ICIBACC2014

INTERNATIONAL CONFERENCE ON ISLAMIC BUSINESS, ART, CULTURE & COMMUNICATION

"Addressing Challenges & Sustaining Excellence in a Globalised Malay & Islamic World"

DEPARTMENT OF
RESEARCH & INDUSTRIAL LINKAGES
UNIVERSITI TEKNOLOGI MARA, MELAKA

KEMENTERIAN PENDIDIKAN MALAYSIA

AKEPT HIGHER EDUCATION LEADERSHIP ACADEMY
AKADEMI KEPEMIMPINAN PENGAJIAN TINGGI

UNIVERSITI TEKNOLOGI MARA

sponsored by
karangkraf
Asian Geos Sdn Bhd
Suria Mekar Sdn Bhd

DEVELOPMENT OF ETHNO-MATHEMATICS OF AL-QUR'AN, AL HADITH AND JAWI SCRIPTS FOR COMPUTER SECURITY

A.Faizul Shamsudin[1], Mohammad Alinor [2]

Kolej Universiti Islam Sultan Azlan Shah[1]
Akademi Kajian Ketammadunan[2]
Kuala Kangsar, Kolej Darul Hikmah Perak Darul Ridzuan, Malaysia
Kajang, Selangor, Malaysia
afaizuls@kuisas.edu.my asasi@kesturi.net

Abstract

Personal data is constantly being compromised not just by the normal identity thefts but also abnormal attacks. A continuous search on new paradigm of non-parametric cryptographs led to the discovery of ethno-mathematics for substitution block- cipher boxes. The objects based on extracted Al-Qur'an and Al-Hadith symbols by use of ethno-mathematical functions. The extracted objects were insufficient to build the 256 bit block-ciphers. The development of expanding objects from Jawi Scripts may fill the gap for a 256 bit block-cipher. Initial tests for algebraic attacks indicate Ethno-Mathematical Block Cipher resistance to be better than the random parametric Khazad and Annubis Block Ciphers.

Keywords: cryptographs; ethno-mathematics; block- cipher;