Abstract

In this paper we propose a mechanism to develop a lightweight encryption technique. We encrypt hierarchical single key-lock access control mechanism key by encoding key (key number). Key number is derived using Chinese reminder theorem and tribes of Gaussian or rational Farey fractions are used to encode the key number. The advantages of the proposed mechanism are i) no decoding overhead as access rights are derived without decoding the encoded the key number, ii) no need to derive the key number for already existing files. Hence this method secures access control system by encoding the key number and acts as a thin layer of security; however the performance of retrieval system remains unchanged.

Reference

**Index Terms**

Computer Science

Information Security

**Key words**

Light weight encryption

Farey fractions

Access control mechanism

Chinese remainder theorem