# Application of Chinese Remainder Theorem to Find The Messages Sent in Broadcast

**Authors :** Ayubi Wirara, Ardya Suryadinata

**Abstract :** Improper application of the RSA algorithm scheme can cause vulnerability to attacks. The attack utilizes the relationship between broadcast messages sent to the user with some fixed polynomial functions that belong to each user. Scheme attacks carried out by applying the Chinese Remainder Theorem to obtain a general polynomial equation with the same modulus. The formation of the general polynomial becomes a first step to get back the original message. Furthermore, to solve these equations can use Coppersmith's theorem.

**Keywords :** RSA algorithm, broadcast message, Chinese Remainder Theorem, Coppersmith’s theorem

**Conference Title :** ICAM 2014 : International Conference on Applied Mathematics

**Conference Location :** Bali, Indonesia

**Conference Dates :** October 09-10, 2014

Open Science Index, Mathematical and Computational Sciences Vol:8, No:10, 2014 publications.waset.org/abstracts/9543.pdf