# Bahim

## A Provably-secure Symmetric Cipher

Rajululkahf[1]

April 5, 2022

## Abstract

Bahim is a symmetric cipher that uses a pre-shared key to encrypt cleartexts into ciphertexts. If an $n$-bits long key is chosen uniformly and randomly, then no cryptanalysis can reduce key's search space below $2^n$ possibilities.

## 1 Bahim

[1]Author's e-mail: {author's name}@protonmail.com.