, 2857, 2859, 2861, 2863, 2865, 2867, 2869, 2871, 2873
, 2875, 2877, 2879, 2881, 2883, 2885, 2887, 2889, 2891, 2893, 2895, 2897, 2899, 2901, 2903, 2905, 2907
, 2909, 2911, 2913, 2915, 2917, 2919, 2921, 2923, 2925, 2927, 2929, 2931, 2933, 2935, 2937, 2939, 2941
, 2943, 2945, 2947, 2949, 2951, 2953, 2955, 2957, 2959, 2961, 2963, 2965, 2967, 2969, 2971, 2973, 2975, 29
79, 2981, 2983, 2985, 2989, 2991, 2993, 2995, 2997, 2999, 3001, 3005, 3007, 3009, 3011, 3013]
3
Your public key is a pair of numbers (e=3, n=3127).
Your private key is a pair of numbers (d=2011, n=3127).
Enter a message to encrypt: sahil
Plain message: sahil
Encrypted message: 2540
Decrypted message: sahil
PS E:\LP2>
```