RESEARCHERID
THOMSON REUTERS

[Kumar, 5(4): April 2018]

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

APPLICATION OF GROUP THEORY TO PUBLIC KEY CRYPTOGRAPHY

Pankaj Kumar[1], Vijai Kumar[2], Neha Gupta[3]
Applied sciences and humanities, Ganga Technical Campus (India)

ABSTRACT

In the mid-1970s, Ronald Rivest, Adi Shamir, and Leonard Adleman Devised an ingenious method that permits each person who is to receive a secret message to tell publicly how to scramble messages sent to him or her. And even though the method used to scramble the message is known publicly, only the person for whom it is intended will be able to unscramble the message. The idea is based on the fact that there exist efficient methods for finding very large prime numbers and for multiplying large numbers, but no one knows an efficient algorithm for factoring large integers. The person who is to receive the message chooses a pair of large Primes p and q and chooses an integer e (called the encryption exponent) with 1<e<m, where m=lcm (p-1, q-1), such that e is relatively prime to m (any such e will do). This person calculates n= pq (n is called the key) and announces that a message M is to be sent to him or her publicly as Me mod n. Although e, n, and Me are available to everyone, only the person who knows how to factor n as pq will be able to decipher the message.

Keywords: *cryptography.*

I. INTRODUCTION

Abstract algebra is that branch of mathematics in which we study algebraic structures like groups, rings and fields and their properties in detail. The paper presented here shows the application of U groups to public key cryptography. In many situations there is a desire for security against authorized interpretation of coded data, the most obvious being military and diplomatic transmissions. The different TV channels we view on cable TV or dish TV also have a need to protect their television signals to local cable operators and satellite dish subscribers .

In the mid-1970s, Ron Rivest, Adi Shamir and Len adleman devised an ingenious method that permits each person who is to receive a secret message to publicly tell how to scramble messages sent to him or her. And even though the method used to scramble the message is known publicly, only the person for whom it is intended will be able to unscramble the message.

The algorithm involved in cryptography is explained below involving receiver and sender:-

Receiver

1. Pick very large primes p and q and compute $n = pq$.
2. Compute the least common multiple of $p - 1$ and $q - 1$; let us call it m.
3. Pick e relatively prime to m.
4. Find d such that ed mod $m = 1$.
5. Publicly announce n and e.

Sender

1. Convert the message to a string of digits.
2. Break up the message into uniform blocks of digits; call them $M_1, M_2, \ldots\ldots, M_k$
3. Check to see that the greatest common divisor of each Mi and n is 1. If not, n can be factored and our code is broken. (In practice, the primes p and q are so large that they exceed all M_i, so this step may be omitted.)
4. Calculate and send $R_i = M_i^e \ mod \ n$

ISSN 2348 – 8034
Impact Factor- 5.070

.

Receiver

1. For each received message *Ri*, calculate $R_i^d \mod n$.
2. Convert the string of digits back to a string of character

II. GROUP THEORY EXPLAINING THE WORKING OF ABOVE ALGORITHM

Well, we know that U (n) is isomorphic to U (p) direct sum U (q) which is isomorphic to Z_{p-1} direct sum Z_{q-1}. Thus, an element of the form x^m in U (n) corresponds under an isomorphism to one of the form (mx_1, mx_2) in Z_{p-1} direct sum Z_{q-1} . Since m is the least common multiple of p - 1 and q -1, we may write m = s(p - 1) and m = t(q -1) for some integers s and t. Then $(mx_1, mx_2) = (s(p - 1)x_1, t(q - 1)x_2) =(0, 0)$ in Z_{p-1} direct sum Z_{q-1}, and it follows that $x^m =1$ for all x in U(n). So, because each message M_i is an element of U(n) and e was chosen so that ed = 1 + km for some k, we have, modulo n,

$R_i^d =(M_i^e)^d = M_i^{ed}= M_i^{1+km} =M_i(M_i)^{mk} = M_i(M_i^m)^k = M_i$

III. CONCLUSION

Mathematics has played an important role in the development of civilizations, it is due to the mathematics only that humans devised computers, able to send rockets into space and even explored planets like mars. Even in our day to day life mathematics is involved but we hardly realises ,for example when we do online payment the programs involved in the security of the transaction are also based on mathematics.

But in reality mathematics is less related to applications and accounting than it is to philosophy. People think of mathematics as some kind of practical art but it is more of abstract in nature. We should not satisfy by application of mathematics only but continue to do work in pure maths because who knows the result or theorem proved today may have applications 500 years later.

REFERENCES

1. Contemporary abstract algebra by Joseph A Gallian