Encryption and Decryption Process using Composite Numbers

Rajendra Hegadi[†], Muppinaiya Nagaraj[††] and Shamshekhar S Patil[†††]

[†]SCT Institute of Technology, [††] Deccan Institute of Advanced Studies, [†††]Dr. Ambedkar Institute of Technology, Bangalore, India

Summary
Our main aim in the present paper is the extension of the Encryption/Decryption processes using products of primes. We now show in this paper how to generate a group from any general natural number or a product of such natural numbers. We then show how this group can be used for generation of a simple (yet as secure, as the one that is generated with the help of larger primes) encryption /decryption process. This work is continuation of the work that the first author had undertaken with Dr. H. Chandrashekhar in the 90's using Farey Fractions summary.

Key words:
Encryption, Decryption, Primes and composite numbers.

1. Introduction

Our aim in the following discussion is the study of the Cryptology with the help of application of number groups in the generation of secure codes in general. These codes are meant to conceal sensitive data from the prying eyes of hackers whose main objective is three - fold.
(1) Steal the data and put it to destructive uses.
(2) Alter the code in such a way that the objective of original code is completely destroyed.
(3) Use the data for clandestine purposes. The objectives of Cryptology are thus meant to enforce security of the organizations by securing the data and operations on them.

Primes are the bread and butter of the cryptologist. A traditional encryption process requires longer prime numbers (1064 bits). However this long encryption code may lead to easier hacking compared to a large number of primes used for different pieces of code. In this paper we first show how to generate groups of integers with the help of product of primes and then use such group of integers to develop encryption process.

Manuscript received January 10, 2007
Manuscript revised January 25, 2007

2. Groups

Groups, rings and fields are the fundamental elements of abstract algebra or modern algebra. In the abstract algebra we are concerned with the sets on whose we can operate algebraically; that is we combine two elements of the set,

perhaps in several ways, to obtain the third element of the set. These operations are subject to specific rules, which define the nature of the set. By convention, the notation for the two principal classes of operations on set elements is usually the same as the notation for the addition and multiplication on ordinary numbers. However, it is important to note that, in abstract algebra, we are not limited to ordinary arithmetical operations. The symbol N stands for the set of all natural numbers, also called the "Counting Numbers", and is given by: N = {0, 1, 2, 3, …,.n-1, n, n+1, …. }.

3. Theorem

We first prove a simple theorem, which establishes the group structure for the product of two, and hence also for the product of more than two primes.

3.1 THEOREM 1:

Let $p_1, p_2, \cdots p_k$ be any k distinct primes >1. Then the set of all integers n relatively prime to each of the primes pk constitute a multiplicative group Modulo P, where $P= p_1 \bullet p_2 \bullet p_3 \cdots \bullet p_k$

Proof:

The proof of this Theorem is quite straight forward. Note that the closures, Associativity, the identity given by 1 are easily verified. If x is an element of this set, it is relatively prime to P and hence is an element of the group. Use of the Euclidean Algorithm proves the existence of the inverse x^{-1} modulo P. In essence, the set of all those positive integers which are less than P and relatively prime

to P are used for encrypting the given message, since these integers possess their inverses modulo P.

The one problem that we face with this approach is basically due to our choice of the k primes $p_1, p_2, \cdots p_k$. The problem arises when the number k of primes is large. Then necessarily the number of integers we have at disposal for encryption becomes less.

Figure 1: Modulo 17 Multiplication table

$\times_{17}$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	4	6	8	10	12	14	16	1	3	5	7	9	11	13	15
3	3	6	9	12	15	1	4	7	10	13	16	2	5	8	11	14
4	4	8	12	16	3	7	11	15	2	6	10	14	1	5	9	13
5	5	10	15	3	8	13	1	6	11	16	4	9	14	2	7	12
6	6	12	1	7	13	2	8	14	3	9	15	4	10	16	5	11
7	7	14	4	11	1	8	15	5	12	2	9	16	6	13	3	10
8	8	16	7	15	6	14	5	13	4	12	3	11	2	10	1	9
9	9	1	10	2	11	3	12	4	13	5	14	6	15	7	16	8
10	10	3	13	6	16	9	2	12	5	15	8	1	11	4	14	7
11	11	5	16	10	4	15	9	3	14	8	2	12	7	1	12	6
12	12	7	2	14	9	4	16	11	6	1	13	8	3	15	10	5
13	13	9	5	1	14	10	6	2	15	11	7	3	16	12	8	4
14	14	11	8	5	2	16	13	10	7	4	1	15	12	9	6	3
15	15	13	11	9	7	5	3	1	16	14	12	10	8	6	4	2
16	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

The ideal thing is to take 2 primes and their product, or even better, one takes the square of a single prime. Note that taking cubes and higher powers will not be as efficient as the square. For example, choose the prime 3 and its cube as the modulus. The cube defines 27 elements including 1, and 27 which plays the role of 0: The 27 elements of the set are {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26}. Out of the 27 elements, there are 9 elements which are already divisors of zero.

Example 1: Consider the prime 17. The numbers of positive integers less than 17 are 1, 2, 3,····· 15, and 16. Note that none of these 16 elements is omitted from consideration; under multiplication modulo 17, all these 16 elements constitute a multiplicative group modulo 17. The Table in figure 1 establishes this fact.

Example 2: Next consider the square $17^2 = 289$. There are exactly 16 elements, namely 17, 34, 51, 68, 85, 102, 119, 136, 153, 170, 187, 204, 221, 238, 255, 272 which are divisors of 0 modulo 289 and hence do not possess their inverses mod $289 = 17^2$. All other (289 – 16 =) 273 numbers satisfy the following conditions:

a. They are relatively prime to 17 and hence to 289.

b. They posses their multiplicative inverses modulo $17^2 = 289$.

Since these 273 numbers are relatively prime to 289, they possess their multiplicative inverses modulo 17^2. This fact follows from the Euclidean Algorithm. For example,

consider 25 which is relatively prime to 17 and hence to 289. Note that $185 \times 25 = 4625 = 16 \times 289 + 1 \equiv 1 \bmod 289$. Hence the two integers 185 and 25 are inverses of each other under modulo 289 by the Euclidean Algorithm. In fact, we can show that all positive integers less than 289 and not equal to the following 16 numbers: $\{17r \mid 1 \le r \le 16\}$ = [17, 34, 51, 68, 85, 102, 119, 136, 153, 170, 187, 204, 221, 238, 255, 272} are relatively prime to 289. Note that the positive numbers which are different from these 16 numbers and less than 289 possess their inverses modulo 289.

Let n be any integer less than 289 is also relatively prime to 289. We show that its inverse modulo 289 exists. First, we list all those elements which are relatively prime to 289: {1, 2, 3,…, 16; 18, 19,….., 33; 35, 36, …..., 50; 52, 53, …., 67; 69, 70, 71, …., 84; 86, 87, …., 101; 103, 104,….,118; 120, 121, …., 135; 137, 138, …., 152; 154, 155, …., 169; 171, 172, 173, …., 186; 188, 189, …., 203; 205, 206, …., 220; 222, 223, …., 237; 239, 240, ….,254;

356, 257,….,271; 273, …., 288}. The elements that are left out are the 17 multiples of 17 which are divisors of zero mod 289.

3.2 Euclidean Algorithm:

Consider the element 100. We find its multiplicative inverse mod 289 using the Euclidean Algorithm: $289 = 2\times100 + 89 \rightarrow 100 = 1 \times 89 + 11 \rightarrow 89 = 8\times11 + 1 \Leftrightarrow 1 = 89 - 8\times11 = 89 - 8\times(100 - 89) = 9\times89 - 8\times100 = 9\times[289 - 2\times100] - 8\times100 \equiv 26\times100 = (289 - 26)\times100 \equiv 263\times100 \Leftrightarrow$ the inverse of 100 is 263.

Figure 2: Modulo 17 Multiplication table

× 60	01	07	11	13	17	19	23	29	31	37	41	43	47	49	53	59
01	01	07	11	13	17	19	23	29	31	37	41	43	47	49	53	59
07	07	49	17	31	59	13	41	23	47	29	37	01	29	43	11	53
11	11	17	01	23	07	29	13	19	41	47	31	53	37	59	43	49
13	13	31	23	49	41	07	59	17	43	01	53	19	11	37	29	47
17	17	59	07	41	49	23	31	13	47	29	37	11	19	53	01	43
19	19	13	29	07	23	01	17	11	49	43	59	37	53	31	47	41
23	23	41	13	59	31	17	49	07	53	11	43	29	01	47	19	37
29	29	23	19	17	13	11	07	01	59	53	49	47	43	41	37	31
31	31	37	41	43	47	49	53	59	01	07	11	13	17	19	23	29
37	37	19	47	01	29	43	11	53	07	49	17	31	59	13	41	23
41	41	47	31	53	37	59	43	49	11	17	01	23	07	29	13	19
43	43	01	53	19	11	37	29	47	13	31	23	49	41	07	59	17
47	47	29	37	11	19	53	01	43	17	59	07	41	49	23	31	13
49	49	43	59	37	53	31	47	41	19	13	29	07	23	01	17	11
53	53	11	43	29	53	47	19	37	23	41	13	59	31	17	49	07
59	59	53	49	47	43	41	37	31	29	23	19	17	13	11	07	01

Further, since all these (289 – 16 = 273) numbers are relatively prime to 289; their products are also relatively prime to 289. Their inverses modulo 289 exist and the closure law under multiplication modulo 289 holds. The unit 1 plays the role of the identity and the associative law modulo 289 is inherited from the associative law of ordinary multiplication of integers.

The integer 1 modulo 289 plays the role of the identity for multiplication modulo 289. Therefore we conclude that the set of all integers less than $289 = 17^2$ and relatively prime to 17 constitute a commutative group under multiplication operation modulo $17^2 = 289$. The order of this group is 273.

3.3 Propositions:

Proposition 1:

Let G_n $\{x \in N \mid x \neq 0, (x, n) = 1\}$, we have the set of all integers in G_n relatively prime to $n \in N$, $n \neq 0$ constitutes a multiplicative group under mod n.

Example 3**:** Let $n = 2^2\times3\times5 = 60$. Then $G_{60} = \{1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59\}$

The set G_{60} has 16 elements, all of which are invertible modulo 60. Further note that 49 is a composite integer. But yet it possesses its multiplicative inverse modulo 60 with which it is relatively prime. In the same way, it is interesting to construct the group structure for the set of all the 25 elements which are relatively prime to 70.

Note that this relative primality of integers is a useful tool in the construction of group structures for all the relatively prime integers. Integers 3, 9, 27 are relatively prime to 70, and yet they possess their multiplicative inverses modulo 70. We obtained the group table for the group $\{G_{70}, \times_{70}\}$ in the same manner, without much difficulty. Note that the integer 70 is a composite integer. Integers less than 70 and relatively prime to it could also be composite without losing their ability to possess multiplicative inverses modulo 70.

Proposition 2:

Every positive integer n is a unique product of powers of primes, $n = p_1^{\alpha 1} \bullet p_2^{\alpha 2} \bullet p_3^{\alpha 3} \ldots\ldots\ldots p_n^{\alpha n}$ Where α1, α2, α3…….. αn are positive integers ≥ 0. We define the set G_n such that $G_n = \{m \in N^+ \mid (m, n) = 1\}$. Then (G_n, X_n) is a commutative group.

Proof:

Closure: For every a and b in G_n, (a × b) mod n is also in G_n
Associativity: For every a, b, c in G_n, we have (a × b) × c = a × (b × c)
Existence of Identity: There is a unique element 1 in G_n, called the identity, such that for any a in G_n, we have 1 × a = a × 1 = a
Existence of inverses: For every a in G_n there is a unique element b in G_n such that a × b = b × a = 1 mod n. This b is denoted by a^{-1} and is called the inverse of a.
Commutative: For every a, b in G_n, a × b = b × a.

4. Encryption and Decryption (ED) Process

We work out a relatively new concept of the construction and usage of the encryption process. Note also the fact that we can construct, quite easily with the help of a suitable program, a simple function of selected set of primes of the type that suits the ED processes. The ED process that we describe is a variable process and it does not necessarily require us to construct the type of large primes that are in use with the current methods. Instead of working with ED processes with primes containing around 350 decimal digits, we shall work with a large number of primes of moderate size. But the technique used in the ED procedures change, depending on the following factors: i) Level of security, ii) size of the file, iii) availability of the computing facility.

In this procedure we use product (and hence powers of primes) for encryption process. The main reason for this approach is three-fold.

There are a large number of primes.

Since the integers are used in this new encryption procedure, hacking a given message becomes all the more time consuming as it is difficult to compute the integer which is the product of primes. The hacker will have to fix the set of primes and their products which is being used in representing alphabets.

The present usage of a very long (1064 bits) encryption code that is being used may lead to easier hacking compared to integer which is product of number of primes used for encryption with this procedure in mind. We describe the one such ED process with an example below.

4.1 Example:

Let us look at simple situation, the word *JERRY* is being encrypted by choosing 3 small primes p_1=7, p_2=7 and p_3=11. The important fact we keep in mind is that it is not necessary to restrict our self to just the two prime numbers, viz 7 and 11, we could indeed choose , for example, a much larger primes and their powers to deal with its subsets for the ED processes.

Step 1: Compute n and N:
We compute n = 7 × 7 × 11 = 539, note that n is composite (not a prime) number.
Now we have commutative group N which is a set of all integers from 1 to 539 excluding the integers 7, 11 and their multiples.
N={1,2,3,4,5,6,~~7~~,8,9,10,~~11~~,12,13,~~14~~,15,16,17,18,19,20,~~21~~ ,~~22~~,23,24,25,.....538, ~~539~~}
By above proposition any a in N, has its inverse element a' in N, such that a × a' = 1 mod n. There are totally 119 integers that do not belong to N. Hence N has totally 539-(49+77-7) = 420 integers which have their inverse elements in N under modulo n. (use Venn diagram to calculate |N|)

Step 2: Dividing N into blocks of integers
We now divide the set of all integers N to number of blocks. For simplicity we make the following assumptions. Leaving 1 and 538 from the group N, as their inverses are themselves, we are left with 418 integers.
Blocks are of size 26 integers (to increase the complexity we can choose the blocks of different sizes).
One-to-one onto mapping of integers in each block with each English alphabet. (Association of alphabet with integers can be made randomly for further increase in the complexity)

Then we have total of 17 blocks, 16 of them are of size 26 integers each, and last block is of size 2 integers, constituting total of 418 integers. Figure 2 shows the first block, in which.

Column 1: Set of Integers from N assigned to Block-B1.
Column 2: One-to-one onto association of Alphabet with the integers.
Column 3: The corresponding inverse integers from N under modulo n
Column 4: The corresponding inverse alphabet.
Column 5: The Block numbers to which the inverse integers and inverse alphabets belong.

Step 3: Association of alphabets with blocks
Associate each alphabet of the plain text *JERRY* with different blocks in random way J→B1, E→B3, R→B7, R→B9 and Y→B16. Note: only one letter is chosen from every block.

Step 4: Encryption
The table below gives the complete picture about the encryption process of the plain text in to cipher text. We

do select the blocks and associate the integers with alphabets randomly so that the hacker will have the tougher task to find the exact association.

In some cases it may happen that, due to random association, all the cipher text alphabets may end up with a single alphabet in place of all the places. In this situation even though the encryption algorithm is know by the hacker it is much difficult to identify integer n (product of primes) and decrypt the cipher text.

Figure 3: First block of integers with their inverse integers & inverse alphabets

N	Alpha bet	Inverse Integer (mod 539)	Inverse Alphabe t	Block Number
2	A	270	B	B9
3	B	180	J	B6
4	C	135	Z	B4
5	D	108	F	B4
6	E	90	R	B3
8	F	337	B	B11
9	G	60	T	B2
10	H	54	P	B2
12	I	45	H	B2
13	**J**	83	M	B3
15	K	36	A	B2
16	L	438	C	B14
17	M	222	P	B7
18	N	30	W	B1
19	O	227	T	B7
20	P	27	U	B1
23	Q	375	E	B12
24	R	292	S	B9
25	S	345	H	B11
26	T	311	H	B10
27	U	20	P	B1
29	V	316	L	B10
30	W	18	N	B1
31	X	313	J	B10
32	Y	219	N	B7
34	Z	111	H	B4

Step 5: Decryption

Decryption process is simply the reverse process of encryption. Known the cipher text alphabet and the associated integers, we have to compute their inverses by identifying the blocks associated with the integers of cipher text

Observe that if we encrypt word ZIST using only block-B1, the cipher text will be HHHH. Known the algorithm the hacker will have tougher task to break such cipher text.

4.1 Why hacking is difficult task?

To break the cipher text hacker has to compute the following

i) Identify accurately, the prime numbers used to obtain n.

ii) Identify the powers of the primes, i. e compute α1, α2, α3, α4……. αn, that are chosen randomly.

Figure 4: Plain text Encryption

Plain Text Alphabets	J	E	R	R	Y
Block Number (Random association)	B1	B3	B7	B9	B16
Associated Integer	13	74	225	257	534
Inverse Integer (mod 539)	83	51	218	388	431
Block number of Inverse Integer	B3	B2	B7	B12	B13
Inverse Alphabet (cipher text)	M	M	M	W	W

Figure 5: Decryption of Cipher Text

Cipher Text	M	M	M	W	W
Block number of Cipher Text Integer	B3	B2	B7	B12	B13
Integer Associated Cipher Text	83	51	218	388	431
Inverse Integer	13	74	225	257	534
Block Number of Inverse Integer	B1	B3	B7	B9	B16
Plain Text Alphabets	J	E	R	R	Y

iii) Identifying the Number of blocks which are of arbitrarily different in sizes. It will be a very cumbersome task to find these blocks, if some of the blocks are of size less than 26 integers.

iv) Associate alphabets with the integers in each block. This is purely a random process. Blocks with integers fewer that 26 will not have all alphabets from English language associated. However this can be an advantage as it confuses the hacker in association of fewer alphabets with the integers.

Note that these limits of the blocks are artificially chosen for a better understanding and of increasing the complexity of decryption for a hacker. The crucial thing for encryption is the omission 1 and 538 from the set of blocks. The omissions are the simplest of give-always while the hacker tries in decrypting the message: the 1 hint the hacker get straight away is: whatever the prime is used for encryption as soon as hacker sees 1, he/she fixes its inverse as 1, which is its own inverse. The same motive makes us to remove the number 538 from all considerations

5. Conclusion

We have 181 prime numbers of size less than 4 digits between 1 and 1000. We can obtain the larger primes and use to build more and better security environments for information systems. But at this stage, it becomes less important that to design methods of using these already accessible primes to construct security systems. The principle is to design newer methods based on the already known primes.

References

[1] H. Chandrashekhar: ALGEBRAIC CODING THEORY BASED ON FAREY FRACTIONS: Thesis submitted to the BANGALORE UNIVERSITY for the award of the Ph. D. Degree. 1997.

[2] H. Chandrashekhar & M. Nagaraj: KEY – LOCK PAIR MECHANISM FOR ACCESS CONTROL USING TRIBES OF FAREY FRACTIONS, Jour of Discrete Mathematics & Cryptography, Vol. 3, 2000).

[3] R. C. Baker and G. Harman, `Shifted primes without large prime factors', Acta Arithm., 83 (1998), 331-361.

[4] D. Boneh, S. Halevi and N. A. Howgrave-Graham, `The modular inversion hidden number problem', Proc. Asiacrypt'2001, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, 2248 (2001), 36-51.

[5] R. Cramer and V. Shoup, \A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack", in proc. Crypto '98, pp. 13-25, 1998.

[6] Andreas Meyer, Stefan Neis, and Thomas Pfahler, First implementation of cryptographic protocols based on algebraic number fields, Information Security and Privacy, ACISP 2001, Sydney (Vijay Varadharajan and Yi Mu, eds.), Lecture Notes in Computer Science, vol. 2119, Springer, 2001.

[7] D. Stinson, Cryptography, Theory and Practice, Chapman & Hall/CRC, 2002.

[8] B. Schneier, Applied Cryptography, Protocols, Algorithms, and Source Code in C, John Wiley & Sons, inc., 1996.

[9] Cryptography, Wiki Books, http://en.wikibooks.org/wiki/Cryptography

[10] Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/wiki/Main Page

[11] Pascal Paillier, Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, J. Stern, Ed., Advances in Cryptology - EUROCRYPT'99, vol. 1592 of Lecture Notes in Computer Science, pp. 223-238, Springer-Verlag, 1999.

[12] William Aiello, Yuval Ishai, and Omer Reingold. Priced oblivious transfer: How to sell digital goods. In Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding, pages 119–135, 2001.

[13] Vikraman Arvind and Johannes KÖbler. On pseudorandomness and resource-bounded measure. Theoretical Computer Science, 255(1-2):205–221, 2001.

[14] Manindra Agrawal, Neeraj Kayal, Nitin Saxena, PRIMES is in P (2002). URL : http://www.cse.iitk.ac.in/news/primality.html.

[15] Andrew Granville, It is easy to determine whether a given integer is prime, Bulletin of the American Mathematical Society 42 (2005), 3-38; online in 2004. ISSN 0273-0979.

[16] Joshua Holden, Comparison of Algorithm to calculate Quadratic Irregularity of Prime Numbers, Mathematics of Computation, Volume 71, Number 238, Pages 863-871, S 0025-5718(01)01341-2, 2001.

Dr. Muppinaiya Nagaraj

Dr. Muppinaiya Nagaraj received B.Sc. Honors and, M. Sc. in Mathematics from Mysore University India in1958 and 1960 respectively, Ph. D. in Differential Geometry from Graduate Institute of Mathematics and Mechanics, Indiana University, Bloomington, Indiana, U.S.A. in1965. He has been Research Assistant, Teaching Associate in Graduate Institute of Mathematics and Mechanics, Indiana University, Bloomington, Indiana, U.S. He worked as Assistant Professor of Mathematics from 1965 – 1966: Louisiana State University, Baton Rouge, Louisiana, U.S.A., as Scientist in Department of Applied Mathematics, Indian Institute of Science, Bangalore, India: from 1966 – 1967, as Reader in Mathematics and Professor of Mathematics, Bangalore University, Bangalore, India, from 1967 – 1979 and 1979 – 1998 respectively. Since January 1, 2005 he is associated with Deccan Institute of Advanced Studies, Bangalore, India. He has been a reviewer for both the Review Journals in Mathematics: The Mathematical Reviews of the American Mathematical Society and the Zentralblatt fûr Mathematik, Herausgegeben der Berliner Akademie der Wissenschaften und Deutsche Akademie der Wissenschaften. Guided 6 students Ph.D. Degrees. His interests have mainly been in the area of number theory, use of Farey Fractions in generating encryption codes, Differential Geometry, applications to the General and Unified Field Theories of Relativity.

Rajendra Hegadi

Rajendra Hegadi, faculty in department of Information Science and engineering, SCT Institute of technology, Bangalore has received M.Tech degree in Computer Science and Engineering from National Institute Technology, Surathkal, Karnataka, India in 2000, and currently Ph. D student of Computer Science Department of Dr. M.G.R University, Chennai.

Shamshekhar S Patil

Shamshekhar S Patil, faculty in department of Computer Science and engineering, Dr. Ambedkar Institute of technology, Bangalore has received M.Tech degree in Computer Science and Engineering from Manipal Institute Technology, Manipal, Karnataka, India in 1999, and currently Ph. D student of Computer Science Department of Dr. M.G.R University, Chennai.