INTEGRASI KAEDAH PEMBAHAGIAN BERTERUSAN TERHINGGA DAN ALGORITMA EUKLID DALAM KAEDAH MAMPATAN KRIPTO BAGI MENINGKATKAN KECEKAPAN ENKRIPSI-DEKRIPSI SISTEMKRIPTO TAK SIMETRIK

ARIF MANDANGAN
PROF. MADYA DR. ABDULLAH BADE
ASDALIFAH TALIBE

LAPORAN AKHIR GERAN PENYELIDIKAN

RAG0001-SG-2012

UNIVERSITI MALAYSIA SABAH

ABSTRAK

Demi membekalkan tahap keselamatan yang baik, sistemkripto moden perlu menggunakan nombor-nombor besar dan dilaksanakan menggunakan operasi-operasi matematik yang rumit. Natijahnya, kecekapan menjadi isu besar dalam kriptografi. Dengan menggunakan parameter-parameter yang bersesuaian, beberapa sistemkripto tak simetri adalah dipercayai mampu untuk membekalkan suatu tahap keselamatan yang baik. Sejak itu, matlamat untuk membangunkan suatu mekanise bagi melajukan proses-proses enkripsi-dekripsi sistemkripto tak simetrik tanpa mengubah algoritma-algoritma enkripsi dan dekripsi yang asal menjadi suatu pertimbangan yang besar. Matlamat kajian ini adalah untuk mencadangkan integrasi suatu teknik mampatan yang dinamakan sebagai teknik CFEA ke dalam sistemkripto tak simetri yang terkenal seperti sistemkripto RSA dan ElGamal. Teknik Mampatan-CFEA merupakan gabungan Pecahan Berterusan dan Agoritma Euklid yang mampu mengurangkan bilangan teks biasa dan teks sifer sebelum proses-proses enkripsi dan dekripsi dilaksanakan.

ABSTRACT

In order to provide good level of security, modern cryptosystems need to implement large numbers and complicated mathematical operations. As a consequence, efficiency becomes a new major issue in cryptography. By using proper parameters, some of established asymmetric cryptosystems are believed to be able to provide a good level of security. Since that, aim to develop a mechanism to accelerate encryption and decryption processes of asymmetric cryptosystem without altering their original encryption and decryption algorithms become a big consideration. The aim of this study is to propose the integration of a technique that named as CFEA technique into some established asymmetric key cryptosystem such as RSA and El-Gamal cryptosystems. CFEA-technique is a combination of Continued Fraction and Euclidean Algorithm (CFEA) which is able to reduce the number of plaintext and ciphertext prior the encryption and decryption processes.