International Journal of Innovation in Science and Mathematics
Volume 4, Issue 2, ISSN (Online): 2347–9051

Aryabhata and the Information Security

K. N. Shukla

***Abstract* – With a brief historical description of cryptology, symmetric and asymmetric cryptography are outlined, RSA algorithm is elaborated Aryabhata algorithm is explained to find the multiplicative inverse in a group that is of interest in cryptology, signal processing, coding and computer design.**

***Keywords* – Cryptology, Multiplicative Inverse, RSA Algorithm, Aryabhata Algorithm.**

I INTRODUCTION

As the information society evolves, one faces new threats on data security. More and more bungling are reported everyday during banking transactions through ATM. Governments, military, private enterprises, financial institutions, even an individual possess a great deal of information about their employees, business details, products, financial status, personal details stored in electronic form on the computers. This information is communicated across the networks electronically. Any breach of security may lead this confidential information falling in the wrong hands who may exploit the system and results into fraud, theft or information leak. Proper controls and their implementation in the information system from the beginning may reduce these risks to some extent. One of such controls is the cryptology which transforms the information unusable to the party not authorized to receive the information. Various cryptosystems are used for preventing leakage of information or unauthorized access. Nevertheless no cryptosystem can be fool proof. The history of cryptosystem is indeed an invention of new cipher methods and deciphers techniques which evolve a new area of study, known as cryptography. Cryptography is a science of information security. It deals with the construction of computer algorithm that overcomes the influence of adversaries which are related to various aspects of information security such as data confidentiality, network security. The word is derived from the Greek-Krypto meaning hidden. Modern cryptography is an interdisciplinary topics combining knowledge of mathematics, computer science and electrical engineering. It has applications in ATM, password and e-commerce.

There is a history of cryptography being used before the Christian era. The Roman ruler Julius Caesar (*100*BC-*44*BC) used a very simple cipher for secret communication between his army. This is a class of substitution cipher wherein a rule is to substitute each letter by another letter of the alphabet. He substituted each letter of the alphabet with a letter three points further along. Later any cipher that used this substitution concept for creation of a cipher alphabet was referred as a Caesarcipher [1]. Of all the substitution type ciphers, the Caesar cipher was the simplest to solve as it has only 25 possible combinations. The encryption can also be expressed by modular arithmetic. The letters of the alphabets are first represented by numbers with *A=0, B=1… Z=25*. The encryption of a letter x can be with shift n can be expressed mathematically as,

$$En(x) = (x + n) \bmod 26 \quad (1)$$

Decryption is performed similarly by,

$$Dn(x) = (x-n) \bmod 26 \quad (2)$$

The replacement remains the same throughout the message, so the cipher is classified as mono alphabetic substitution. The code can be easily decoded by the frequency analysis. In *2011*RajibKarim was convicted in the United Kingdom of terrorism offences after using Caesar cipher in communicating with Bangladesh Islamic activist to blow a British Airways plane [2].

One of the earliest descriptions of the text encryption by substitution code is also found in one of the chapters of Indian erotic manual Kama Sutra authored by Mallanga Vatsayan of 4th century AD, referred as the Vatsayanacipher or Kamsutra cipher [3]. The cipher involves randomly pairing letters so that each plain text letter gets substitution for its pair letter in the cipher text and vice versa. The purpose was to make women understand how to hide secret messages from prying eyes. The Devanagari Indian alphabet is divided into two halves to pair the letters.

अखघचजञनर	स य
कगङछझटम	ल षश

The other letters remain the same. Thus a text message कमल becomes अन र in the cipher text. The Kamasutra cipher can easily be decoded like the Caesar cipher by the frequency analysis. One of the most prominent mathematicians of ancient India of the 5th century was Aryabhata born in 3577 Kali, corresponding to 476 AD in Kusumpura, presently Patna of Bihar state of India. His mapping of the numbers to the Devanagari alphabets –36 consonants and 14 vowels is another example of the substitution code, see Kak[4]. The twenty five consonants letters from क to म are made to represent from 1 to 25, there maining 8 letters from य to ह represent (30, 40, 50, 60, 70, 80, 90, 100) and the 8 vowels अ to औ represent (100, 1002, ------ 1008) . This creates a notational value for the numbers as large as 10^{17}.Thus a code message-299792458 represents the text message, जल घघघन झसु भृसृ ख, where (जल) (घघघन) (झसु) (भृसृ) ख = (8+50) (4+20)(9+70)(90+9)2 and the letters are written from right to left.

Cryptography got importance during the two world wars. During the First World War both sides employed cipher techniques almost exclusively for tactical communications while code systems were still used mainly for high command and diplomatic communications. Although the field cipher systems such as the US signal crops cipher disc lacked sophistication; some complicated cipher systems were used for high level

communications by the end of the war. The most famous of these was the German ADFGVX fractionation cipher. Figure 1 presents the German Enigma machine working on the principle of electro-mechanical rotor device invented by a German engineer-Arthur Sicherbius [5, 6]. The machine worked on the principle that when an operator typed a message and scramble it by using rotors it displayed different letters of the alphabet. The receiver needed to know these exact setting of the rotors in order to decipher the message.

Fig. 1. Enigma machine

This system was so named because it used a 6×6 matrix to substitution encrypt the 26 letters of the alphabet and 10 digit into pairs of the symbols A, D, F, G, V and X, see Fig.2.

	A	D	F	G	V	X
A	S	U	B	J	E	C
D	T	A	D	F	G	H
F	I	K	L	M	N	O
G	P	Q	R	V	W	X
V	Y	Z	0	1	2	3
X	4	5	6	7	8	9

Fig . 2. ADFGVX fractionation cipher

The application of this cipher results into an intermediate cipher which is then put into a rectangular matrix and transposed to produce the final cipher for transmission. For example, the text message "Indian army" with this cipher can be written as,

FV DF FA DD FVDD GFFG VA

Thus the intermediate cipher can be put in a transposition matrix as

C	I	P	H	E	R
1	4	5	3	2	6
F	A	F	V	D	F
F	A	D	D	F	V
D	D	G	F	F	G

Fig. 3. Fractionation cipher for 'Indian Army'

The final cipher is therefore FDDFFVDFAADFDGFVG.

The greatest triumphs occurred when the three Polish cryptologists-Marian Rajeswki, Jerzy Rozycki and Henryk Zygalski working together succeeded in breaking the Enigma cipher [7]. The mechanical devices breaking the Enigma code worded cryptography distinguishes between two different approaches to cryptography-symmetric and asymmetric (or public key) mechanism. The defining property of the symmetric mechanism is that the sender and receiver use the same key for the secured communication. It work son simple operation like bit shift and is more efficient. Larger messages usually have to be split up before encryption, as this procedure requires an input of a fixed length. The symmetric algorithms are divided into two categories- stream ciphers and block ciphers. In stream ciphers, a character could be a bit or a byte (8 bits). In block ciphers, the plain texts are encrypted in bit groups which are called blocks. Stream ciphers are usually faster in hardware implementations than block ciphers, because the bits-or byte wise processing is better adapted to a hard ware solution.

II. DATA ENCRYPTION STANDARD (DES)

DES is the classic symmetric algorithm widely used throughout the world. It was developed at IBM as a result of a tender on the National Bureau of Standards (NBS, nowadays NIST) for a uniform encryption standard and was presented in 1976; see Diffe and Hellman [8]. NIST certifies every 5 year the DES algorithm. It was last certified in 1999 under the condition that its version-third would be used as no longer DES meets today's security threat. An Advanced Encryption Standard (AES) has succeeded DES. DES has a 64-bit block size and uses a 56-bit key during encryption; on the other hand AES has128-bit block size and has a provision of 128, 192 and 256 bit key during encryption.

Asymmetric Cryptography

It was assumed that the encryption process is undertaken with the same key as the decryption process, and that only the sender and the receiver possess the secret key. With the rapidly increasing number of participants and new applications beyond closed user groups, these drawbacks of symmetric cryptography concerning key handling and key storage become critical. These problems were overcome with the invention of public key cryptography. Any message (text, binary files or documents) that are encrypted by using the public key can only be decrypted by applying same algorithm but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the public key which is made freely available to anyone who might want to send a message. The private key is kept secret. For illustration, one may think of keeping a message in a box securing it with a padlock provided by the intended receiver. While any one who has such a padlock (public key) can lock the box (i.e. encrypt the message), only the receiver can open it by using the private key (i.e. decrypt the message). The most popular asymmetric cryptographic system is the RSA system named after its inventors-Ron Rivest, Adi Shamir and Leonard Adelman [9].

III. RSA ALGORITHMS

In RSA crypto system a user chooses a pair of prime numbers so large that factoring the product is beyond all computing capabilities. This is possible because testing for primes is easy as compared to factoring a product. The algorithm works as follows: Let a user takes two large primes, *p* and *q*, and compute their product $n=p* q$, where *n* is called modulus. The user then chooses a number, $e < n$ and with no common factors with *(p-1) (q-1)*, except1. Another number, d is then found; subject to the condition that *(e, d-1)* is divisible by *(p-1) (q-1)*.

Here "*e*" is called the public exponent; "*d*" is called the private exponent. The public key is therefore the pair of *n* and *e* while the private key is the pair of *n* and *d*. The factors of *n*, *p* and *q*, can either be kept secret with the private key or destroyed. Thus the message can be communicated as follows:

Let Ram receives a message from Sham. Ram distributes s public key pair and Sham composes a plain text, m, and then uses Ram's public key to encrypt the message and form the cipher text, c. c is the remainder left when m is raised to the power of e and divided by the modulus n.

$c=m^e \bmod n$ (where e and n are Ram's public key pair) (3)

Sham sends the cipher text, c, to Ram, who decrypts the cipher text and retrieves the plain text message, m. m is the remainder obtained when c is raised to the power of d and divided by n.

$$m=c^d \bmod n, \quad (4)$$

This process requires the private key, d, which cannot be intercepted by a third person. For example, let

$$p=5,\ q=11,\ n= p.\ q = 55.$$

The least common multiple (LCM) of *(p-1), (q-1)* is $20= 2^2 x\ 5$. Any key, *e*, not divisible by *2* and *5*will have a matching key, i.e. "e" must be relatively prime to LCM of *(p-1). (q-1)*.

Thus $e=7$ and the private key, *d* must satisfy,

$$(d-1) \bmod (p-1).\ (q - 1)=0,\ d=3. \quad (5)$$

Let the plain text message for communication is m=c=3 (third letter in alphabet), then the cipher text,

$$c=m.^e \bmod n = 2^7 \bmod 55=42. \quad (6)$$

Hence, the decrypted message is

$$m = c^d \bmod n = 42^3 \bmod 55= 3 \quad (7)$$

Thus we get third letter of the alphabet, C. In the above example, small primes are considered in which the factorization of *n* is simple. However, it is suggested to use strong primes, making their product extremely difficult to factorize even by advanced factoring techniques. The biggest advantage of the RSA cryptosystem is its security and convenience. It is part of the many official standards including internet.

IV. ARYABHATA ALGORITHMS

The RSA algorithm was based on the factorization of a large number. As seen above, in RSA algorithm, calculations are made modulo n, where n is a product of two large numbers p and q. Aryabhata presented a general solution to the linear indeterminate equation which may be adopted to find the multiplicative inverse in a group that is of interest in cryptology, signal processing, coding and computer design. He called the method as KUTTAKA (pulverizer) and is now referred as Aryabhata algorithms. The Kuttaka means a process of breaking into small pieces and thus it involves a recursive algorithm for writing the original factor in terms of smaller numbers. The algorithm is stated as follows:

Find a number, $x < d_1.d_2=n$, when divided by d_1 and d_2 leaves the residues x_1 and x_2, where x_1-x_2 = c and d_1 and d_2 are relatively prime!

In mathematical form, the problem is stated as below:

$$x \bmod d1=x1,$$
$$x \bmod d2=x2=c+x1. \quad (8)$$

The solution of the problem is described in the following verses of Aryabhatiya (Ganita, verse-32-33),

adhikāgra bhāghāram chindyāt ūnāgrabhāgahārena ।
śeṣa parasparasparabhaktam mati gunam agrāntare ksiptam II
adhaupari gunitam antyayuk nāgra cchedabhajite śesṣam।
adhikāgr accheda gunam dvicchdāgram adhikāgrayutam II

English translation of these verses with commentary is available in a text on the Aryabhatiya of Aryabhata by Clark [10], Shukla [11] as below:

"Divide the divisor corresponding to the greater remainder by the divisor corresponding to smaller remainder. (Discard the quotient). Divide the remainder obtained (and the divisor) by one another(until the number of the quotients of the mutual division is even and the final remainder is small enough). Multiply the final remainder by an optional number (मतिगुणम) and the product obtained add the difference of the remainders (corresponding to the greater and smaller divisors; then divide this sum by the last divisor of the mutual division. The optional number is to be so chosen that this division is exact. Now place the quotients of the mutual division one below the other in a column below them write the optional number and underneath it the quotient just obtained. Then reduce the chain of numbers which have been written down one below the other as follows: Multiply by the last but one number (in the bottom) the number just above it and then add the number just below it (and discard the lower number). (Repeat the process until there are only two numbers in the chain). Divide(the upper number) by the divisor corresponding to the smaller remainder, then multiply the remainder obtained by the divisor corresponding to the greater remainder, and then add the greater remainder: the result is the dwicchedgra (i.e. the number answering to the two divisors). (This is also the remainder corresponding to the divisor equal to the product of the two divisors)."

As an illustrative example, find a number, *x* which when divided by *60* gives a remainder *1*while by *137* gives a remainder *11*!

The problem reduces to finding an integer solution of the indeterminate equation,

$$137a+10=60b \quad (9)$$

As above the divisor*137* gives a greater remainder *11* as compared to the divisor *60*, we divide *137* by*60* and proceed as below:

60) 137 (2
120
17) 60 (3
51
9) 17 (1
9
8) 9 (1
8
1

The optional number (मतिगुणम), R is determined as

$$1*R-10=8 \rightarrow R=18. \quad (10)$$

The Aryabhata array is as below:

2	130*2+37=297=a;
3	3*37+19=130=b;
1	1*19+18=37;
1	1*18+1=19;
18	18
1	

Noting that *297* mod *137=23* and *130* mod *60=10*, we get *a=10* and *b=23* as simple solutions of the indeterminate equation. The required number, $x = 137\times10+11= 60\times23+1=1381$.Similar to the RSA algorithm, calculations are made modulo *x*, where *x* is a product of two large numbers d_1 and d_2 in the Aryabhata algorithm. The simplicity of Aryabhata method of solving the indeterminate equations is of paramount importance. The historians of mathematics have already recognized his brilliance and the cryptology communities are reassessing the method, in particular the factorization of large numbers for the development of RSA algorithm. The annual conference on RSA in 2006 selected Aryabhata algorithm as one of the themes for discussion.

REFERENCES

[1] Reinhard Wobst, Cryptology Unlocked, Wiley, p. 19, 2001, ISBN978-0-470-06064-3.
[2] WWW.BBC.com/ news/UK-12573824
[3] Simon Singh, The Code Book, Anchor Book, p.9, 1999, ISBN 0-385-49532-33.
[4] S.Kak, Aryabhata's Mathematics, RSA Conference, Sn Jose, Feb., 13-17, 2006.
[5] Arthur Scherbius, A Scherbius Ciphering Machine, US Patent no US1657411 A, 1928.
[6] WWW.BBC.co.uk/history/topics/engima,
[7] Kozaczuk Wladyslaw, Engima: How the German Machine CIPHER was broken and How it was Read by the Allied Forces in World War II, edited and translated by Christopher Rasparek Friedrick, MD University Publications of America, 1984, ISBN 0-89093-547-5
[8] W. Diffe, M.E. Hellman, Exhaustive Crypto analysis of the NBS Data Encryption Standard, Computer, 10 (6) 74-80, 1977; doi:10.1109/C-M1977.217750.
[9] R.Rivest, A.Shamir and L.Adelman, A Method for obtaining Digital Signatures and Public key, Crypto systems, Communications of the ACM, 21(2):120-124, 1978; doi:10.1145/359340-359342.
[10] W. E.Clark, 1930, The Aryabhatiya of Aryabhata: Translation with notes, The University of Chicago Press, Chicago, Illinois. 1930.
[11] K N Shukla, The linear indeterminate equation- a brief historical account, RBHM, Vol 15(30) 83-94, 2015.

AUTHOR'S PROFILE

K. N. Shukla holds PhD (1973) degree in Mathematics from the Banaras Hindu University, Varanasi. He has worked in Vikram Sarabhai Space Centre, Trivandrum (1974-2005), Karunya University, Coimbatore (2005-2009) and Gurgaon College of Engineering (2009-10). A recipient of Alexander von Humboldt Fellowship, he conducted researches in the University of Stuttgart, Munich and Darmstadt universities of Technology and University of Erlangen. He was a DAAD visiting Professor (2011) in the University of Applied Sciences, Rosenheim, Germany.
Email ID : kn_shukla@rediffmail.com