GCD attack on the LUC4 cryptosystem.

Abstract

LUC4 cryptosystem is derived from a fourth order linear recurrence relation and is based on the Lucas function. This cryptosystem is analogous to the RSA, LUC and LUC3 cryptosystems. Therefore, the security for this cryptosystem is similar to the RSA cryptosystem. This paper reports an investigation in to the GCD attack on the LUC4 cryptosystem and GCD attack is one of the polynomial attacks on LUC4 cryptosystem. The GCD attack can succeed if two messages differ only from a known fixed value Δ and are RSA-encrypted under same RSA-modulus n.

Keyword: GCD attack; LUC cryptosystem; Polynomial attack.