International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Shift Ciphers and RSA - Encryption Algorithm

Vivek Parkash

Assistant Professor of Mathematics, Dyal Singh College , Karnal (Haryana), India
Email: *lethal007[at]hotmail.com*

Abstract: ***With the advancement of era of technology, the comforts of our lives are the combined effects of risk of privacy and data security. It is quite challenging to maintain privacy of our data and messages. This is where Cryptography comes to our rescue. Basically it deals with the study of encrypting and decrypting data and information to prevent any unauthorized and illegal access. In this paper, shift cipher and RSA algorithm are discussed*.**

Keywords: Coding, Cryptography, Encryption, Decryption, plaintext

1. Terminology

Plaintext: Message in raw form without any coding effect.

Ciphertext: The transformed message after coding is applied.

Cipher: A cipher (or code) is a process of hiding or making the contents of the message invisible so that only the authorised person reads and understands the message. We can say that cipher is an encryption algorithm.

Encryption: The process of converting a plaintext (Message in raw form) to cipher text (Coded message) using a cipher is known as encryption.

Decryption: Converting cipher text back to plaintext, is known as decryption.

Cryptography: The study of encrypting and decrypting messages is known as cryptography.

Greatest Common Divisor: Let a and b are positive integers. The greatest common divisor of 'a' and 'b' is largest positive integer 'c 'such that c divides both a and b.

And this Greatest Common Divisor is a unique number and we write as (a,b)=c

For example, we have two integers as 3 and 7. Then only positive integer that divides both 3 and 7 is 1. So, Greatest Common Divisor of 3 and 7 is 1 and we write as (3,7)=1.

Congruent Modulo: We say 'r' and 's' are congruent modulo m if m divides r-s.
For example, 17 and 3 are congruent modulo 2 as 2 divides 17-3=14

Asymmetric encryption: This is also known as Public Key Encryption Algorithm. Here the person sending the message and the person receiving the message use two different keys for encryption and decryption. The Public key is for encrypting message and the secret key for decrypting the message. The encrypted message can be decrypted only if a person has secret key.

Method of Shift Ciphers:
It is quite useful way of encrypting the messages. Let us see how it works:
Here, we shift or displace the letter A some positions to the right/left, and start the alphabet from there, wrapping around when we get to Z. The way in which the shifted alphabet lines up with the original sequence of alphabets is the cipher. For example, a three places shift appears as

Plain Text	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher text	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Suppose "TOM" sends the following message to "HARRY" :
'HAVE YOU GOT WHAT YOU WANTED'

Then the cipher text corresponding to this message is written as :

'EXSB VLR DLQ TEXQ VLR TXKQBA'

Now "HARRY" replies with the message:
'L DP VWLOO QUBLQJ WR JHW'. Then to decrypt this message, "TOM" just needs to swap the roles of above list of alphabets as:

Cipher text	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Plain Text	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Therefore, the decrypted message is:
'I AM STILL TRYING TO GET'
This is how shift cipher algorithm works.
Now, I am discussing RSA Algorithm which is an asymmetric encryption.

RSA Algorithm:
RSA is a public-key encryption algorithm, and got its name after its name of its inventors Rivest, Shamir and Adelman.
RSA is an asymmetric cryptographic algorithm. Block cipher concept is the basis of this algorithm thus converting

plain text into ciphertext and other way round at the receiver's end.

Using RSA algorithm involves the following steps:

1) Take two primes as a and b where a not equal to b.
2) Calculate r= a*b and s= (a-1)*(b-1)
3) Choose number k: Such that k is less than s such that G.C.D. of k and s=1
4) Find number f such that (kf-1) is exactly divisible by 2.
5) Keys are generated using r, f, and k
6) Encryption process
   c=p pow(k) mod r
   (where p is plain text and c is ciphertext)
7) Decryption process
   p= c pow(f) mod r
8) Public key is shared and the private key is hidden.
   (k, r) is the public key used for encryption. (f, r) is the private key used for decryption.

Let us describe the algorithm with the help of following example:

Let us take a=3 and b=11. Then r=a*b=3*11=33
And s=(a-1)*(b-1)=2*10=20. Now choose k such that k<s and (k,s)=1.
k can have values like 3,7,9,11,13,17,19. So ,we can choose k=7.
Now find out f so that 2 divides (7*f-1). We can take f=3.
Now the public key is (k,r)=(7,33)
And the private key is (f,r)=(3,33)

Now consider the plain text p=2 which is to be encrypted.

Then using c=p pow(k) mod r i.e. c= 2 pow(7) mod 33=29
and if we use p= c pow(f) mod r i.e. p=29 pow(3)mod33=2

Thus we see that RSA algorithm plays its role beautifully in encrypting and decrypting data.

When we encrypt a message with the public key, it is ensured that the message's confidentiality and authenticity is not challenged as no one else is able to decrypt it without knowing the private key.

References

[1] Rivest, R., Shamir, A., & Adleman, a. L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM , 120- 126.
[2] Diffie, W., and Hellman, M. New directions in cryptography. IEEE Trans. Inform. Theory IT-22, (Nov. 1976), 644-654
[3] Niven, I., and Zuckerman, H.S. An Introduction to the Theory of Numbers. Wiley, New York, 1972.
[4] Rabin, M.O., Probabilistic algorithms. In Algorithms and Complexity, J. F. Traub, Ed., Academic Press, New York, 1976, pp. 21-40