ชื่องาน: The Improving Decryption Process of RSA by Choosing New Private Key
วารสาร/งานประชุมวิชาการ: International Conference on Information Technology and Electrical Engineering
ผู้เขียน: ผศ.ดร.กฤษณพงศ์ สมสุข
ระดับ: นานาชาติ
ปี: 2016
สถานะผู้เขียน: ผู้เขียนหลัก
บทคัดย่อ: -

Abstract:

RSA is the best well – known and the most widelyused of public key cryptosystem. The advantage of this algorithm is that the senders who have the public key and the receivers whohave private key can communicate each other via the unsecured channel secretly. However, the processes of RSA have to take very great computation cost especially in the decryption process. In this paper, the improving decryption process of RSA, is called New Private Key of RSA (d-RSA),is proposed to reduce the computation cost of the decryption process. The key is to find the new private key, which has low Hamming weight while the values of public key and modulus are not changed. With the low Hamming weight, it implies that the computation cost of decryption process of d-RSA is certainly reduced when compared with the same process which has the higher Hamming weight in RSA. Furthermore, it implies that not only the private key which is the inverse of public key modulo Euler function but also the other keys that can decrypt the ciphertext. In addition, with reducing computation cost, the proposed method is the better choice when low power devices are chosen to decrypt the ciphertext.