iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** III **Month of publication:** March 2020

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue III Mar 2020- Available at www.ijraset.com

Design of Public and Private Key using Inverse Theorem

Agnes Ahalya. A[1], Janet Silviya. J[2]
[1, 2]*Computer Science Engineering, Loyola-ICAM College of Engineering and Technology*

***Abstract:** This study shows the design of a new public-private key design using mathematical functions that can be used for image encryption. The input to this key is an image which is the actual private key of the receiver and the public key is generated from this image. The basis of this public-private key design is the inverse theorem.*
***Keywords:** Inverse theorem, image encryption, mathematical function, private-key, public-key.*

I. INTRODUCTION

Public key cryptography consists of public keys that are distributed to a large number of users and private keys are known only to the user. If the public key is unique that is used identifying a user then it is known public authentication key. The working of public-key cryptography will be like encrypting with the public key of the receiver and decrypting with his/her private key. Public key cryptography is also known as asymmetric cryptography. RSA, Diffie Hellman key exchange algorithm, ElGamal falls under asymmetric cryptography where key design is based on log, mod and other algorithm primitives are based on prime numbers, polynomials. This study explains the design of the key using functions and theorems related to it.

II. DESIGN OF KEY

The traditional way of designing an asymmetric key includes two important components; the public and private key. While the public key is used by the sender for encryption, the private key deciphers the message during process. In this work, a novel procedure for public-key encryption and private key decryption is developed

A. Design of Private key

Any image of type jpg, gif, png and other image extensions can be used for generating the private key. Once the image selected by the user, the image is converted to byte format. The byte value ranges from -128 to 127. The user has the independence to choose his/her seed image and then mark it is as his/her private key.

Fig. 1. Sample image chosen as private key

Fig. 2. Byte array of the image

B. Design of Public key

Once the private key is designated by the user, it paves the way for the design of the public key. A monomial function which is both continuous and differentiable is selected by the receiver and the output of the private key generation module is passed into this function. The function can be selected with the aid of the MatLab code or manually. The value returned by this function forms the public key.

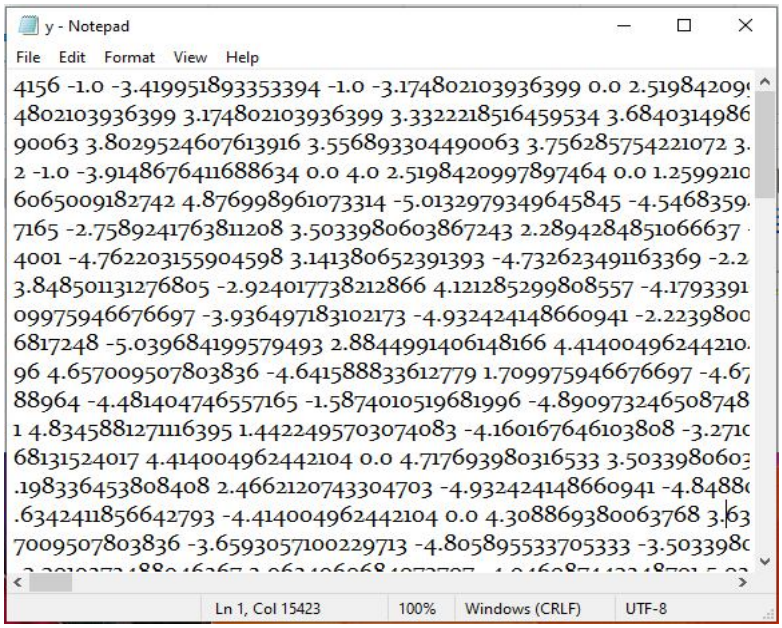


Fig. 3. Public key generated from the private key

The continuous differentiable function used her is

$Y_i=(X_i)^{\wedge} \text{ frac } \{1\}\{3\}$

where X_i is byte of private key

C. Inverse Theorem

The basis of this key generation is inverse theorem. The statement of the theorem goes as

If ‘f’ is a continuously differentiable function with nonzero derivative at the point ‘a’; then ‘f’ is invertible in a neighbourhood of ‘a’, the inverse is continuously differentiable, and the derivative of the inverse function at ‘b=f (a)’ is the reciprocal of the derivative of ‘f’ at ‘a’:

$$\{f^{\wedge} \{-1\}\}'(b) =\text{frac } \{1\}\{\{f\}'(a)\}$$

D. Public vs Private key Manipulation

The public undergoes $\{f^{\wedge} \{-1\}\}'(Y)$ transformation and XORed with the secret image and transferred to the receiver through a secure channel. The receiver transforms $\text{frac } \{1\}\{\{f\}'(X)\}$ and XORed with encrypted to obtain the original secret image. For example the transformation is given as $Yi=(Xi)^{\wedge} \text{ frac } \{1\}\{3\}$. The $\{f^{\wedge} \{-1\}\}'(Y)$ is defined as function $3*(Yi^{\wedge}2)$. The function should be passed through a secure channel agreement like the exchange of ‘p’(prime number) in Diffie Hellman.

On encryption side, Yi after passing through $\{f^{\wedge} \{-1\}\}'(Y)$ is then XORed with bytes of the secret image.

Fig. 4. Secret image

Fig. 5. Secret image value

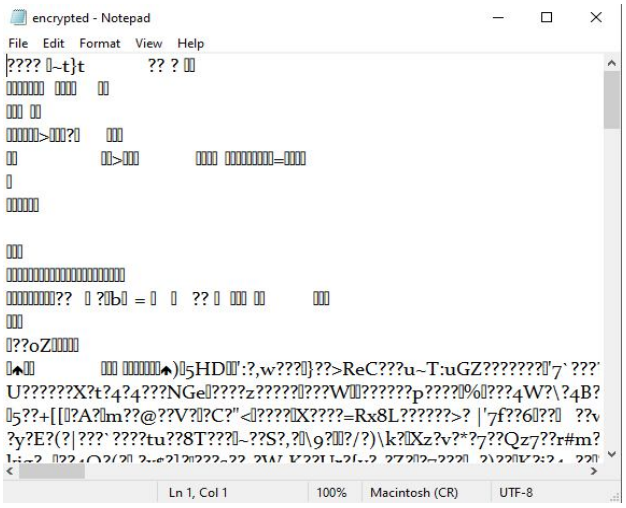


Fig. 6. Encrypted image value

E. Performance Metrics

Accuracy is the calculation of similarity between the original image and the decrypted image. SSIM (Structural Similarity Index) is calculated to determine accuracy. The SSIM value was found to be 1.00 stating that accuracy is 100%.

Fig. 7. The result of SSIM

III. CONCLUSIONS

The public key mechanism has been proposed and been tested. The encryption process is done with the public key and decryption process with the private key. The accuracy has been tested and results were favourable.

IV. ACKNOWLEDGMENT

We like to thank Loyola-ICAM College of Engineering and Technology for their constant support and we would also like to extend our gratitude to Santa Maria Matric. Hr. School for allowing us to test this public key design as part of the ICE algorithm on their official website.

REFERENCES

[1] Leihong Zhang , Xiao Yuan , Kaimin Wang , Dawei Zhang, "Multiple-Image Encryption Mechanism Based on Ghost Imaging and Public Key Cryptography", IEEE Photonics Journal, Volume 11, Number 4, August 2019.

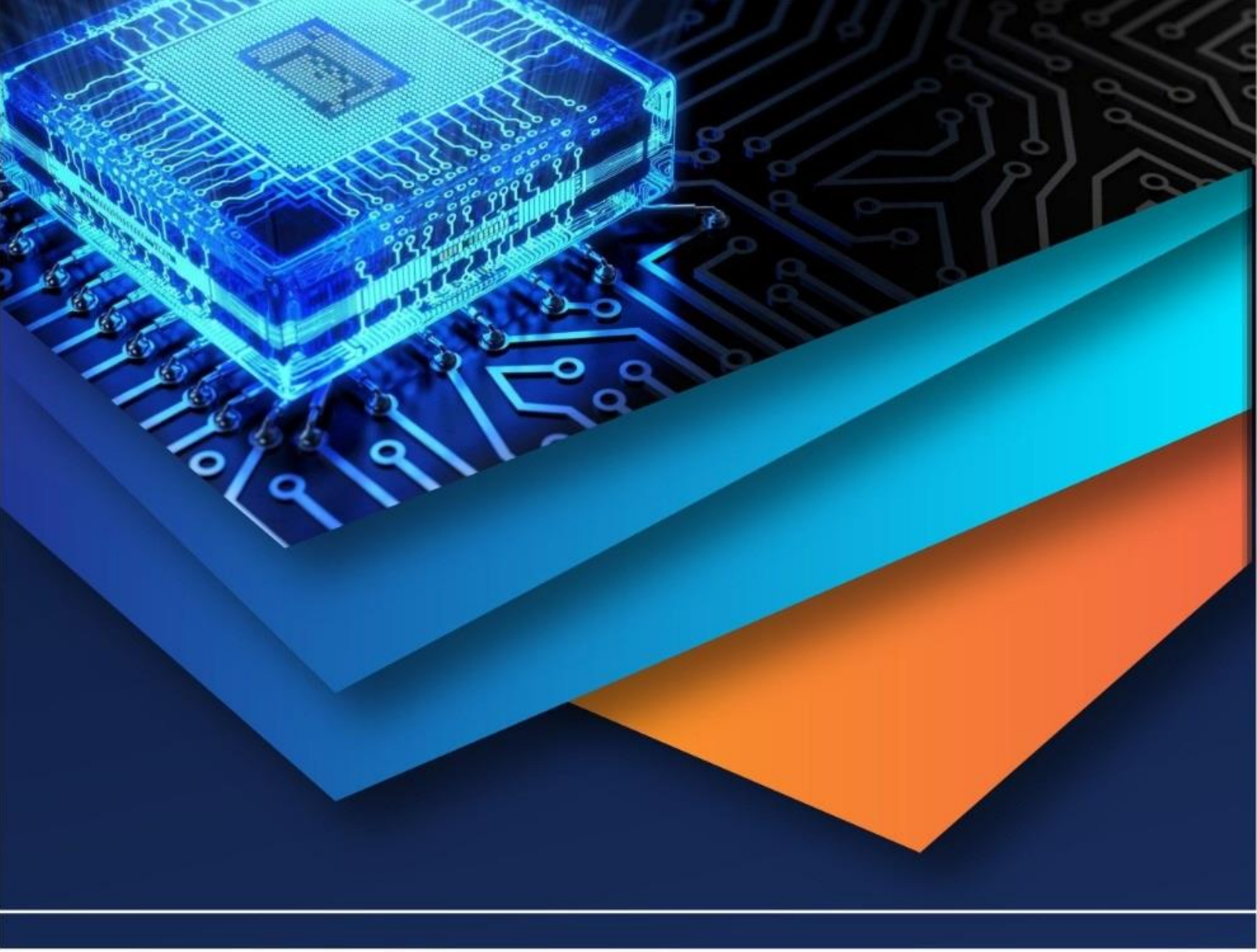
[2] Eduardo Ochoa-Jiménez , Luis Rivera-Zamarripa , Nareli Cruz-Cortés , Francisco Rodríguez-Henríquez , "Implementation of RSA Signatures on GPU and CPU Architectures",on IEEE Access published January 3, 2020.

[3] Houzhen Wang, Huanguo Zhang, Shaowu Mao, Wanqing Wu, and Liqiang Zhang," New Public-Key Cryptosystem Based on the Morphism of Polynomials Problem", Tsinghua Science And Technology ISSNll1007-0214ll06/11llpp302–311 Volume 21, Number 3, June 2016.

[4] Jaihui Chen∗ , Chik How Tan, and Xiaoyu Li.," Practical Cryptanalysis of a Public Key Cryptosystem Based on the Morphism of Polynomials Problem", ISSN 1007-0214 04/10 pp 671–679 DOI: 10.26599 / TST.2018.9010028 Volume 23, Number 6, December 2018.

[5] Xiaoqiang Zhang And Xuesong Wang," Digital Image Encryption Algorithm Based on Elliptic Curve Public Cryptosystem", on IEEE Access published December 18, 2018.

[6] Roayat Ismail Abdelfatah," Secure Image Transmission Using Chaotic-Enhanced Elliptic Curve Cryptography", on IEEE Access published January 7, 2020.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY