International Journal of Science Engineering and Advance Technology

Number Theory and Cryptography: An Analytical Approach

P. N. V .Prasada Rao, B. Srinivasa Rao
Senior Lecturer in Mathematics
Sir C. R. R. Autonomous College, Eluru, Andhra Pradesh, India
Prasad.potturi999@gmail.com, srinivasrao.banda@gmail.com

Abstract

The more I have considered Computer Science, the more I see that it is truly a type of connected Mathematics. The two are regularly combined in University divisions, and numerous understudies study both for a more profound comprehension of the key procedures of PCs. As innovation advances, the abilities of PCs increment significantly. Basically, these capacities are simply numerical capacities that run speedier and control more information. To better my comprehension of PC innovation, I contemplated the science behind two long time (and everlastingly) executed PC forms: Cryptography and security.

I. INTRODUCTION

Cryptography is the way toward outlining frameworks to ensure information prior to the security and honesty of information was taken care of by the PC, confidential messages experienced different types of encryption and decoding that, while obsolete today, are still scientifically difficult and fascinating to study. The second range that interests me as a fundamental PC procedure is information pressure. During a time where organizations report that their purchaser information is worth more than their physical organization resources [9], there is a definite need to concentrate on how we store information. More information requires more accessible space on the PC hard plate. Strategies for pressure have dependably existed with PCs and are reliably enhancing to take into consideration more information to _t on a solitary plate. Today, the basic PC client interfaces with compacted files ordinary [1,2].

For a huge number of years, all codes and figures depended on the presumption that the general population endeavoring to impart, call them Bob and Alice, shared a mystery key that their foe, call her Eve, did not have. Sway would utilize the mystery key to scramble his message, Alice would utilize the same mystery key to decode the message, and poor Eve, not knowing the mystery key, would be not able play out the unscrambling. A burden of these private key cryptosystems is that Bob and Alice need to trade the mystery key before they can begin. we focus on open key cryptography. Yet, even inside this area, we have pursueed a little choice of themes to a sensible scientific profundity, instead of giving a more superficial depiction of a more extensive scope of subjects [3,4]. We feel that any peruser who has aced the material in this book won't just be very much arranged for further study in cryptography, however will have obtained a genuine comprehension of the fundamental scientific standards on which current cryptography is based.

The causes of cryptography are lost in the fogs of time, yet probably mystery composing emerged not long after individuals began utilizing some type of composed correspondence, since one envisions that the idea of confidential data must go back to the beginning of development. There are early recorded depictions of figures being utilized as a part of Roman times, including Julius Caesar's work day figure from Section 1.1, and unquestionably from that time ahead, numerous human advancements have utilized both substitution figures, in which every letter is supplanted by another letter or image, and transposition figures, in which the request of the letters is reworked [5,6,7,8].

The innovation of cryptanalysis, that is, the specialty of decoding messages without past information of the key, is later. The most established surviving writings, which incorporate references to prior lost volumes,

are by Arab researchers from the fourteenth and fifteenth hundreds of years. These books depict straightforward substitution and transposition figures, as well as the first recorded occasion of a homophonic substitution figure, which is a figure in which a solitary plaintext letter might be spoken to by any of a few conceivable ciphertext letters.

All the more essentially, they contain the first portrayal of genuine techniques for cryptanalysis, including the utilization of letter recurrence numbers and the probability that specific sets of letters will seem neighboring each other. Shockingly, a large portion of this information appears to have vanished by the seventeenth century [9, 10].

II. Introduction to Number theory

Certain ideas and consequences of number hypothesis come up frequently in cryptology, despite the fact that the methodology itself doesn't have anything to do with number hypothesis. The arrangement of all whole numbers is indicated by Z. The arrangement of nonnegative numbers {0, 1, 2, . . . } is known as the arrangement of characteristic numbers and it's indicated by N. Expansion and duplication of whole numbers are natural commutative and affiliated operations, with personality components 0 and 1 separately. Likewise review the distributive law x(y +z) = xy +xz and the definitions of inverse number - x = (- 1)x and subtraction x - y = x + (- 1)y. [11]

Division of numbers means the accompanying operation: When isolating a whole number x (profit) by a number y 6 = 0 (divisor), x is to be given in the structure x = qy + r, where the whole number r is called leftover portion and fulfills the condition

0 = r < |y|. The number q is called remainder. Including over and again - y or y to x we see that it's conceivable to compose x in the fancied structure. On the off chance that it's conceivable to give x in the structure x = qy, where q is a whole number then it's said that x is separable by y or that y isolates x or that y is a component of x or that x is a numerous of y, and this is meant by y | x. The alleged paltry elements of a whole number x are ±1 and ±x. Conceivable different elements are nontrivial [12].

The accompanying properties of distinctness are entirely self-evident:

(1) 0 is divisible by any integer, but divides only itself.
(2) 1 and -1 divide all integers, but are divisible only by themselves and by one another.
(3) If y | x and x 6 = 0 then |y| = |x|.
(4) If x | y and y | z then also x | z (in other words, divisibility is transitive).

(5) If x | y and x | z then also x | y ± z.
(6) If x | y and z is an integer then x | yz.

The result of division is unique since, if x = q1y + r = q2y + r2 ,where q1, q2, r1, r2 are integers and 0 < r1r21< |y|, then y divides r1-r2. From the fact that|r1-r2| < |y| it then follows that r1= r2 and further that q1= q2. An integer that has only trivial factors is called indivisible. An indivisible integer is a prime number or just a prime2, if it is greater than equal to 2. The first few primes are2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, . . .2 is the only even prime. One basic task is to test whether or not a natural number is a prime [13,14].

III. Euclidean algorithm:

1. If x = 0 then we come out of the algorithm with GCD(x, y) = (y, 0, 1) and quit.
2. If x > 0 then first we divide y with x: y = qx + r, where 0 = r < x. Next we find
GCD(r, x) = (d, e). Nowd = e1, e21r + e2x = e1(y - qx) + e2x = (e2- ey.
We end the algorithm by returning GCD(x, y) = (d, e2- e11q)x + e) and quit.
Since r = y - qx, gcd(x, y) divides r and hence gcd(x, y) = gcd(x, r). Similarly gcd(x, r) q, e1divides y and thus gcd(x, r) = gcd(x, y), so gcd(x, r) = gcd(x, y). Hence #2 produces the correct result. The recursion ends after a finite number of iterations because min(r, x) < min(x, y), and so every time we call GCD (iterate) the minimum value gets smaller and is eventually = 0.
If x, y 6 = 0 then apparently right before stopping in #1 in the recursion we have y = qx and r = 0 and d = x, whence at that point c1= 1 = y and c= 0 = x. On the other hand, every time when in #2 we have y = qx + r and d = e 1r + e22x, where |e11| = x and |e| = r, then e1and e2have opposite signs and thus |e|q = r + xq = y. So, the new coefficients c1= e2- e2q and c2= e12- e1q| = |e2| + |e1will then also satisfy the claimed conditions [15].

$$
\begin{aligned}
a &= b \cdot q_1 + r_2 && \text{with } 0 \le r_2 < b, \\
b &= r_2 \cdot q_2 + r_3 && \text{with } 0 \le r_3 < r_2, \\
r_2 &= r_3 \cdot q_3 + r_4 && \text{with } 0 \le r_4 < r_3, \\
r_3 &= r_4 \cdot q_4 + r_5 && \text{with } 0 \le r_5 < r_4, \\
&\vdots && \vdots \\
r_{t-2} &= r_{t-1} \cdot q_{t-1} + r_t && \text{with } 0 \le r_t < r_{t-1}, \\
r_{t-1} &= r_t \cdot q_t
\end{aligned}
$$

Then $r_t = \gcd(a, b)$.

IV. Congruence Calculus or Modular Arithmetic

The possibility of compatibility math is that you process just with the remnants of numbers utilizing a fixed divisor (or a few of them), the purported modulus m = 1. Compatibility math is likewise regularly called particular number juggling. We say that whole numbers x and y are consistent modulo m, indicated x = y mod m (an alleged harmoniousness), if x-y is detachable by m. This may be perused as "x is compatible to y modulo m" or just "x rises to y modulo m". On the other hand, if x - y is indissoluble by m, it's said that x and y are incongruent modulo m and this is meant by x 6= y mod m. Note that x = 0 mod m precisely when x is detachable by m, and that each number is compatible to each other number modulo 1.

The harmoniousness x = y mod m says that while partitioning x and y by m the rest of the same, or at the end of the day, x and y have a place with the same deposit class modulo m. Each whole number dependably has a place with one deposit class modulo m and just in one. There are precisely m deposit classes modulo m, as there are m distinctive remnants[16].

Clearly x is constantly harmonious to itself modulo m and if x = y mod m, then additionally y = x mod m and - x = - y mod m. Moreover, if x = y mod m and y = z mod m then additionally x = z mod m, for this situation we may compose x = y = z mod m.

Creating an arbitrary whole number Random piece groupings are normally produced utilizing a movement register 8 of p the request modulo 2:ri= a1ri-1+ a2ri-2+ • + amod 2where a1, a2, . . . , apare steady bits (0 or 1, appri-p= 1). To begin with we require he nitial "seed" bitsr. Here we ascertain utilizing the positive deposit framework modulo 2 in other words,using bits. Obviously the acquired arrangement r0, r1, . . . , rp-1, . . . is not irregular at all, for sure, it isobtained utilizing a completely deterministic system and is intermittent (length of period is at most 2p, rp+1).When we pick the coefficients aconveniently, we get the succession to behave"randomly" in numerous faculties, the period is long et cetera, see for instance KNUTH. In thesimplest cases verging on each coefficient is zero.Shift registers of the typer1i, a2, . . . , a= ri-qp-1+ rmod 2,where p is a prime and q is picked advantageously, regularly create great arbitrary bits.

Definition. The fundamental theorem of arithmetic (Theorem 1.21) says that in the factorization of a positive integer a into primes, each prime p appearsto a particular power. We denote this power by ord(a) and call it the order(or exponent) of p in a. (For convenience, we set ordp(1) = 0 for all primes.)

V. Cryptanalysis

The reason for cryptanalysis is to break the cryptosystem, as it were, to find the unscrambling key or encoding key, or to in any event create a technique which will give us a chance to get some informationout of scrambled messages. For this situation it is generally expected that the cryptanalyzer is an eavesdropperor some other threatening gathering and that the cryptanalyzer knows which cryptosystem isbeing utilized yet does not know the key being utilized. A cryptanalyzer may have distinctive data accessible:

(CO) simply a few, possibly irregular, (cryptotext as it were), (KP) a few, possibly irregular, plaintext and the relating cryptotext (known plaintext), (CP) a picked plaintext and the relating cryptotext (picked plaintext), (CC) a picked cryptotext and the relating plaintext (picked cryptotext). Traditional assault strategies are frequently in light of recurrence investigation, that is, learning of the actuality that in long cryptotexts certain images, image sets, image triplets et cetera, happen at certain frequencies. Recurrence tables have been set up for the conventional English dialect, American English et cetera.

```
LOJUM YLJME PDYVJ QXTDV SVJNL DMTJZ WMJGG YSNDL UYLEO SKDVC
GEPJS MDIPD NEJSK DNJTJ LSKDL OSVDV DNGYN VSGLL OSCIO LGOYG
ESNEP CGYSN GUJMJ DGYNK DPPYX PJDGG SVDNT WMSWS GYLYS NGSKJ
CEPYQ GSGLD MLPYN IUSCP QOYGM JGCPL GDWWJ DMLSL OJCNY NYLYD
LJQLO DLCNL YPLOJ TPJDM NJQLO JWMSE JGGJG XTUOY EOOJO DQDMM
YBJQD LLOJV LOJTV YIOLU JPPES NGYQJ MOYVD GDNJE MSVDN EJM
```

Substitution cipher for cryptanalysis

Symmetric and asymmetric ciphers

We have now seen a few different case of figures, all of which have various elements in like manner. Bounce needs to send a mystery message to Alice. He utilizes a mystery key k to scramble his plaintext message m andturnitintoa ciphertext c. Alice, after accepting c, utilizes the mystery key k to unscramble c and reconstitute m. On the off chance that this strategy is to work legitimately, then both Alice and Bob must have duplicates of the mystery key k, and if the framework is to give security, then their foe Eve must not know k, must not have the capacity to figure k,and must not have the capacity to recuperate m from c without knowing k. In this area we figure the idea of a cryptosystem in unique scientific terms. There are numerous reasons why this is attractive. Specifically, it permits us to highlight likenesses and differences between different frameworks, while likewise giving a structure inside which we can thoroughly examine the security of a cryptosystem against different sorts of assaults[17].

Classical Cryptographic Systems

Established cryptography incorporates techniques for hiding plain content that about-face at any rate to antiquated Rome and kept on being utilized something like and amid the world wars. With the emotional enhancements in PC innovation since World War II, these techniques no more o_er security. Notwithstanding, their improvement, execution, and scientific aestheticism is deserving of study [8,9].

To contemplate these techniques, we should _rst de_ne the connection between a plain instant message and its scientific identicalness. Traditionally, this is finished by allocating every letter of the English letter set a numerical worth somewhere around 0 and 25, such that A = 0; B = 1; C = 2; D = 3; : Y = 24; Z = 25. These frameworks likewise join the modulus operation, making the number space [0; 25]. Thusly, all conditions in this area will be done modulus 26. For instance, if an operation yields 27, it will be lessened thusly: 27 mod 26 _ 1 This number speaks to the character B. This can be essentially considered as the letters in order wrapping from Z ! A.

I start by introducing, illustrating, and breaking down a portion of the better known traditional cryptographic frameworks:

Shift Cypher

The shift cypher is the simplest method of cryptography. It shapes a scrambled content string of the same length as the first message. The scrambled string seems scattered and ambiguous. The figure essentially maps every plain content letter to a letter a fixed separation ahead in the letters in order (wrapping from Z to A). Julius Caesar is known not utilized a shift figure with a movement estimation of 3 when trading messages with his military; subsequently, today this specific figure is known as a Caeser Cipher.

The define figure adds another measurement to the movement figure. Prior to the movement worth is included, the plain content character is duplicated by affixed coefficient. Every plain content character now maps to a different encoded character in the same character space, however the difference is not consistent among contiguous letters. The calculation is abridged as:PlainT ext i_ a + b mod 26 = EncryptedT ext I Where a is the coe_cient by which each character is multiplied, b is the shift value and I represents a character in the string.

Plain Text	H	E	L	L	O
	$\Downarrow 5x+9 \mod 26$				
Encrypted	S	D	M	M	B

Decryption

The decoding of an a_ne figure encryption requires the multiplicative opposite of a. Consequently, conceivable estimations of an are restricted to those delightful: gcd (a; 26) = 1 To unscramble, the multiplicative opposite is substituted for 1a.Example: The given specimen, y = 5x + 9 mod 26 is decoded by explaining for x: x =15(y 9)Where y is the encoded content character and x is the plain content character. In any case, since estimations in this

condition are mod 26, 21 is substituted for[20, p.14]. This is legitimate in light of the fact that 21 is the multiplicative opposite of 5 mod 26: 5 _ 21 _ 1 mod 26

In this way, x = 21y 189 mod 26. 32 Plugging in the encoded characters above (S; D; M; M; B) as y yields the first message HELLO.

The affine figure is marginally more secure than a basic movement figure in light of the fact that the movement esteem differs with every character. Be that as it may, the movement esteem for a specific character will dependably be the same. In this manner, if an outsider can decide only two characters in the first message, ordinarily done by recurrence investigation 4 , then the movement quality can be comprehended for in two conditions with two obscure variables. This is more secure than a movement figure, which just required learning one unique plain content character, yet was promptly made back the initial investment before PC innovation, so is no more utilized as a part of handy application .

VI. Cryptography & Data Compression

The security of interchanges and trade in a computerized age depends on the cutting edge incarnation of the old craft of codes and figures. Fundamental the introduction of current cryptography is a lot of entrancing arithmetic, some of which has been created for cryptographic applications, however a lot of which is taken from the traditional scientific standard. The essential objective of this book is to acquaint the peruser with an assortment of scientific points while all the while incorporating the arithmetic into a depiction of current open key cryptography [11,12].

It ought to be noted here that pressure must happen first; since a solid encryption technique wipes out examples and redundancies in the figure content, encoded _les have terrible pressure proportions.

In this way, Bruce Schneier suggests that clients take after these progressions in secure information exchange:

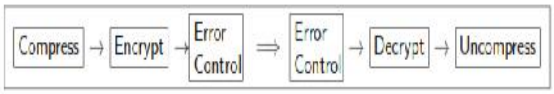

Figure 2: Data Compression and Cryptography together

VII. Conclusion

To apply this to cryptography, two individuals can transmit photons over a system and record their positions as coming through specific enraptured filters. What goes over the system is not as a matter of course secure, but rather what is recorded will be. On the off chance that the system is tapped, then the third pernicious onlooker is recording the photon's position also. The straightforward demonstration of this outsider watching the photon always shows signs of change the stream and the first sender and recipient will have the capacity to tell that the line is unreliable.

VIII. References

[1] Jackson, William. "Experts approve of new encryption standard." Government Computer news 16 Oct. 2000: 6. Academic OneFile. Web. 16 Nov. 2011.

[2] Jallad, Kahil, Jonathan Katz, Jena J. Lee, and Bruce Schneier. Implementation of Chosen-Cyphertext Attacks against PGP and GnuPG. Information Security Conference, 2002. PDF.

[3] Lv, Chuanfeng, and Qiangfu Zhao. "Integration of Data Compression and Cryptography: Another Way To Increase the Information Security." 21st International Conference on Advanced Networking and Applications Workshops/Symposia 2 (2007): 543-47. Print.

[4] Marshall, Dave. CS 421: Computer Network Security. Carroll College. Spring 2012. Lecture.

[5] Nelson, Mark. \LZW Data Compression." Dr. Dobb's Journal 1 Oct. 1989. Web. 19 Mar. 2012 http://marknelson.us/1989/10/01/lzw-data-compression/

[6] Nelson, Mark, and Jean-loup Gailly. The Data Compression Book. University of Bahrain: College of Applied Studies. PDF Web. 19 Mar. 2012.

http://sta_.uob.edu.bh/_les/781231507_____les/The-Data-Compression-Book-2ndedition.pdf

[7] Null, Linda, and Julia Lobur. Essentials of Computer Organization and Architecture. Sudbury, MA: Jones & Bartlett Learning, 2012. Print.

[8] R. P. Brent. An improved Monte Carlo factorization algorithm. BIT, 20(2):176–184, 1980.

[9] E. R. Canfield, P. Erd˝os, and C. Pomerance. On a problem of Oppenheim concerning "factorisatio numerorum". J. Number Theory, 17(1):1–28, 1983.

[10] J. W. S. Cassels. Lectures on Elliptic Curves, volume 24 of London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 1991.

[11] H. Cohen. A Course in Computational Algebraic Number Theory, volume 138 of Graduate Texts in Mathematics. Springer-Verlag, Berlin, 1993.

[12] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Ver- cauteren, editors. Handbook of Elliptic and Hyperelliptic Curve Cryptography. Discrete Mathematics and Its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[13] S. A. Cook. The complexity of theorem-proving procedures. In STOC '71: Proceedings of the Third Annual ACM Symposium on Theory of Computing, pages 151–158, New York, NY, USA, 1971. ACM.

[14] D. Coppersmith. Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm. Math. Comp., 62(205):333–350, 1994.

[15] D. Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Cryptology, 10(4):233–260, 1997.

[16] D. Coppersmith. Finding small solutions to small degree polynomials. In Cryptography and Lattices (Providence, RI, 2001), volume 2146 of Lecture Notes in Comput. Sci., pages 20–31. Springer, Berlin, 2001.

[17] R. Crandall and C. Pomerance. Prime Numbers. Springer-Verlag, New York, 2001.