CS 58000\_01 Design, Analysis, and Implementation Algorithms (3 cr.)

Assignment As\_02 (Exam 01)

Student Name: **Harsh Sharma**

This assignment As\_02 is due at 11:59 p.m., Sunday, October 1, 2023. Please submit your assignment to Brightspace (purdue.brightspace.com). No late turn-in is accepted. Please write your name on the first page of your assignment. Your file name should be your last name such as NgP\_As02.docx. Please number your problem-answer clearly such as Problem I.1.a, I.1.b, I.1.c, I.2, …, I.7, Problem II.1, II.2, II.3, II.4. The problems’ answers must be arranged according to the order of the given problem. Please answer your questions using only a Word file (.docx file only). No pdf file will be accepted. Without using a Word file (.docx file) the submitted problems’ answers would not be graded.

The total number of points for this Assignment\_02 (Exam 01) is 150 points.

Problem I [110 points]:

This problem is an exercise using the formalization of the RSA public-key cryptosystem. To solve the problems, you are required to use the following formalization of the RSA public-key cryptosystem.

Given the following formalization of the RSA public-key cryptosystem, each participant creates their public key (n, g) where a is a small prime number, and n is the product of two large primes, p and q. However, the two large primes p and q are secret keys.

1. Select two very large prime numbers p and q. The number of bits needed to represent p and q might be 1024.
2. Compute

n = pq

(n) = (p – 1) (q – 1).

The formula for (n) is owing to the Theorem: The number of elements in is given by Euler’s totient function, which is

where the product is over all primes that divide n, including n if n is prime.

1. Choose a small prime number as an encryption component g, that is relatively prime to (n). That means,

gcd(g, (n) ) = 1, i.e.,

gcd(g, (p-1)(q-1)) = 1.

1. Compute the multiplicative inverse That is,

The inverse exists and is unique.

That is, the decryption component h = g-1 mod (n).

1. Let pkey = (n, g) be the public key, and skey = (p, q, h) be the secret key.

* For any message M mod n, the encryption of M is C = Mg mod n.
* The decryption of C is M = Ch mod n.

End of the formalization of the RSA public-key cryptosystem.

Use the RSA Cryptosystem formalism for solving problem I.

Given g = 59, p = 991 and q = 997.

I.1. [30 pts.] Show that the given values of g, p, and q are prime,

I.1.a Use the Algorithm Sieve (the Sieve of Eratosthenes Method) to check whether p is a prime.

Solution:

In order to check whether p, 991, is prime or not using Sieve of Eratosthenes Method we need to have a list of integers from 2 to 991. Then need to remove all the multiples of numbers from 2 to square root of 991, i.e., till 32 (upper limit).

List of integers which are multiple of 2 and hence to be removed: [2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164, 166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192, 194, 196, 198, 200, 202, 204, 206, 208, 210, 212, 214, 216, 218, 220, 222, 224, 226, 228, 230, 232, 234, 236, 238, 240, 242, 244, 246, 248, 250, 252, 254, 256, 258, 260, 262, 264, 266, 268, 270, 272, 274, 276, 278, 280, 282, 284, 286, 288, 290, 292, 294, 296, 298, 300, 302, 304, 306, 308, 310, 312, 314, 316, 318, 320, 322, 324, 326, 328, 330, 332, 334, 336, 338, 340, 342, 344, 346, 348, 350, 352, 354, 356, 358, 360, 362, 364, 366, 368, 370, 372, 374, 376, 378, 380, 382, 384, 386, 388, 390, 392, 394, 396, 398, 400, 402, 404, 406, 408, 410, 412, 414, 416, 418, 420, 422, 424, 426, 428, 430, 432, 434, 436, 438, 440, 442, 444, 446, 448, 450, 452, 454, 456, 458, 460, 462, 464, 466, 468, 470, 472, 474, 476, 478, 480, 482, 484, 486, 488, 490, 492, 494, 496, 498, 500, 502, 504, 506, 508, 510, 512, 514, 516, 518, 520, 522, 524, 526, 528, 530, 532, 534, 536, 538, 540, 542, 544, 546, 548, 550, 552, 554, 556, 558, 560, 562, 564, 566, 568, 570, 572, 574, 576, 578, 580, 582, 584, 586, 588, 590, 592, 594, 596, 598, 600, 602, 604, 606, 608, 610, 612, 614, 616, 618, 620, 622, 624, 626, 628, 630, 632, 634, 636, 638, 640, 642, 644, 646, 648, 650, 652, 654, 656, 658, 660, 662, 664, 666, 668, 670, 672, 674, 676, 678, 680, 682, 684, 686, 688, 690, 692, 694, 696, 698, 700, 702, 704, 706, 708, 710, 712, 714, 716, 718, 720, 722, 724, 726, 728, 730, 732, 734, 736, 738, 740, 742, 744, 746, 748, 750, 752, 754, 756, 758, 760, 762, 764, 766, 768, 770, 772, 774, 776, 778, 780, 782, 784, 786, 788, 790, 792, 794, 796, 798, 800, 802, 804, 806, 808, 810, 812, 814, 816, 818, 820, 822, 824, 826, 828, 830, 832, 834, 836, 838, 840, 842, 844, 846, 848, 850, 852, 854, 856, 858, 860, 862, 864, 866, 868, 870, 872, 874, 876, 878, 880, 882, 884, 886, 888, 890, 892, 894, 896, 898, 900, 902, 904, 906, 908, 910, 912, 914, 916, 918, 920, 922, 924, 926, 928, 930, 932, 934, 936, 938, 940, 942, 944, 946, 948, 950, 952, 954, 956, 958, 960, 962, 964, 966, 968, 970, 972, 974, 976, 978, 980, 982, 984, 986, 988, 990]

List of integers which are multiple of 3 and hence to be removed: [3, 9, 15, 21, 27, 33, 39, 45, 51, 57, 63, 69, 75, 81, 87, 93, 99, 105, 111, 117, 123, 129, 135, 141, 147, 153, 159, 165, 171, 177, 183, 189, 195, 201, 207, 213, 219, 225, 231, 237, 243, 249, 255, 261, 267, 273, 279, 285, 291, 297, 303, 309, 315, 321, 327, 333, 339, 345, 351, 357, 363, 369, 375, 381, 387, 393, 399, 405, 411, 417, 423, 429, 435, 441, 447, 453, 459, 465, 471, 477, 483, 489, 495, 501, 507, 513, 519, 525, 531, 537, 543, 549, 555, 561, 567, 573, 579, 585, 591, 597, 603, 609, 615, 621, 627, 633, 639, 645, 651, 657, 663, 669, 675, 681, 687, 693, 699, 705, 711, 717, 723, 729, 735, 741, 747, 753, 759, 765, 771, 777, 783, 789, 795, 801, 807, 813, 819, 825, 831, 837, 843, 849, 855, 861, 867, 873, 879, 885, 891, 897, 903, 909, 915, 921, 927, 933, 939, 945, 951, 957, 963, 969, 975, 981, 987]

List of integers which are multiple of 4 and hence to be removed: [] (all multiples of 4 already removed by 2.)

List of integers which are multiple of 5 and hence to be removed: [5, 25, 35, 55, 65, 85, 95, 115, 125, 145, 155, 175, 185, 205, 215, 235, 245, 265, 275, 295, 305, 325, 335, 355, 365, 385, 395, 415, 425, 445, 455, 475, 485, 505, 515, 535, 545, 565, 575, 595, 605, 625, 635, 655, 665, 685, 695, 715, 725, 745, 755, 775, 785, 805, 815, 835, 845, 865, 875, 895, 905, 925, 935, 955, 965, 985]

List of integers which are multiple of 6 and hence to be removed: [] (all multiples of 6 already removed by 2 and 3.)

List of integers which are multiple of 7 and hence to be removed: [7, 49, 77, 91, 119, 133, 161, 203, 217, 259, 287, 301, 329, 343, 371, 413, 427, 469, 497, 511, 539, 553, 581, 623, 637, 679, 707, 721, 749, 763, 791, 833, 847, 889, 917, 931, 959, 973]

List of integers which are multiple of 8 and hence to be removed: []

List of integers which are multiple of 9 and hence to be removed: []

List of integers which are multiple of 10 and hence to be removed: []

List of integers which are multiple of 11 and hence to be removed: [11, 121, 143, 187, 209, 253, 319, 341, 407, 451, 473, 517, 583, 649, 671, 737, 781, 803, 869, 913, 979]

List of integers which are multiple of 12 and hence to be removed: []

List of integers which are multiple of 13 and hence to be removed: [13, 169, 221, 247, 299, 377, 403, 481, 533, 559, 611, 689, 767, 793, 871, 923, 949]

List of integers which are multiple of 14 and hence to be removed: []

List of integers which are multiple of 15 and hence to be removed: []

List of integers which are multiple of 16 and hence to be removed: []

List of integers which are multiple of 17 and hence to be removed: [17, 289, 323, 391, 493, 527, 629, 697, 731, 799, 901]

List of integers which are multiple of 18 and hence to be removed: []

List of integers which are multiple of 19 and hence to be removed: [19, 361, 437, 551, 589, 703, 779, 817, 893]

List of integers which are multiple of 20 and hence to be removed: []

List of integers which are multiple of 21 and hence to be removed: []

List of integers which are multiple of 22 and hence to be removed: []

List of integers which are multiple of 23 and hence to be removed: [23, 529, 667, 713, 851, 943, 989]

List of integers which are multiple of 24 and hence to be removed: []

List of integers which are multiple of 25 and hence to be removed: []

List of integers which are multiple of 26 and hence to be removed: []

List of integers which are multiple of 27 and hence to be removed: []

List of integers which are multiple of 28 and hence to be removed: []

List of integers which are multiple of 29 and hence to be removed: [29, 841, 899]

List of integers which are multiple of 30 and hence to be removed: []

List of integers which are multiple of 31 and hence to be removed: [31, 961]

List of integers which are multiple of 32 and hence to be removed: []

After removing all the multiples from the list of integers, we are left with this list: [37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991]

As per Sieve of Eratosthenes Method, this list is a list of all prime numbers. And since 991 is in the list, 991 must be a prime number.

Note: To implement the above Sieve of Eratosthenes Method, I wrote a code whose screenshot I’m attaching below.

A screenshot of a computer

Description automatically generated

I.1.c. How do you check that g is a prime? Show the work of how you compute.

Solution: I’m using Sieve of Eratosthenes Method to check whether g, 59, is prime or not. For this I need to create a list of integers from 2 to 59, i.e., integers = {2, 3, 4…, 59}

Now we need to remove all the multiples of primes from 2 to square root of 59, i.e., till 8 (taking upper limit).

List of integers which are multiple of 2 and hence to be removed: [2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58]

List of integers which are multiple of 3 and hence to be removed: [3, 9, 15, 21, 27, 33, 39, 45, 51, 57]

List of integers which are multiple of 4 and hence to be removed: [] (all the multiples of 4 already removed by 2).

List of integers which are multiple of 5 and hence to be removed: [5, 25, 35, 55]

List of integers which are multiple of 6 and hence to be removed: []

List of integers which are multiple of 7 and hence to be removed: [7, 49]

List of integers which are multiple of 8 and hence to be removed: []

List of integers we are left with are: [11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59]. As per Sieve of Eratosthenes Method this list of integers is all prime. Therefore, 59 is a prime number.

I.2.[10 pts.] Compute n = pq and (n) = (p – 1) (q – 1).

Solution:

To calculate the value of n we need to multiply p and q. We have the value of p and q as,

p = 991

and, q = 997

Therefore, n = p \* q

= 991 \* 997

= 988,027

Now, to calculate (n) we need to multiply the value of (p-1) with (q-1). So, let’s first find those values.

(p-1) = 991 – 1 = 990

(q-1) = 997 – 1 = 996

Therefore, (n) = (p – 1) (q – 1)

= 990 \* 996

= 986,040

I.3.[20 pts.] Given a plaintext **M = 506574**, what is the encryption of M, using

C = Mg mod n.

Show in detail how you derive C, which is the ciphertext of the plaintext M.

Solution:

To calculate C, we need to calculate Mg mod n.

We have M as the message which is **506574.**

g has the value of 59 from the question.

And we have calculated the value of n which is 988,027.

Therefore, on substituting the value in the above equation we have **50657459** mod 988,027.