CS 467 - Cyber Security: Course Project

Brendan Teasdale (201704913)

April 2021

1 RSA Cipher

1.1 Problem

The following example of RSA cipher text is presented. Your task is to decrypt it. The public parameters of the systems are $n = 31313$ and $e = 4913$. In order to translate the plaintext back into ordinary English text, you need to know how alphabetic characters are encoded as elements in Zn. Each element of Zn represents three alphabetic characters as in the following examples:

DOG: $3x26^2 + 14x26 + 6 = 2398$
CAT: $2x26^2 + 0x26 + 19 = 1371$
ZZZ: $25x26^2 + 25x26 + 25 = 17575$

6340 8309 14010 8936 27358 25023 16481 25809 23614 7135 24996 30590 27570 26486 30388 9395 27584 14999 4517 12146 29421 26439 1606 17881 25774 7647 23901 7372 25774 18436 12056 13547 7908 8635 2149 1908 22076 7372 8686 1304 4082 11803 5314 107 7359 22470 7372 22827 15698 30317 4685 14696 30388 8671 29956 15705 1417 26905 25809 28347 26277 7897 20240 21519 12437 1108 27106 18743 24144 10685 25234 30155 23005 8267 9917 7994 9694 2149 10042 27705 15930 29748 8635 23645 11738 24591 20240 27212 27486 9741 2149 29329 2149 5501 14015 30155 18154 22319 27705 20321 23254 13624 3249 5443 2149 16975 16087 14600 27705 19386 7325 26277 19554 23614 7553 4734 8091 23973 14015 107 3183 17347 25234 4595 21498 6360 19837 8463 6000 31280 29413 2066 369 23204 8425 7792 25973 4477 30989

You will have to invert this process as the final step in your program.

2 ElGamal Cipher

2.1 Problem

Decrypt the ElGamal ciphertext presented in the following table. The parameters of the system are the prime number $p = 31847$, primitive root $e1 = 5$,

$e2 = 18074$. Each element of Zn represents three alphabetic characters as in the above problem.

ElGamal Ciphertext

(3781, 14409) (31552, 3930) (27214, 15442) (5809, 30274) (5400, 31486) (19936, 721) (27765, 29284) (29820, 7710) (31590, 26470) (3781, 14409) (15898, 30844) (19048, 12914) (16160, 3129) (301, 17252) (24689, 7776) (28856, 15720) (30555, 24611) (20501, 2922) (13659, 5015) (5740, 31233) (1616, 14170) (4294, 2307) (2320, 29174) (3036, 20132) (14130, 22010) (25910, 19663) (19557, 10145) (18899, 27609) (26004, 25056) (5400, 31486) (9526, 3019) (12962, 15189) (29538, 5408) (3149, 7400) (9396, 3058) (27149, 20535) (1777, 8737) (26117, 14251) (7129, 18195) (25302, 10248) (23258, 3468) (26052, 20545) (21958, 5713) (346, 31194) (8836, 25898) (8794, 17358) (1777, 8737) (25038, 12483) (10422, 5552) (1777, 8737) (3780, 16360) (11685, 133) (25115, 10840) (14130, 22010) (16081, 16414) (28580, 20845) (23418, 22058) (24139, 9580) (173, 17075) (2016, 18131) (19886, 22344) (21600, 25505) (27119, 19921) (23312.16906) (21563, 7891) (28250, 21321) (28327, 19237) (15313, 28649) (24271, 8480) (26592, 25457) (9660, 7939) (10267, 20623) (30499, 14423) (5839, 24179) (12846, 6598) (9284, 27858) (24875, 17641) (1777, 8737) (18825, 19671) (31306, 11929) (3576, 4630) (26664, 27572) (27011, 29164) (22763, 8992) (3149, 7400) (8951, 29435) (2059, 3977) (16258, 30341) (21541, 19004) (5865, 29526) (10536, 6941) (1777, 8737) (17561, 11884) (2209, 6107) (10422, 5552) (19371, 21005) (26521, 5803) (14884, 14280) (4328, 8635) (28250, 21321) (28327, 19237) (15313, 28649)