# ABSTRAK

**Bella Kusumawati, 2018. *Kriptosistem Kunci Publik LUC serta Implementasinya pada Program Lazarus*. Skripsi. Program Studi Pendidikan Matematika, Jurusan Pendidikan Matematika dan Ilmu Pengetahuan Alam, Falkutas Keguruan dan Ilmu Pendidikan, Universitas Sanata Dharma.**

Penelitian ini bertujuan untuk mengkaji kriptosistem kunci publik LUC sebagai perkembangan dari kriptosistem kunci publik RSA serta implementasinya pada program Lazarus. Penelitian diawali dengan membahas mengenai kriptosistem kunci publik RSA. Selanjutnya dibahas mengenai tanda tangan digital serta skema tanda tangan menggunakan algoritma RSA. Langkah berikutnya akan dibahas mengenai salah satu kelemahan pada algoritma RSA yakni penipuan tanda tangan RSA menggunakan *adaptive chosen message attack*. Serangan ini mungkin terjadi karena proses enkripsi dan dekripsi pada algoritma RSA menggunakan perkalian bilangan asli.

Berdasarkan kelemahan dari algoritma RSA terhadap *adaptive chosen message attack*, maka dikembangkan sebuah kriptosistem kunci publik yakni kriptosistem LUC. Kriptosistem LUC menggunakan fungsi Lucas dalam proses enkripsi dan dekripsinya. Sehingga dianggap dapat bertahan dari serangan *adaptive chosen message attack*.Selain itu peneliti membuat simulasi sederhana dari algoritma LUC dengan menggunakan program Lazarus.

**Kata Kunci** : Kriptosistem, Kriptosistem Kunci Publik LUC, Program Lazarus

# ABSTRACT

**Bella Kusumawati, 2018. *LUC Public Key Cryposystem and its Implementation in Lazarus Program*. Thesis. Mathematic Education Study Program, Mathematic and Science Education Departement, Faculty of Teacher Training and Education, Sanata Dharma University, Yogyakarta.**

This research aims to examine the LUC public key cryptosystem as the development of the RSA public key cryptosystem and also implementation in Lazarus program. The research is begins by discussing RSA public key cryptosystem. Further, discussed about digital signatures and signature schemes using the RSA algorithm. The next step will be discussed about one of the weaknesses in RSA algorithm is the signature forging using adaptive chosen message attack. This attack may occur because the encryption and decryption process of the RSA algorithm uses the multiplication of natural numbers.

Based on the weakness of the RSA algorithm towards adaptive chosen message attack, then developed a public key cryptosystem that is LUC cryptosystem. The LUC cryptosystem uses the Lucas function in its encryption and decryption process. Therefore it is considered to survive from an adaptive chosen message attack. In addition, the researchers made a simple simulation of the LUC algorithm using Lazarus program.

**Keyword**: Cryptosystem, LUC Public Key Cryptosystem, Program Lazarus.