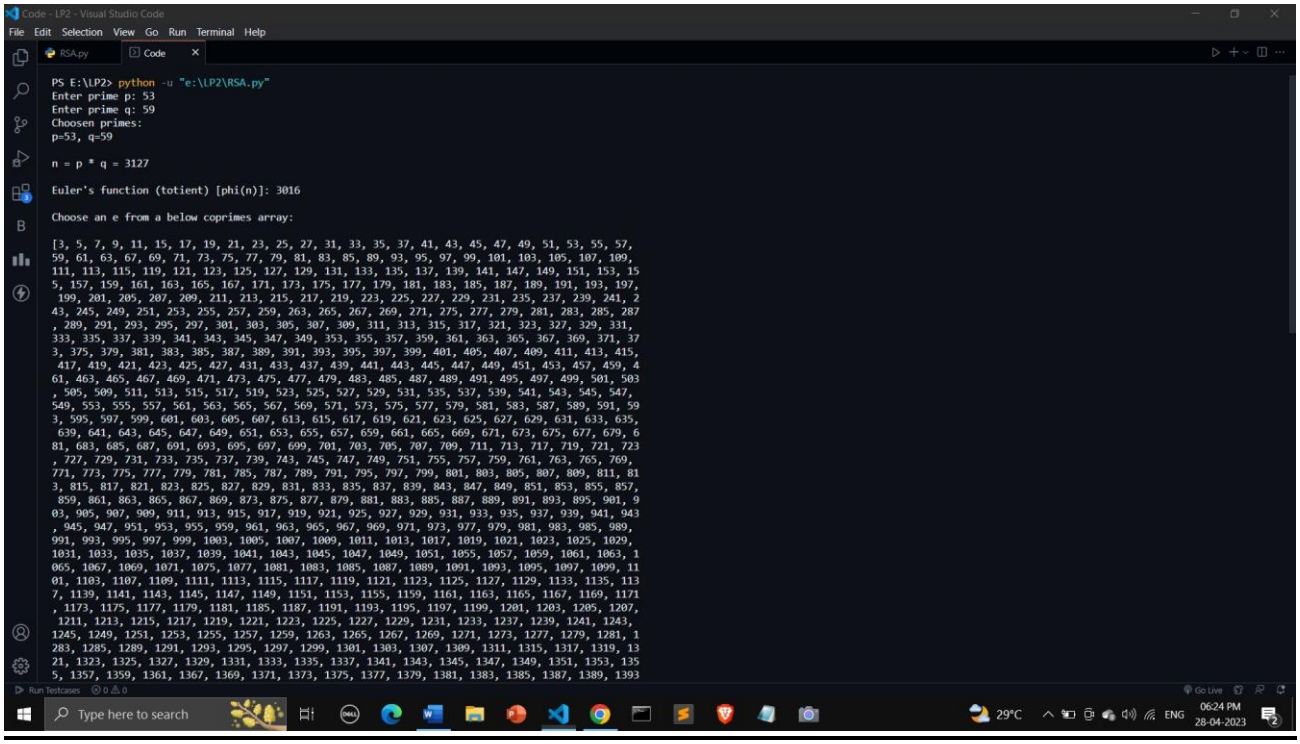
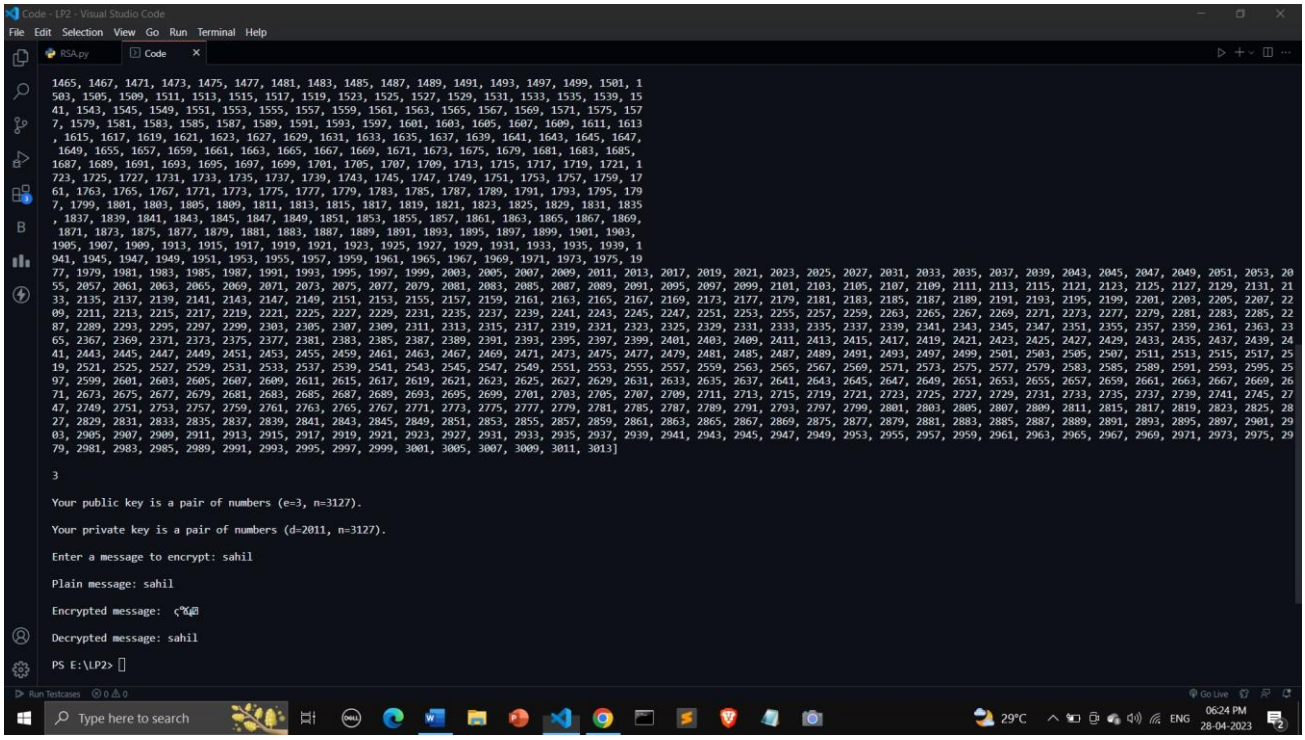
RSA Program :

```
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:




Code - LP2 - Visual Studio Code
File Edit Selection View Go Run Terminal Help
RSA.py
Code
1465, 1467, 1471, 1473, 1475, 1477, 1481, 1483, 1485, 1487, 1489, 1491, 1493, 1497, 1499, 1501, 1503, 1505, 1509, 1511, 1513, 1515, 1517, 1519, 1523, 1525, 1527, 1529, 1531, 1533, 1535, 1539, 1541, 1543, 1545, 1549, 1551, 1553, 1555, 1557, 1559, 1561, 1563, 1565, 1567, 1569, 1571, 1575, 1577, 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, 1723, 1725, 1727, 1731, 1733, 1735, 1737, 1739, 1743, 1745, 1747, 1749, 1751, 1753, 1757, 1759, 1761, 1763, 1765, 1767, 1771, 1773, 1775, 1777, 1779, 1783, 1785, 1787, 1789, 1791, 1793, 1795, 1797, 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, 1941, 1945, 1947, 1949, 1951, 1953, 1955, 1957, 1959, 1961, 1965, 1967, 1969, 1971, 1973, 1975, 1977, 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, 2055, 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, 2133, 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, 2209, 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, 2355, 2357, 2359, 2361, 2363, 2365, 2367, 2369, 2371, 2373, 2375, 2377, 2381, 2383, 2385, 2387, 2389, 2391, 2393, 2395, 2397, 2399, 2401, 2403, 2409, 2411, 2413, 2415, 2417, 2419, 2421, 2423, 2425, 2427, 2429, 2433, 2435, 2437, 2439, 2441, 2443, 2445, 2447, 2449, 2451, 2453, 2455, 2459, 2461, 2463, 2467, 2469, 2471, 2473, 2475, 2477, 2479, 2481, 2485, 2487, 2489, 2491, 2493, 2497, 2499, 2501, 2503, 2505, 2507, 2511, 2513, 2515, 2517, 2519, 2521, 2525, 2527, 2529, 2531, 2533, 2537, 2539, 2541, 2543, 2545, 2547, 2549, 2551, 2553, 2555, 2557, 2559, 2563, 2565, 2567, 2569, 2571, 2573, 2575, 2577, 2579, 2583, 2585, 2589, 2591, 2593, 2595, 2597, 2599, 2601, 2603, 2605, 2607, 2609, 2611, 2615, 2617, 2619, 2621, 2623, 2625, 2627, 2629, 2631, 2633, 2635, 2637, 2641, 2643, 2645, 2647, 2649, 2651, 2653, 2655, 2657, 2659, 2661, 2663, 2667, 2669, 2671, 2673, 2675, 2677, 2679, 2681, 2683, 2685, 2687, 2689, 2693, 2695, 2699, 2701, 2703, 2705, 2707, 2709, 2711, 2713, 2715, 2719, 2721, 2723, 2725, 2727, 2729, 2731, 2733, 2735, 2737, 2739, 2741, 2745, 2747, 2749, 2751, 2753, 2757, 2759, 2761, 2763, 2765, 2767, 2771, 2773, 2775, 2777, 2779, 2781, 2785, 2787, 2789, 2791, 2793, 2797, 2799, 2801, 2803, 2805, 2807, 2809, 2811, 2815, 2817, 2819, 2823, 2825, 2827, 2829, 2831, 2833, 2835, 2837, 2839, 2841, 2843, 2845, 2849, 2851, 2853, 2855, 2857, 2859, 2861, 2863, 2865, 2867, 2869, 2875, 2877, 2879, 2881, 2883, 2885, 2887, 2889, 2891, 2893, 2895, 2897, 2901, 2903, 2905, 2907, 2909, 2911, 2913, 2915, 2917, 2919, 2921, 2923, 2927, 2931, 2933, 2935, 2937, 2939, 2941, 2943, 2945, 2947, 2949, 2953, 2955, 2957, 2959, 2961, 2963, 2965, 2967, 2969, 2971, 2973, 2975, 2979, 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:
Decrypted message: sahil
PS E:\LP2>
Run Testcases
Go Live
Type here to search
29°C
ENG
06:24 PM
28-04-2023