LSA Cryptosystem

Francesco Lucente Stabile
marchesedp@gmail.com
Salem State University

Carey Patrick Atkins
carey.atkins@gmail.com
Salem State University

Arthur James Rosenthal
arosenthal@salemstate.edu
Salem State University

1 Introduction

The LSA cryptosystem is an asymmetric encryption algorithm which is based on both group and number theory that follows Kerckhoffs's principle, and relies on Gauss's Generalization of Wilson's Theorem. Unlike prime factorization based algorithms, the eavesdropping cryptanalyst has no indication that he has successfully decrypted the ciphertext. For this reason, we aim to show that LSA is not only more secure than existing asymmetric algorithms, but has the potential to be significantly computationally faster.

2 Preliminaries

2.1 Groups

Any readers with prior knowledge of group theory (abstract algebra) may skip this section and start directly from section 2.2.

Since the LSA is operated from within mathematical groups, we will briefly explain the nature of a group and the properties used in this algorithm: A group is a set equipped with a binary operation. More specifically, it is a set of elements for which, when the elements are operated on with a specific binary operation (in our case modular multiplication) the following properties hold:

- *Closure:* If two elements are operated upon, the resulting element is an element of the group.

- *Transitivity:* If $*$ is a binary operation and a, b, and c are elements of the group, then $a * (b * c) = (a * b) * c$.

- *Identity:* All groups have a unique identity element e such that, for all elements a of the group, $a * e = a$.

- *Inverse:* Every element a of the group has a unique inverse. The inverse is an element, a^{-1}, of the group such that $a * a^{-1} = e$, where e is the aforementioned identity of the group.

The main group that is used for LSA is the *multiplicative group modulo n*. This is the set of all the integers coprime to, and less than, an integer n, equipped with modular multiplication. By convention, this group can be referred to symbolically as $U(n)$. For example, for $n = 12$ we have that $U(12) =< 1, 5, 7, 11 >$ is a group if operated with multiplication modulo 12.

2.2 Theorem

A reader with prior knowledge of Gauss's Generalization of Wilson's Theorem can skip to section 2.3.

The core of the algorithm is based on a mathematical theorem called Gauss's generalization of Wilson's Theorem.

The theorem states that, if $U(n)$ is a group of all the integers relatively prime to n and less then n, equipped with multiplication modulo n we have that:

$$\prod_{i=1}^{\phi(n)} a_i = \begin{cases} 0 & n = 1 \\ -1 & n = 4, p^t, 2p^2 \\ 1 & \text{otherwise} \end{cases}$$

where p is a prime number, t is a positive integer and the a_i's are elements of the group $U(n)$, with $1 \leq i \leq \phi(n)$. Also recall that $\phi(n)$ is the Euler's Tuotient Function which represent the number of integers coprime with an integer n and less than n

In other words, if $n = p^t$ or $2p^t$ we have that in $U(n) =< a_1, a_2, a_3, ..., a_{\phi(n)} >$ it's always true that

$$a_1 \cdot a_2 \cdot a_3 \cdots a_{\phi(n)} \equiv -1 \mod n.$$

For the explanation of the procedure of the LSA we will use only the case where $n = p^t, 2p^t$. However the reader will easily understand how to use the algorithm in case $n \neq p^t, 2p^t$

3 Key Exchange

A connection through a key exchange is necessary in order to perform the LSA. We will not suggest any algorithm, if we name any, it is just to ensure the cleaner explanation.

Also, we now anticipate that when we refer to a key "k", the length of such integer is between 5 and 10 digit, which will ensure maximum security. Hence, if the algorithm starts by a connection through a Diffie-Hellman algorithm for example, the number k is not intended be the whole number generated by the algorithm, but only a choice of digits of it, between 5 and 10.

4 THE LSA

Suppose two parties want to secretly exchange information. This information should be considered symbolic by nature (e.g. numerically, alphabetically, etc.). It is customary in the field of cryptography, to assign names to the sender, receiver, and potential eavesdropper, as such we will we choose Alice, Bob and Eve respectively. They perform the following steps:

1. Alice and Bob begin by sharing a secret number k that is only known to Alice and Bob.

2. Next, k will be used as a reference by both parties to find the smallest positive integer n that satisfies the following properties:

   I) $k < n$.
   II) $n = p^t$ or $n = 2 \cdot p^t$ where p is an odd prime number and t a positive integer.

   Note: The key exchange algorithms might generate massive numbers as keys. In that case, the k should be a derivation of a larger key K. It is very important to know that the length of k is efficient as long as $U(n)$ contains enough elements as there are symbols to share. For a merely alphabetical and digital messages 34 elements are enough. This means that a k of 4 digits is long enough to ensure security. It is not the scope of this paper to discuss the derivation of k from K and how long k must be; this will pertain the security that the user wants to provide. However, as an example, if the Diffie-Hellman algorithm generates a massive number K, then let k be the first 4 digits of K. Then derive n from k

3. Assuming that the above conditions have been met, then in $U(n)$ by Gauss's Generalization of Wilson's Theorem we have that

$$a_1 \cdot a_2 \cdot a_3 \cdots a_{\phi(n)} \equiv -1 \mod n.$$

   At this point, Alice and Bob independently list the elements of $U(n)$ in ascending order as $U(n) =< \epsilon_1, \epsilon_2, \epsilon_3, ..., \epsilon_h, ..., \epsilon_{\phi(n)} >$ where $\epsilon_i < \epsilon_j$ when $i < j$. Note that, since k is only known to Alice and Bob, and $U(n)$ is chosen from the shared knowledge of k, then it must be the case that $U(n)$ is only known to Alice and Bob.

4. Alice chooses an element of the group to represent the plain text of her message, call it ϵ_h.

5. To encrypt, Alice multiplies each of the elements of the group up to ϵ_h in the following way: $\epsilon_1 \cdot \epsilon_2 \cdots \epsilon_h \mod n \equiv c$ where c is a component of the ciphertext.

6. Alice publicly sends c to Bob.

7. Bob receives c and multiplies c with the other elements of the group in descending order and checks if $c \cdot \epsilon_{\phi(n)} \equiv -1 \mod n$, $c \cdot \epsilon_{\phi(n)} \cdot \epsilon_{\phi(n)-1} \equiv -1 \mod n$, all the way to $c \cdot \epsilon_{\phi(n)} \cdot \epsilon_{\phi(n)-1} \cdots \epsilon_{h+1}$ which will necessarily be congruent to -1 modulo n by Gauss's Generalization of Wilson's Theorem, since all the elements of the group have been multiplied (and because n in the desired form). At this point Bob knows that the next element of the group yet to be multiplied, ϵ_h, is indeed the plaintext.

   † Since $n - 1$ is an element of the group and it is indeed the element congruent to -1 modulo n, then the multiplication of the elements of the group might generate $n - 1$ even in some cases where not all the elements of $U(n)$ have been multiplied, unpredictably.
   Thus, before Alice sends the ciphertext c she preforms $c \cdot \epsilon_{\phi(n)} \mod n$, $c \cdot \epsilon_{\phi(n)} \cdot \epsilon_{\phi(n)-1} \mod n$, all the way to $c \cdot \epsilon_{\phi(n)} \cdot \epsilon_{\phi(n)-1} \cdots \epsilon_{h+1} \mod n$ and records the number of additional times she generates elements congruent to -1 modulo n, and calls this number Σ. Then she publicly sends the tuple $C = (c, \Sigma)$, which becomes the ciphertext.

   †† When Bob receives $C = (c, \Sigma)$ he will start multiplying the elements in descending order until he finds $\Sigma + 1$ elements congruent to -1 modulo n, revealing the plaintext.

8. Alice will send another symbol of the plaintext by running the LSA algorithm from the very beginning, including the sharing of the integer k.

4.1 Example

Here is an example of the LSA operated within the group $U(n)$ equipped with multiplication modulo n.

For enhanced readability, we have chosen a group of small order, thus making each step more easily visualized.

Consider the case where Alice wants to secretly share the plaintext '7' with Bob:

1. The key exchange algorithm generates $k = 53$.
2. Alice and Bob independently follow the LSA algorithm and conclude that the next useful integer is 54 because it satisfies the following properties:

   I) $53 < 54$
   II) $54 = 2 \cdot 3^3$.
3. Alice and Bob list the elements of the group in ascending order.
   $U(54) =< 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53 >$.
4. Since Alice wishes to send '7', she picks the 7th element of $U(54)$ in ascending order, which is 19.
5. Alice performs $1 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 1,616,615 \mod 54 \equiv 17 = c$.

† Alice multiplies c by each element in descending order to find the value of Σ in the following way:

$$
\begin{aligned}
17 \cdot 53 = 901 &\mod 54 \equiv 37 \\
37 \cdot 49 = 1,813 &\mod 54 \equiv 31 \\
31 \cdot 47 = 1,457 &\mod 54 \equiv -1 \rightarrow \text{(First } \Sigma) \\
53 \cdot 43 = 2,279 &\mod 54 \equiv 11 \\
11 \cdot 41 = 451 &\mod 54 \equiv 19 \\
19 \cdot 37 = 703 &\mod 54 \equiv 1 \\
1 \cdot 35 = 35 &\mod 54 \equiv 35 \\
35 \cdot 31 = 1,085 &\mod 54 \equiv 5 \\
5 \cdot 29 = 145 &\mod 54 \equiv 37 \\
37 \cdot 25 = 925 &\mod 54 \equiv 7
\end{aligned}
$$

Since $c = 17$ and $\Sigma = 1$ (because Alice generated only one additional element congruent to $-1 \mod n$), then Stella publicly sends $C = (17, 1)$ to Bob.

6. †† Bob receives C and starts to multiply c by the elements of the group in descending order until he finds $\Sigma + 1$ (in this case $1 + 1$) elements congruent to -1 modulo 54 as follows:

$$\begin{aligned}
17 \cdot 53 &= 901 \mod 54 \equiv 37 \\
37 \cdot 49 &= 1,813 \mod 54 \equiv 31 \\
31 \cdot 47 &= 1,457 \mod 54 \equiv -1 \rightarrow (\text{First } \Sigma) \\
53 \cdot 43 &= 2,279 \mod 54 \equiv 11 \\
11 \cdot 41 &= 451 \mod 54 \equiv 19 \\
19 \cdot 37 &= 703 \mod 54 \equiv 1 \\
1 \cdot 35 &= 35 \mod 54 \equiv 35 \\
35 \cdot 31 &= 1,085 \mod 54 \equiv 5 \\
5 \cdot 29 &= 145 \mod 54 \equiv 37 \\
37 \cdot 25 &= 925 \mod 54 \equiv 7 \\
7 \cdot 23 &= 161 \mod 54 \equiv -1 \rightarrow (\Sigma + 1)
\end{aligned}$$

Since Bob found the second element that is congruent to -1 modulo 54, he knows that all of the elements of the group have been multiplied. This tells him that the next number in the sequence is the chosen number (19). Since 19 is the 7th group element, Bob has the plaintext '7'.

5 Extra Security

Note, if p is a prime number, in $U(p)$, the product of all the integers in ascending order is an integer factorial, so recognizable. However, we can still use $U(p)$ groups just by starting the encryption by listing the elements of the group in descending order and use the normal procedure with the elements in backward order. So $c = \epsilon_{\phi(p)} \cdot \epsilon_{\phi(p-1)} \cdot \epsilon_{\phi(p-2)} \cdots \epsilon_h \cdot$, where ϵ_h represent the plaintext.

Note that, for the cyphertext $C = (c, \Sigma)$, the element c is obviously an element of the group $U(n)$. Hence, more likely $c \pm 1$ is not. By previous agreement, Alice can send $C = (c + 1, \Sigma)$ or $C = (c - 1, \Sigma)$ to Bob anytime $c + 1$ or $c - 1$ are **not** in the group (as long as they previously agree on addition or subtraction). In this way, Bob will notice that the element sent by Alice is not listed in his group; In that case, Bob will consider the cyphertext $C = (c, \Sigma)$ after have subtracted (or added) 1 from $c+1$ $(c-1)$.

Alice might send $(c + n, \Sigma)$, or $(c + n \pm 1, \Sigma)$, or $(c \cdot n, \Sigma)$.

Alice might send a fake integer d in $C = (d, \Sigma)$ as fake every once in a while after a certain signal. For example, if the previous element sent was a power of 2, then send $C = (d, \Sigma)$

6 The choice of the elements

In this section we will show one way to map a given group $U(n)$ to a set of meaningful symbols $\mathcal{P}$ that one might wish to encrypt. We will accomplish this via a surjective function $\psi : \mathcal{P} \mapsto U(n)$. The function ψ must be surjective for each member of the codomain to have a corresponding element in the domain $\mathcal{P}$ that maps into it. This is required in order to make sure that each plaintext character is paired with a member of the group.

Example: Assume $\mathcal{P}$ is the set of symbols $\{e, f, g\}$. Then, in $U(9)$, ψ maps the elements as follows:

$$\begin{aligned} 1 &\rightarrow e \\ 2 &\rightarrow f \\ 4 &\rightarrow g \\ 5 &\rightarrow e \\ 7 &\rightarrow f \\ 8 &\rightarrow g \end{aligned}$$

Consider the case where Stella is operating with multiplication modulo 9, and she wants to send the symbol f. She can send this with either $1 \cdot 2 \mod 9 \equiv 2$, or $1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \mod 9 \equiv 1$. So she can send f as either $c = 1$ or $c = 2$ as the first component of C.

7 One-Time-Pad

The LSA can be use as a One-Time-Pad when every symbol of the plaintext is sent through disjoint tuples, which is possible only by performing the algorithm from the very beginning for each symbol. This requires that Alice and Bob are equipped with as many integers k's as there are symbols in the plaintext to share. Since running key exchange algorithms, which generate massive numbers, for each character of a message, is not a feasible task, we we show in this section how to generate a large number of secret k's integers that will be used to start the LSA.

Assume that only one secret integer k is known by Alice and Bob. Also assume that with that k they start the LSA algorithm (see section 4). From k they derive n. Alice sends an element of the group $U(n)$ via the LSA. When Alice and Bob both agree on the element ϵ_h, they both perform the canonical multiplication of all the elements of the group up to ϵ_h:

$$\epsilon_1 \cdot \epsilon_2 \cdot \epsilon_3 \cdots \epsilon_h = M.$$

We will see in the example that for some wisely chosen n and ϵ_h, the integer M is large.

At this point Alice and Bob agree on a way to "cut the number in pieces" to generate many k's.

7.1 Computational example

Assume Stella and Ben needs keys of lengths 4, 5 and 6. Then they will proceed as follow.

Assume the initial key exchange generated the integer 10000, then Stella and Ben List the elements of the cyclic group U(10082), which are 4970. Assume Stella chooses the 500th element of the ordered list. Ben runs the LSA and find the element. Then both multiply the first 500 elements together to generate M_1 and the next 4470 elements to generate M_2. Then they combine M_1 and M_2 and obtain

$M =$ 8 606 842 941 648 980 141 500 390 929 340 333 380 821 688 776 450 913 725 462 959 925 286 301 344 474 920 318 994 753 701 941 060 148 881 573 427 303 951 969 468 229 706 390 675 879 189 573 397 083 298 234 232 002 057 590 825 541 929 196 617 798 357 864 253 415 244 900 822 598 565 148 459 722 700 786 910 964 414 143 234 585 951 686 501 951 456 012 929 058 272 386 770 627 526 673 039 661 180 847 924 218 842 419 368 978 282 454 440 860 900 662 216 576 405 681 454 036 569 302 145 779 655 295 161 024 870 390 029 412 887 939 760 085 690 088 522 580 668 382 601 362 698 591 183 043 906 726 589 771 426 474 327 106 027 446 630 110 424 304 124 378 118 465 405 405 743 664 124 241 120 045 296 239 389 519 468 482 351 202 104 266 957 141 300 679 419 724 335 696 429 700 298 358 638 780 913 615 738 551 744 801 623 131 105 809 471 972 048 150 306 016 295 179 131 035 357 607 223 358 211 005 134 001 883 185 282 488 946 730 500 335 843 269 291 572 586 763 218 825 995 118 857 751 797 398 654 362 527 314 550 465 079 665 086 098 550 853 743 078 745 496 295 016 434 317 612 040 149 655 374 590 841 804 951 466 880 939 961 763 331 490 516 798 658 974 158 057 235 405 502 012 651 675 705 822 721 872 793 215 886 863 022 494 497 302 905 269 956 369 501 159 699 301 180 259 593 349 473 092 183 890

787 780 887 632 929 839 765 511 235 882 266 179 958 154 203 122 544 605
179 768 158 608 370 817 282 915 952 185 488 554 644 390 135 357 993 690
852 190 024 244 441 738 294 724 287 641 573 669 555 968 114 187 428 665
154 287 632 270 613 961 761 228 993 702 172 924 772 283 988 998 374 585
865 730 817 997 320 743 936 406 471 246 649 716 792 358 558 193 101 688
946 873 570 936 618 724 758 204 734 825 994 819 402 694 702 148 437 517
737 689 793 828 514 076 333 122 985 661 430 846 549 596 390 499 041 786
339 192 302 131 572 974 709 297 832 862 110 998 333 744 430 381 166 027
020 236 227 585 570 232 479 531 400 255 215 550 507 793 223 898 616 672
794 387 690 471 541 431 266 631 470 390 924 925 575 080 289 248 572 898
235 540 859 312 582 166 875 527 981 626 703 318 739 803 823 893 869 362
484 894 030 410 653 426 396 140 550 879 075 990 698 831 473 494 647 467
624 071 140 136 070 643 116 364 768 380 235 343 079 887 793 122 682 371
905 764 133 440 974 286 080 554 480 899 049 799 670 035 906 176 288 997
038 034 506 850 282 266 882 379 887 855 145 511 741 817 836 431 793 704
705 538 342 175 539 902 335 022 288 715 454 515 292 921 299 001 450 517
534 804 617 078 059 846 221 953 354 447 346 763 988 810 534 280 535 248
536 141 276 561 197 190 704 889 259 179 509 470 179 929 293 168 306 161
293 551 050 524 730 271 045 098 238 263 274 749 677 657 927 260 730 770
951 419 554 581 076 712 888 127 449 040 228 824 829 271 839 330 285 440
543 057 698 945 980 776 824 086 669 307 423 350 981 165 928 677 510 869
269 231 234 257 505 975 778 193 708 305 434 043 901 594 995 627 485 298
570 161 135 000 472 851 522 386 865 671 670 709 777 818 038 581 352 190
552 307 549 640 904 152 778 929 896 602 199 247 914 384 282 557 034 679
198 435 875 815 015 940 633 828 056 717 610 285 588 851 682 315 342 052
873 729 864 699 776 259 502 087 094 284 484 425 788 628 085 618 911 022
349 536 212 187 262 301 923 859 493 531 187 999 312 856 457 266 758 378
830 271 896 199 828 304 607 049 708 767 178 213 942 117 427 912 961 954
795 876 493 249 900 845 725 960 730 435 337 264 557 072 733 841 601 859
140 757 721 717 387 720 980 721 572 318 546 117 294 697 226 731 357 012
693 921 267 934 601 387 802 704 272 313 047 875 914 620 319 374 143 570
161 689 301 211 035 738 285 648 343 768 191 023 038 934 802 060 100 529
224 998 554 167 930 935 879 676 265 470 227 492 612 347 144 302 355 176
787 618 317 392 434 077 021 130 251 773 572 750 188 964 083 583 557 916
434 630 637 912 014 242 000 284 162 052 170 984 426 050 938 749 536 471
191 311 147 901 081 800 452 549 613 340 070 146 491 054 000 177 696 377
039 636 916 707 683 228 055 317 823 288 252 603 727 945 166 073 371 049
154 671 718 139 268 076 919 586 633 749 279 866 786 550 639 594 094 754
339 139 644 263 239 634 536 977 232 413 464 958 392 122 157 180 052 563
057 150 359 904 568 975 367 449 228 051 948 443 123 946 591 821 960 198
652 462 804 767 069 823 783 671 840 728 124 326 604 621 696 600 185 997
914 898 130 768 239 242 126 413 620 626 383 598 884 108 686 242 258 767
253 666 459 174 445 930 760 227 096 272 379 987 358 262 877 826 819 014

718 821 742 496 850 903 317 261 248 257 138 750 303 501 907 023 733 928
664 616 412 535 249 150 249 742 451 990 510 835 076 802 212 560 174 190
756 967 236 710 715 765 537 174 766 336 355 842 324 628 592 408 122 421
089 250 578 530 837 024 797 136 458 125 779 806 449 492 813 239 926 003
070 187 308 752 552 453 587 607 743 592 184 872 100 038 830 633 177 997
864 246 226 017 657 452 816 957 167 591 196 937 330 361 726 635 318 049
498 301 581 490 280 038 051 517 855 884 394 230 668 156 458 072 790 008
391 139 491 422 249 475 745 374 345 765 091 793 632 499 633 529 332 942
273 332 019 609 017 342 482 067 954 903 499 180 454 652 953 789 732 677
673 205 382 306 034 823 675 389 021 875 547 273 480 561 087 493 303 409
862 385 681 021 786 786 155 492 502 278 027 351 292 560 782 105 815 909
935 886 172 244 032 279 383 464 076 704 448 246 974 239 460 591 665 003
528 538 839 723 998 342 246 959 089 216 089 772 300 240 476 369 085 979
872 458 847 963 945 722 303 407 465 802 979 393 534 587 965 563 643 815
361 749 709 412 091 550 034 814 528 224 914 907 084 395 479 607 639 436
722 296 723 361 874 828 685 858 814 393 069 520 946 568 797 046 822 072
173 614 106 461 936 060 769 930 706 603 745 535 657 667 655 320 168 789
395 773 373 111 030 012 403 839 498 996 183 365 013 397 987 779 025 251
165 484 192 901 680 897 634 953 832 041 983 862 509 551 574 768 643 229
128 025 016 468 651 086 506 599 640 583 523 215 665 250 522 185 835 617
152 317 544 300 288 494 928 833 470 763 325 813 686 969 824 806 623 928
072 530 625 824 206 951 131 930 177 182 683 268 950 206 095 126 702 857
583 326 450 283 203 169 403 860 660 681 176 648 251 577 952 048 962 507
778 578 000 660 082 188 646 580 003 363 178 716 677 646 564 084 970 965
508 347 590 427 183 901 253 672 528 187 841 300 890 531 896 226 558 652
076 442 203 782 291 781 832 818 047 446 602 973 815 167 285 662 945 436
568 320 419 108 571 458 462 789 598 565 851 726 624 576 491 728 995 809
680 926 328 999 029 419 820 910 305 066 359 926 465 231 519 938 208 299
437 147 942 798 861 211 643 610 324 894 878 545 644 990 270 642 244 494
163 879 607 296 898 928 608 214 329 031 013 442 520 705 694 602 975 910
862 339 097 968 516 700 217 190 835 579 783 209 730 771 965 933 299 802
767 173 047 356 432 265 737 421 374 201 679 939 916 447 093 503 319 410
614 048 452 113 106 774 047 266 853 994 715 926 071 444 815 805 630 728
159 738 464 089 536 583 297 762 606 302 967 235 469 223 483 125 398 692
721 666 057 661 176 081 334 211 304 785 339 978 257 960 687 668 862 823
075 700 928 223 018 056 240 006 078 890 106 292 034 871 451 467 219 760
677 785 763 506 617 763 363 852 272 014 153 977 857 513 848 730 417 570
315 752 349 198 258 348 538 314 886 550 011 035 525 313 685 817 282 538
840 037 417 533 862 999 288 370 969 732 846 369 973 691 661 672 284 103
013 676 085 791 089 890 889 506 523 762 923 258 496 281 909 970 809 918
400 788 866 651 529 269 568 609 468 765 756 146 931 005 209 085 560 622
831 045 433 491 207 145 724 078 988 900 503 102 719 846 990 141 052 083
789 861 703 162 342 182 987 276 489 610 345 447 689 093 849 703 737 124

731 925 954 083 389 435 023 672 938 220 648 487 095 506 081 192 062 333
501 693 862 280 003 387 122 341 330 752 940 491 925 176 539 994 279 710
999 957 982 776 404 307 634 035 377 423 424 329 776 762 605 959 549 344
699 096 429 714 399 197 245 631 017 049 782 521 634 787 948 767 131 267
481 473 760 060 648 873 174 177 589 780 839 253 852 748 862 437 382 168
985 359 945 328 081 739 936 320 859 351 257 085 970 854 985 833 375 780
480 233 671 837 312 269 750 681 105 540 775 021 940 566 288 676 256 051
776 979 251 181 501 401 821 202 510 969 840 925 656 930 121 984 173 021
548 544 860 704 210 964 964 111 518 532 453 133 785 236 209 622 026 690
350 799 120 438 379 573 604 585 562 297 850 554 997 039 561 397 413 791
736 521 705 745 609 806 563 014 558 774 863 065 093 131 937 986 110 030
690 694 128 316 266 633 001 557 694 249 929 517 833 719 097 933 691 523
807 124 754 430 806 843 764 648 536 974 180 999 770 274 533 512 255 931
151 605 222 557 639 767 517 137 804 556 522 479 561 451 946 869 850 330
340 504 181 657 999 088 939 196 886 647 942 790 284 443 960 611 959 936
857 010 984 296 198 231 831 435 857 796 073 428 796 209 245 775 992 548
106 998 336 432 150 170 561 357 417 993 833 769 388 627 129 375 639 793
135 915 460 924 322 578 536 674 083 533 782 440 173 369 170 909 867 855
668 338 664 191 230 770 940 009 195 432 886 791 306 303 229 974 149 287
930 785 237 200 876 360 000 715 244 356 361 868 386 575 589 530 547 997
556 903 649 323 311 601 290 252 997 660 825 799 231 519 843 398 684 486
874 185 116 147 645 922 993 804 853 321 478 218 743 953 934 469 383 287
449 755 567 338 206 017 582 490 348 550 327 038 854 565 200 661 105 534
285 657 320 777 812 901 954 127 831 189 950 501 907 367 672 723 916 895
790 052 560 843 807 226 072 217 724 361 524 767 970 150 256 777 547 927
603 561 193 442 336 976 965 832 086 786 622 185 710 286 308 060 450 648
194 582 054 688 746 515 939 755 707 362 222 462 211 414 742 377 500 145
864 453 891 238 847 344 358 351 359 081 922 215 845 520 198 056 029 302
108 301 051 733 795 250 211 204 724 229 092 081 604 643 762 966 700 595
991 061 794 202 447 442 049 442 206 590 768 689 816 166 394 682 961 610
244 700 022 583 621 340 689 823 273 672 337 541 430 287 756 160 894 154
664 146 694 899 094 631 859 055 858 126 543 879 161 832 263 532 679 042
603 693 112 919 918 490 407 836 366 584 851 577 112 699 564 562 129 778
240 171 023 327 014 974 546 574 608 526 191 648 557 492 445 054 761 304
563 966 705 186 905 820 267 783 792 380 292 280 223 058 944 472 603 025
376 169 249 025 550 645 960 627 302 456 343 113 882 279 646 822 010 651
142 996 641 309 746 712 809 263 859 943 175 223 521 732 907 520 336 508
725 163 827 358 034 504 182 596 942 271 811 475 721 483 624 343 915 030
675 128 919 431 428 515 407 520 885 685 791 565 961 172 224 565 905 918
825 083 988 902 188 992 452 664 260 298 762 279 484 998 048 579 013 956
363 735 869 247 862 017 386 223 771 486 506 858 995 989 241 225 871 838
585 257 024 660 773 655 429 722 909 662 952 310 926 997 802 867 535 553
483 915 638 014 762 968 910 361 765 787 126 116 407 406 151 527 841 699

107 953 156 052 866 223 266 950 264 342 106 678 160 291 192 656 982 941
686 270 374 244 965 454 618 354 940 717 424 608 604 605 152 853 610 509
926 207 244 166 942 266 796 821 940 640 729 463 927 559 823 489 838 675
611 132 769 082 329 264 864 581 629 436 214 312 912 104 748 217 974 451
605 844 417 665 468 890 833 837 639 731 218 992 002 734 692 642 575 019
348 234 933 589 658 995 427 330 461 460 604 501 283 319 848 220 333 113
996 230 503 597 159 515 035 533 314 383 009 315 304 071 794 174 919 676
879 844 662 334 740 009 410 300 806 404 361 600 353 385 207 241 325 319
626 763 092 266 501 352 451 215 906 426 019 602 746 107 240 771 546 567
413 954 630 527 466 731 110 873 993 320 063 254 331 268 691 305 137 560
391 494 019 604 750 823 883 323 447 148 594 250 993 441 798 968 727 933
563 463 777 538 738 272 288 990 247 591 539 793 942 694 045 396 017 434
120 847 574 706 086 470 786 466 973 622 544 433 923 051 975 018 038 007
521 375 618 950 841 072 434 980 825 369 771 735 478 253 675 595 277 488
803 650 341 588 292 415 673 100 840 330 550 403 891 708 740 579 718 335
195 153 366 798 311 558 320 380 387 998 628 024 468 783 172 201 581 304
429 716 173 602 738 241 924 798 155 751 871 784 960 328 858 049 760 017
518 789 550 385 654 607 796 157 525 198 265 419 548 774 722 418 140 517
281 254 992 122 935 398 976 875 809 798 056 462 688 477 940 155 569 768
770 556 972 620 216 155 171 185 493 144 397 640 312 978 718 452 326 923
810 346 409 778 132 046 373 921 758 403 880 509 161 192 737 454 656 891
001 661 175 023 272 666 699 305 249 734 097 321 277 768 778 799 107 798
915 661 313 292 360 942 605 309 130 245 770 223 046 346 605 493 789 235
921 054 717 903 337 636 835 239 791 644 075 547 477 933 225 866 423 416
414 402 236 330 435 253 643 407 827 339 100 370 725 594 531 028 635 180
337 992 861 353 054 641 001 627 106 972 860 280 784 664 645 823 029 535
314 125 803 555 965 753 947 343 413 845 742 957 636 320 382 445 269 565
530 965 417 005 472 179 434 416 396 942 613 999 761 087 058 947 856 619
368 606 695 160 260 612 376 108 781 530 284 928 787 345 246 583 194 868
895 553 974 310 990 326 946 394 623 848 877 178 894 301 893 240 260 964
841 630 526 257 381 386 203 776 579 426 831 137 337 498 621 980 376 957
216 930 133 729 765 142 758 624 418 770 014 011 316 986 571 997 900 281
720 661 836 525 433 868 607 411 712 253 495 124 969 077 958 965 068 311
514 745 533 377 656 183 808 511 130 432 927 452 551 993 856 130 041 968
964 422 698 688 952 646 361 005 015 720 312 144 127 810 618 625 203 972
531 858 243 594 322 271 493 244 958 776 795 957 170 713 498 696 824 149
484 074 884 679 390 831 224 572 453 965 087 933 341 859 278 366 216 154
549 682 144 051 775 856 715 199 069 610 399 774 342 604 214 379 331 153
277 519 744 650 229 228 310 850 825 623 866 063 287 314 384 400 506 962
366 667 395 058 277 758 954 827 216 188 164 873 143 976 092 695 054 352
165 570 230 836 280 482 439 273 990 896 906 982 068 861 643 352 802 346
099 174 693 698 275 226 134 799 184 370 304 578 290 829 616 752 962 544
142 853 322 628 873 587 389 638 938 311 922 285 647 018 059 555 239 728

645 390 845 537 684 004 954 607 945 508 802 568 310 808 329 200 753 756
176 906 920 759 478 225 708 163 367 000 364 250 292 172 401 793 427 552
950 547 762 706 079 340 680 817 608 806 260 724 391 570 677 005 954 829
644 602 453 202 940 461 672 746 919 205 082 232 490 190 951 414 930 183
724 186 584 626 862 617 079 139 345 503 809 131 840 576 664 119 192 341
553 347 698 606 182 209 918 432 804 983 052 258 262 722 900 846 720 561
448 599 940 293 227 926 212 780 089 454 163 317 132 082 227 384 987 205
752 755 606 942 865 218 379 341 963 678 704 144 653 328 265 625 368 240
074 137 405 064 935 454 686 785 130 932 705 880 269 104 455 256 716 945
597 995 837 122 198 937 106 342 127 771 388 441 911 289 883 282 036 810
371 900 496 247 894 883 671 516 978 791 864 895 459 921 028 711 661 761
467 629 527 977 545 375 697 057 824 172 654 164 165 711 855 239 786 334
519 797 893 997 340 318 882 462 940 318 968 030 995 408 681 783 138 866
679 558 562 110 071 477 356 775 876 448 539 452 581 216 303 968 390 055
272 353 772 533 865 144 909 270 106 574 226 104 683 985 992 127 684 385
344 472 044 987 476 915 687 178 616 321 904 975 941 299 786 340 195 422
133 153 010 331 912 880 091 473 718 061 359 143 906 761 618 929 875 298
550 866 800 736 240 926 783 618 275 434 686 162 217 292 335 591 942 625
005 984 915 405 807 202 327 386 326 539 840 447 901 245 612 693 201 907
470 127 033 848 551 860 460 176 036 124 757 897 641 997 013 721 668 448
808 002 029 184 861 198 987 538 682 848 292 940 882 553 875 077 469 292
030 598 293 457 187 486 368 469 724 846 453 098 956 513 243 620 461 305
672 196 124 073 878 236 627 965 614 754 289 026 072 437 051 922 410 379
593 900 808 337 838 202 258 715 741 623 658 846 349 735 139 413 416 991
450 603 839 182 184 116 574 111 969 365 095 173 258 865 926 035 002 282
259 593 635 946 205 548 027 434 677 530 960 384 104 720 948 658 997 766
669 177 633 863 148 046 742 850 097 679 116 851 680 389 157 373 621 682
698 132 243 527 204 931 267 766 883 239 717 554 040 390 235 231 844 787
056 712 886 104 685 209 202 874 973 653 282 719 351 699 781 820 743 455
636 775 258 402 395 562 654 321 674 114 772 751 168 204 204 383 669 082
119 092 317 018 084 267 385 243 149 177 509 731 989 011 888 594 801 706
293 522 948 069 571 022 037 775 867 546 186 990 421 213 140 263 982 858
606 875 866 440 527 443 147 648 147 070 120 102 856 325 849 718 294 448
621 433 783 107 233 032 395 177 152 559 393 395 508 496 013 461 695 355
452 543 516 076 603 799 142 731 081 345 270 180 185 220 157 064 325 299
534 622 440 627 000 426 091 065 927 626 913 987 798 082 842 534 361 404
498 167 334 166 872 025 002 755 749 024 925 177 574 351 758 276 207 994
446 652 101 165 690 897 014 546 161 407 722 057 049 485 896 834 880 907
770 361 683 266 004 729 203 071 650 897 985 011 904 484 719 798 989 154
592 666 565 765 945 814 158 062 125 219 864 782 517 856 042 986 814 586
478 740 536 604 329 006 617 671 301 668 788 105 804 185 575 243 268 400
606 618 079 271 685 130 028 175 275 636 432 473 891 039 472 167 063 203
789 243 986 684 375 387 453 927 616 937 034 364 351 039 107 293 394 861

862 662 595 546 761 057 930 722 792 744 267 131 494 427 522 845 128 013
036 657 624 946 452 782 985 405 983 062 113 886 675 029 244 632 235 606
690 519 069 311 964 368 935 272 074 821 653 875 069 270 722 337 523 919
065 435 141 083 520 183 491 728 014 192 112 248 245 261 341 239 535 341
851 286 536 572 330 625 540 501 792 071 879 915 063 570 059 084 336 016
595 934 269 853 673 426 569 990 565 034 116 343 043 882 470 520 370 168
608 626 687 769 380 935 281 094 089 170 718 318 932 955 081 064 751 241
411 502 056 712 039 202 656 663 204 129 544 525 803 665 627 327 595 812
331 836 270 930 240 768 744 573 573 453 029 811 501 259 108 517 706 435
171 452 511 391 127 233 141 524 795 079 363 902 199 492 296 955 075 934
380 912 375 723 410 327 521 381 718 150 366 780 711 756 875 866 000 841
417 906 567 107 658 484 561 838 583 140 604 836 658 827 370 620 342 762
853 737 600 455 078 700 232 523 680 679 119 265 510 746 238 925 184 496
268 174 035 678 351 680 594 358 089 078 902 872 683 834 637 243 993 780
088 764 162 217 410 619 742 750 357 616 307 169 640 787 779 589 280 596
308 080 309 683 005 991 461 801 862 400 207 982 436 287 427 145 754 166
584 387 761 880 964 895 236 983 111 218 367 141 945 069 008 607 692 019
929 016 435 453 805 253 567 233 202 896 373 379 902 523 326 055 802 807
962 730 413 244 518 579 419 465 989 526 223 546 343 165 766 180 733 855
532 047 971 458 812 932 460 158 284 986 815 299 201 695 780 453 148 914
945 983 614 921 320 401 669 244 672 540 366 801 580 300 263 584 826 947
442 371 007 451 583 127 765 844 100 491 212 294 681 140 748 031 584 816
250 826 874 122 734 130 491 322 306 672 940 241 168 513 054 719 933 273
691 618 014 463 398 260 020 316 489 949 416 932 771 892 343 522 158 282
147 111 844 239 479 987 933 549 914 256 860 182 831 592 176 144 701 431
391 935 374 448 784 512 733 579 909 853 566 309 118 853 148 833 198 202
458 827 658 831 718 283 275 579 535 355 222 227 543 172 435 913 801 211
789 917 947 696 287 476 759 459 329 511 000 661 850 612 488 531 099 005
834 471 822 691 720 755 654 281 519 926 000 059 186 489 465 803 170 227
988 118 986 098 623 278 298 080 241 984 778 131 483 894 028 759 168 473
532 872 268 421 456 967 682 357 423 654 359 454 538 890 294 473 270 991
447 518 306 202 852 267 977 103 520 105 300 249 646 199 089 204 990 772
179 195 719 856 538 877 128 175 100 232 179 384 704 089 340 108 640 164
282 517 830 453 311 712 600 070 623 906 175 169 342 932 040 173 137 105
048 445 214 447 178 249 012 362 136 601 893 785 252 480 477 233 892 728
634 017 873 977 222 864 878 044 172 505 999 071 642 016 720 749 726 539
661 876 626 784 802 877 757 224 578 337 922 394 814 477 645 651 708 412
522 728 368 732 328 313 471 249 917 757 312 749 874 932 032 327 748 809
956 931 659 432 748 966 122 292 736 633 487 332 487 986 892 826 135 082
833 850 494 221 682 942 905 767 113 657 819 500 733 829 153 621 717 050
578 939 059 481 295 314 507 612 176 011 501 082 360 618 595 313 336 995
746 277 928 399 315 951 765 699 923 842 832 857 319 308 813 365 094 330
219 015 197 991 242 735 504 249 580 443 998 243 630 256 065 202 200 933

907 003 403 375 548 365 751 171 530 812 754 109 093 520 175 245 337 314
748 078 875 272 807 596 956 616 856 081 043 771 023 366 911 431 882 354
610 904 409 965 302 853 123 148 884 785 260 632 069 998 751 669 100 412
236 632 604 605 874 364 267 781 638 573 073 917 125 650 760 022 632 977
718 248 702 434 562 446 124 874 236 734 365 680 015 461 439 306 818 233
259 052 479 426 540 423 766 840 072 412 716 998 446 755 873 493 853 504
854 200 411 001 835 817 315 186 866 147 451 024 072 129 197 060 785 550
917 569 830 829 970 023 123 455 626 984 345 575 032 001 371 539 561 915
924 856 996 083 853 695 312 290 523 261 244 214 024 693 836 624 232 286
025 044 984 335 404 357 405 020 208 034 125 870 972 048 972 726 991 976
458 851 476 610 801 807 662 641 078 351 151 847 051 196 236 646 853 371
662 513 951 121 690 632 383 422 892 994 682 240 804 667 268 461 305 251
698 574 903 295 400 753 069 806 202 594 989 287 606 040 979 502 581 961
445 679 503 672 111 074 209 697 985 200 711 989 364 886 707 668 236 129
429 841 459 174 865 696 959 445 926 306 250 187 700 088 693 770 640 933
102 276 186 409 677 793 889 885 958 447 769 553 517 275 959 200 546 741
179 425 305 508 107 766 791 343 731 947 608 541 967 310 254 395 379 362
513 820 068 207 049 078 382 534 991 752 587 504 732 118 844 049 635 064
984 493 150 377 357 213 601 675 934 134 884 535 876 688 682 043 776 131
943 341 617 631 222 509 001 073 019 137 423 847 056 598 586 734 489 236
171 855 998 323 178 445 025 165 495 513 026 840 033 826 829 773 131 336
848 614 173 268 731 685 156 171 907 131 766 133 899 460 359 426 877 361
856 401 464 829 912 001 331 621 505 196 263 678 293 996 080 026 563 549
616 629 320 666 564 292 120 490 340 427 815 613 870 541 306 290 652 779
178 532 328 387 983 185 168 962 669 174 303 763 824 960 808 139 399 246
232 802 512 505 224 598 275 316 155 800 730 225 381 040 567 594 092 418
131 191 933 780 595 793 667 880 013 086 919 952 691 801 656 491 200 086
263 420 801 920 595 734 817 944 570 788 905 235 040 799 009 083 307 115
939 270 414 285 375 660 678 899 695 393 356 647 085 675 504 860 888 183
802 965 616 346 393 549 448 266 687 033 344 056 917 308 017 195 721 370
052 118 120 344 726 238 424 795 765 986 119 173 788 901 342 091 679 925
794 035 672 189 514 693 371 780 263 866 054 407 016 929 606 174 263 595
021 286 074 182 556 971 257 048 730 384 462 506 215 017 096 510 425 746
690 630 916 110 610 649 745 139 700 160 570 777 593 955 151 220 241 827
612 408 569 102 067 026 930 336 505 196 060 409 403 669 722 471 642 856
654 806 249 581 930 932 045 319 903 700 257 217 796 755 184 431 899 147
659 731 413 398 216 731 842 613 989 043 051 963 893 452 081 641 205 741
402 386 859 422 150 819 235 820 188 131 600 400 426 242 412 703 104 933
475 193 773 453 392 698 416 023 648 559 120 267 714 921 559 920 096 043
252 285 862 164 390 526 484 536 279 090 439 567 022 263 359 595 733 748
937 986 732 684 010 570 260 839 057 748 947 468 909 595 142 090 238 873
827 459 603 865 242 058 618 363 561 394 931 319 169 747 665 569 165 983
255 069 839 044 731 325 788 001 824 844 639 329 560 284 557 546 338 601

554 544 981 986 101 878 330 383 388 074 928 073 647 994 351 331 492 858 392 002 423 201 073 477 846 624 814 307 635 553 735 066 519 032 258 039 977 860 246 199 552 893 831 590 213 995 728 230 430 999 288 827 488 617 987 649 709 841 226 890 907 255 259 713 788 299 398 367 196 476 402 732 479 426 051 693 901 452 340 598 402 117 422 904 826 753 773 939 997 753 285 314 424 674 820 643 685 791 820 779 490 359 955 638 643 060 152 653 062 031 833 458 086 443 497 652 265 666 646 202 323 163 581 570 712 228 533 339 386 192 794 765 912 722 129 684 110 120 733 163 494 780 684 946 864 086 937 714 246 531 578 472 004 469 780 107 348 882 502 798 191 607 151 778 725 892 654 620 110 988 616 943 359 375

Since they need keys of length 4,5 and 6 then we scroll the number M and see that the first 4 appears after the sequence 8 606 8. So Stella and Ben take 4 digits after the first 4 which are 2941. So, $m_{1(4)} = 2941$. Where the notation $m_{s(t)}$ represent the sth key of lenght t. The first 5 appears after the sequence 606 842 941 648 980 141 and it is followed by the digits 00 390 , so $m_{1(5)} = 00390$. If we continue we find $m_{1(6)} = 684294$, $M_{2(4)} = 1648$ and so on. It is easy to see that there is a large number of 4, 5 and 6's in M, so the number of keys is very large; in this case there are 5277 k's.

Here is the full list of the keys of length 4:

2941, 1648, 8980, 1500, 333, 5091, 6295, 4474, 4749, 7492, 9203, 7537, 1060, 8881, 2730, 6822, 2320, 1929, 2534, 1524, 4900, 9008, 8459, 5972, 4141, 1414, 1432, 3234, 5859, 5601, 7924, 2188, 2419, 1936, 5444, 4408, 4086, 860, 568, 5403, 365, 5779, 8703, 1288, 3906, 2647, 7432, 3271, 4663, 6630, 2430, 3041, 1243, 3781, 6540, 540, 574, 3664, 1242, 2411, 1120, 5296, 6848, 8235, 2669, 1300, 1972, 3356, 2970, 4801, 8016, 7197, 8150, 18, 8894, 6730, 3269, 3625, 5504, 6507, 3078, 5496, 9629, 3431, 3176, 149, 9655, 5908, 1804, 9514, 6688, 9051, 1580, 550, 9449, 4973, 9730, 9473, 7309, 2031, 4605, 6051, 8855, 6443, 4390, 3901, 2444, 4441, 4417, 4173, 1738, 7242, 2876, 1573, 1874, 2866, 2876, 7722, 5858, 3936, 647, 7124, 6649, 9716, 6873, 7582, 7348, 8259, 8194, 269, 7021, 8437, 3751, 763, 3084, 6549, 9596, 9904, 1786, 7092, 4430, 4303, 3038, 7953, 25, 3876, 7154, 1431, 3126, 7039, 9255, 8572, 859, 8489, 8940, 304, 1065, 2639, 550, 7349, 9464, 6474, 7467, 6762, 711, 136, 3116, 7683, 3079, 1334, 4097, 974, 2860, 4808, 8089, 9799, 5068, 5511, 1817, 3179, 7055, 2175, 5451, 5152, 5051, 8046, 6170, 6221, 4473, 4734, 7346, 6763, 2805, 8536, 1276, 8892, 7017, 7302, 5098, 7496, 9677, 1955, 5810, 4904, 9040, 228, 8292, 4054, 543, 3057, 5980, 866, 2335, 2575, 3404, 439, 3901, 9956, 8529, 7285, 9640, 904, 1527, 7914, 3842, 2825, 6791, 3587, 633, 2052, 6997, 2844, 4844, 8442, 4257, 2578, 9536, 9353, 5726, 6070, 9708, 2117, 2791, 7958, 9324, 9900, 5725, 3533, 5570, 1601, 757, 6117, 6972, 6013, 2723, 7875, 6203, 1435, 3570, 8343, 3768, 8020, 9985, 1679, 7022, 9261, 7144, 4302, 3023, 3407, 770, 835, 3463, 6306, 2420, 2000, 1620, 4260, 2605, 9536, 7119, 7901, 5254, 9613, 70, 6491, 9105, 1, 5166, 9154, 6717, 9279, 947, 7543, 3391, 4263, 2632, 5369, 1346, 6495, 9583, 5689, 4922, 9228, 8443, 4312, 3123, 6591, 6280, 7670, 728, 3266, 6216, 8981, 2126, 1362, 1086, 2258, 5917, 4459, 4593, 5930, 7188, 2496, 9685, 8257, 6164, 1253, 9150, 9742, 2451, 5199, 1907, 7663, 2324, 6285, 812, 2108, 7971, 5812, 4949, 9492, 9281, 5358, 3592, 8721, 2462, 6226, 5281, 9498, 9830, 9028, 3942, 2306, 5807, 9142, 2224, 9475, 7574, 5374, 3457, 5765, 9963, 2273, 2482, 8206, 9034, 9918, 5465, 6529, 8236, 7273, 8056, 9330, 986, 9250, 4032, 322, 6407, 767, 4482, 4824, 8246, 6974, 2394, 6059, 2246, 6959, 476, 7636, 5884, 7963, 5722, 746, 6580, 5879, 3815, 9709, 1209, 8145, 5282, 9149, 9070, 3954, 7960, 3672, 8286, 3930, 6568, 6822, 1064, 6193, 5535, 383, 9899, 8419, 1929, 9538, 1983, 7686, 3229, 6865, 583, 4300, 3002, 9492, 9288, 7076, 8066, 2069, 5028, 386, 8251, 8962, 6580, 6564, 849, 9709, 7590, 2718, 1300, 4220, 2203, 7446, 4660, 6602, 5436, 3656, 1910, 5846, 6278, 5764, 9172, 1982, 6523, 3714, 7942, 2798, 3610, 8948, 8785, 5644, 4990, 9902, 2244, 4494, 4941, 9416, 1638, 3290, 4252, 2520, 6029, 7356, 3226, 2137, 2016, 4709, 7093, 1061, 484, 8452, 5211, 472, 7266, 7159, 4481, 4815, 8158, 6408, 895, 6922, 8312, 2113, 7853, 6, 8714, 5146, 6721, 1539, 8730, 1757, 9198, 8538, 8865, 37, 1753, 6369, 1030, 9628, 78, 6876, 6931, 5433, 3349, 9120, 5724, 789, 6990, 1052, 2182, 8961, 5447, 4768, 7689, 9703, 7319, 833, 3502, 8487, 8709, 1330, 491, 9192, 2797, 430, 3076, 353, 2342, 2432, 3297, 9344, 4699, 6990, 2971, 3991, 5631, 9782, 7879, 8767, 8147, 7376, 8873, 1775, 8862, 3738, 5328, 9858, 8023, 775, 566, 182, 925, 1730, 8544, 4860, 8607, 2109, 9641, 1115, 5313, 3837, 5855, 9970, 1379, 5609, 5587, 8630, 1283, 2499, 9929, 7544, 4308, 3080, 3764, 6485, 8536, 1809, 5335, 5565, 7956, 5194, 6869, 504, 1816, 7942, 2790, 4439, 4396, 3960, 2961, 3585, 2879, 5775, 8106, 3215, 1799, 6092, 3225, 835, 4017, 173, 1912, 9, 3288, 1492, 9287, 4356, 3563, 7997, 9323, 3398, 4868, 8687, 1851, 7645, 5922, 8533, 7821, 3953, 4693, 6938, 4975, 9755, 9034, 8550, 5652, 2856, 1278, 3807, 3615, 7679, 7927, 4233, 2336, 5064, 8194, 5820, 6887, 6515, 6221, 1474, 7423, 2377, 5864, 4538, 5389, 7344, 4358, 3583, 5520, 7242, 2290, 6437, 3762, 2024, 4744, 7442, 4204, 2049, 9442, 4220, 2206, 6829, 4700, 7000, 689, 1430, 3028, 1546, 6641, 1466, 6694, 8990, 6318, 3879, 2603, 9040, 783, 8515, 5621, 171, 9745, 5465, 6574, 6085, 8557, 9244, 4505, 5054, 7613, 5639, 4472, 4726, 7260, 9025, 5960, 5634, 3113, 6822, 2996, 1309, 6712, 3175, 5041, 1825, 2271, 7572, 8362, 3439, 3915, 3142, 2851, 752, 5659, 5266, 2602, 8499, 9980, 8579, 7862, 8650, 1225, 6607, 2972, 8391, 7629, 740, 615, 1699, 3421, 2106, 1686, 2449, 4965, 9654, 5461, 6183, 9407, 717, 2460, 6086, 6051, 4166, 1669, 2266, 640, 729, 6392, 8983, 8645, 5816, 3621, 3129, 7482, 8217, 4516, 5160, 4417, 4176, 1766, 6889, 6926, 2575, 8234, 9335, 2733, 6146, 6060, 5012, 8220, 3830, 717, 1749, 9196, 4662, 6623, 7400, 9, 1030, 436, 3616, 1325, 5121, 2601, 6107, 771, 6567, 1395, 6305, 6673, 3312, 9401, 196, 7508, 4714, 7148, 8594, 2509, 4179, 1798, 6377, 7591, 2694, 453, 5396, 3412, 1208, 7574, 7060, 7078, 6697, 4433, 4339, 3392, 1072, 3498, 9808, 7825, 8880, 1588, 1567, 330, 389, 579, 4687, 6878, 4297, 2971, 1924, 7981, 9603, 9760, 6077, 1954, 8774, 7224, 1814, 517, 9921, 6268, 7794, 155, 9314, 4397, 3976, 312, 5232, 6409, 977, 6373, 388, 5465, 6568, 9734, 973, 2605, 5770, 6346, 6605, 9378, 7179, 4075, 755, 7477, 7793, 2341, 1641, 1440, 4022, 223, 3525, 3407, 782, 5310, 6410, 1001, 6646, 6458, 5823, 1258, 7343, 3413, 1384, 5742, 2957, 4526, 5269, 1700, 7217, 3441, 4163, 1639, 2613, 7856, 9287, 5246, 6583, 8688, 3109, 6394, 6238, 8877, 3018, 260, 8416, 1630, 2683, 9862, 2758, 4187, 1877, 113, 3386, 1171, 9512, 9690, 7455, 5533, 3292, 5255, 1968, 4226, 2269, 6361, 4127, 1278, 3594, 3222, 9324, 4958, 9587, 9869, 1494, 9484, 8407, 748, 8846, 6793, 5724, 5396, 1859, 5496, 9682, 4051, 517, 3426, 2604, 2143, 3793, 4650, 6502, 3844, 4005, 50, 8272, 8731, 3976, 3521, 8243, 3927, 3352, 6099, 6936, 7991, 3703, 5782, 4142, 1428, 2853, 7018, 5390, 5537, 49, 9546, 6079, 5508, 7822, 2502, 179, 2755, 7762, 680, 3915, 8296, 4602, 6024, 5320, 461, 6167, 6919, 9019, 1493, 9301, 1865, 6268, 5503, 576, 1191, 1553, 7698, 3280, 9830, 6720, 4859, 8599, 293, 5416, 1633, 9872, 2865, 1963, 1446, 4653, 6533, 74, 1374, 506, 9354, 5468, 6867, 4552, 5525, 5597, 2127, 4191, 1911, 9624, 7894, 8836, 8954, 5992, 6762, 5375, 1726, 1641, 1657, 5197, 318, 6294, 318, 868, 7735, 4853, 8539, 5258, 4909, 9092, 2261, 6839, 3853, 4472, 4720, 7204, 4987, 9874, 7691, 9759, 1299, 195, 2213, 7371, 3906, 926, 3468, 6861, 2625, 9154, 580, 447, 4790, 7901, 5612, 7012, 8551, 6017, 7578, 1997, 4880, 8808, 8611, 8292, 882, 6929, 5718, 8636, 6972, 8464, 6453, 5309, 3620, 6130, 738, 7542, 2890, 3705, 1037, 1623, 6349, 9735, 1341, 1699, 5060, 1165, 1119, 6205, 8027, 3467, 6775, 1047, 7209, 8658, 8046, 6742, 2850, 3527, 9312, 403, 390, 4787, 7870, 6852, 9736, 3455, 5563, 239, 3216, 1147, 7727, 2043, 3836, 2673, 3149, 9177, 8017, 8069, 6186, 2121, 263, 4052, 527, 4314, 3147, 7648, 8147, 7070, 9718, 4486, 4862, 8621, 3378, 9601, 6169, 5254, 3516, 2731, 5270, 3252, 6224, 4062, 627, 2609, 2534, 3614, 449, 4981, 9816, 1668, 9024, 9251, 3517, 4466, 4665, 6652, 5461, 6161, 772, 9485, 8589, 8809, 7292, 4847, 8471, 7197, 5926, 5814, 1580, 7825, 2986, 5864, 7874, 536, 3290, 1855, 3268, 60, 3247, 7389, 7216, 3986, 3753, 5392, 3643, 3510, 8618, 6761, 4267, 2671, 9442, 4275, 2752, 5128, 9464, 6452, 5278, 598, 4632, 6322, 3689, 8216, 3514, 1083, 9172, 1921, 8245, 5261, 1239, 1851, 501, 3360, 2698, 2656, 1163, 3043, 3882, 7052, 891, 7512, 1411, 1150, 1295, 4525, 5258, 768, 4573, 5735, 5302, 3517, 5251, 1524, 7950, 9229, 3809, 1032, 1417, 1790, 8456, 5618, 604, 8366, 2762, 5507, 6238, 4962, 9626, 356, 3580, 6372, 3993, 1622, 1061, 2750, 787, 6180, 20, 3628, 2714, 5754, 1665, 3877, 8952, 1945, 5069, 3545, 5380, 1324, 4518, 5185, 1946, 6598, 6343, 3165, 7971, 5881, 6015, 9868, 5314, 8914, 9459, 5983, 9213, 166, 4672, 6725, 366, 8269, 7442, 4237, 2371, 5158, 4100, 1004, 9121, 6811, 748, 8031, 8162, 1227, 1304, 9132, 241, 1168, 7199, 4633, 6339, 8994, 9416, 1693, 3522, 7111, 4239, 2394, 7998, 9914, 2568, 4701, 7014, 3139, 4487, 4878, 8784, 5127, 8833, 5882, 3172, 3591, 7696, 7675, 5932, 8853, 4718, 7182, 2815, 8946, 6580, 1984, 7781, 8389, 287, 7353, 2145, 5696, 2365, 3594, 5453, 5388, 4732, 7327, 4751, 7518, 9646, 6199, 9907, 7040, 893, 108, 164, 2825, 5331, 2932, 173, 8445, 4521, 5214, 4471, 4717, 7178, 9012, 8047, 7723, 178, 8780, 4172, 1725, 2016, 9726, 8028, 5783, 8144, 4776, 7764, 5651, 1252, 7124, 9917, 9874, 9320, 8809, 3274, 8966, 8733, 8798, 9422, 2216, 2905, 8129, 5076, 6277, 2832, 3302, 2735, 2495, 9580, 4399, 3998, 3630, 337, 8365, 1090, 5337, 7480, 8078, 3771, 3188, 6109, 4099, 996, 8884, 7852, 1223, 6058, 3642, 2677, 8702, 3456, 5624, 4612, 6124, 8742, 2367, 3656, 6143, 3930, 7942, 2654, 423, 2376, 72, 1271, 4675, 6755, 9385, 8542, 2004, 1100, 7451, 5102, 721, 5562, 3455, 5575, 8569, 4214, 2140, 246, 6938, 2322, 4984, 9843, 3354, 435, 3574, 502, 1258, 8972, 5885, 7661, 1078, 7051, 6853, 2289, 6822, 804, 6672, 6130, 9032, 75, 9892, 979, 4567, 5679, 2096, 8867, 2984, 1459, 5917, 8656, 4592, 5926, 933, 967, 4776, 7769, 6741, 1179, 2530, 3731, 7608, 1967, 3953, 9078, 9917, 7321, 4049, 496, 9635, 9844, 4931, 9315, 1348, 8845, 5358, 3776, 3341, 1617, 2384, 7056, 4892, 8923, 4502, 5025, 9551, 33, 8614, 1732, 6035, 2687, 146, 6482, 8299, 9616, 2921, 9034, 427, 2781, 1306, 3037, 9608, 6232, 5982, 567, 924, 1813, 9120, 2080, 8179, 4570, 5707, 799, 1428, 2853, 7085, 8608, 6393, 9448, 4826, 8266, 4056, 569, 4726, 7262, 2479, 7957, 2091, 356, 6933, 4070, 701, 2635, 1825, 8730, 4625, 6250, 2574, 6690, 9745, 5139, 1827, 856, 940, 366, 7164, 2856, 8062, 9581, 5319, 4318, 3189, 7659, 1339, 2613, 3051, 5208, 1205, 1402, 238, 2215, 42, 2624, 2412, 1270, 9334, 7519, 5339, 1602, 8559, 9215, 3252, 3905, 8453, 5362, 3956, 8937, 105, 8947, 7468, 6890, 2090, 5960, 2058, 9313, 7665, 4731, 7313, 8446, 4639, 6393, 5575, 6338, 5449, 4981, 9819, 9280, 7994, 3513, 9285, 2320, 7784, 6624, 8143, 3076, 6199, 3099, 8861, 9709, 1226, 7640, 273, 7942, 2605, 5234, 598, 211, 2290, 8267, 4246, 2467, 6748, 8206, 3685, 9035, 3060, 5808, 4349, 3497, 9765, 6202, 7659, 1101, 9478, 7806, 9468, 6864, 869, 2465, 6531, 7200, 4697, 6978, 8882, 6201, 3359

8 Conclusions

We hope to have left the reader with the understanding that the LSA algorithm can be used with different combinations of cyclic and non-cyclic groups. This means that this algorithm can be used in either symmetric or asymmetric modes of encryption. It is also of great benefit to the users of this algorithm that we can design systems of varying computational complexity and security by using different groups, encrypting Σ, and various other methods that make a group discovery by the cryptanalyst meaningless. In fact, we believe that exchanging keys between each character gives the LSA algorithm an equivalent time complexity to that of a one-time-pad.

In closing, the authors of this paper sincerely hope that if this bit of mathematics is found to be a useful tool, then humanity will use it to find ways to improve our standing in nature.

References

[1] Francesco Lucente Stabile, Carey P. Atkins *The Lucente Stabile Atkins Cryptosystem*, 2019.

[2] David Burton, *M. Elementary Number Theory*, 7^{th} ed., McGraw-Hill Education (India) Private Limited, 2016.

[3] Joseph A. Gallian *Contemporary Abstract Algebra*, 8^{th} ed., Cengage Learning, 2016.

[4] Wade Trappe and Lawrence C. Washington, *Introduction to Cryptography: with Coding Theory*, Pearson Education, 2006.