

# IMPLEMENTASI ALGORITMA BC3 DAN RSA DALAM SISTEM KEAMANAN PESAN *ELECTRONIC MAIL* (EMAIL)

Oleh

Dyah Ayu Kusumawardhani, dyah.a@student.upi.edu

1206140

## ABSTRAK

Teknologi informasi yang berkembang saat ini, sejalan dengan peningkatan arus pengiriman dan penerimaan data. Salah satu perputaran data saat ini terdapat pada *electronic mail* (email). Terlihat pada pendaftaran akun di berbagai situs, jejaring sosial, *messenger*, dan sebagainya mengharuskan penggunanya memiliki akun email. Namun, penggunaan *password* yang sama untuk semua akun *online* masih ditemukan. Hal tersebut membuka peluang untuk meretas email pengguna dari berbagai jejaring sosial yang pengguna daftarkan. Sehingga data pada email dikhawatirkan dapat disalahgunakan dan tersebar luas. Oleh karena itu, dibutuhkan algoritma untuk mengamankan data dan informasi yang kita kirim melalui email. Peneliti menggunakan algoritma kriptografi simetri dan asimetri, yaitu Algoritma BC3 dan algoritma RSA. Algoritma BC3 merupakan algoritma kriptografi simetri yang dikembangkan dengan dua pertimbangan: ketahanan pada berbagai serangan dan efisiensi dalam implementasinya. Algoritma RSA dapat menjadi salah satu solusi untuk pendistribusian kunci dari BC3. Keunggulan algoritma RSA terletak pada keamanan yang lebih tinggi dibandingkan algoritma simetris, namun membutuhkan waktu komputasi yang lebih lama. Algoritma BC3 akan digunakan sebagai pengamanan isi pesan email, sedangkan algoritma RSA akan digunakan untuk pengamanan kunci dari algoritma BC3. Hasil penelitian ini menyimpulkan bahwa kombinasi dua algoritma ini dapat diimplementasikan pada pesan email dan memenuhi dua tujuan kriptografi yaitu kerahasiaan dan integritas data. Selain itu dilakukan juga pengujian terhadap lama waktu proses enkripsi dan dekripsi. Berdasarkan hasil pengujian tersebut disimpulkan bahwa kecepatan proses enkripsi dan dekripsi dipengaruhi panjang pesan. Adapun rata-rata kecepatan proses enkripsi yaitu 8876.5138 bit/detik. Sedangkan untuk proses dekripsi memiliki rata-rata kecepatan proses dekripsi 13775.3 bit/detik.

**Kata Kunci:** BC3, RSA, Email.

**IMPLEMENTATION OF BC3 AND RSA ALGORITHM  
IN AN *ELECTRONIC MAIL (EMAIL)* MESSAGE SECURITY SYSTEM**

By

Dyah Ayu Kusumwardhani, dyah.a@student.upi.edu

1206140

**ABSTRACT**

The recently developing technology information is in accordance with sending and receiving data stream. One of currently data turnaround is contained in electronic mail (email). We can see at various sites, social network, messengers and its kind that oblige users to create email account. Unfortunately, we still find the use of same password on different accounts. This creates opportunities for hackers to abuse of user email used at various registered social networks. As a result, personal data contained in emails may spread and abused in publik sphere. Therefore, we need algorithm to protect data and information we send through email. Research scientist uses symmetrical and asymmetrical cryptography algorithm, that is BC3 algorithm and RSA algorithm. BC3 algorithm is a symmetrical cryptography algorithm developed by two reasons, resistance to robustness and efficiency in its implementation. Meanwhile, RSA algorithm can be a solution for the distribution of the secret-key BC3 algorithm. The excellence of RSA algorithm relies on better security than BC3 algorithm but it needs a longer time computation process. BC3 algorithm can be used to protect email message's text content while RSA algorithm can be used to protect the secret-key BC3 algorithm. The research result concludes that combination of the two algorithms can be implemented on email messages based on two cryptography goals, that is confidentiality and data integrity. In addition, it can be used to examine encryption and decryption time performance. Based on the research result, it can also be concluded that the speed of encryption and decryption time depends on the length of email message. As for average speed of encryption process is 8876.5138 bits per second. While average speed of desryption process is 13775.3 bits per second.

***Keyword : BC3, RSA, Email***