سیویلیکا - ناشر تخصصی مقالات کنفرانس ها و ژورنال ها
گواهی ثبت مقاله در سیویلیکا
CIVILICA.com

We Respect the Science
CIVILICA

عنوان مقاله:

Design and Implementation of a New Hmac Algorithms Based on New Hash Functions Like Blake and Grostl to Increase Security

محل انتشار:

هفتمین کنفرانس بین المللی اقتصاد و مدیریت (سال: 1395)

تعداد صفحات اصل مقاله: 8

نویسندگان:

Farzaneh Vosoughi Rahbari - *Young Researchers and Elite Club, Sirjan Branch, Islamic Azad University, Sirjan, Iran*

Hamid Mirvazir - *Assistant Professor of computer Engineering Department of computer Engineering, Shahid BahounarUniversity of Kerman, Kerman, Iran*

خلاصه مقاله:

Given the growing demand for digital data security, the most importantmatter for specialists is the way of protection and data encryption.Encrypting the hashed message authentication code (HMAC) includedhash function and an encryption secured key that is one of the mostuseful and important tools in credit issues, cryptographic and use ofhash functions that can be used to verify the data and messageauthentication simultaneously. Due to the attacks on hash functionssuch as MD5 and SHA-1, nowadays the functions are not secure todesign HMAC. This article deals with the implementation of HMAC byusing the new hash functions Keccak, Blake and Grostl in the 256-bitversion. The Implementation of HMAC, Keccak function comparedwith other hash functions show that there is a relative improvement intesting the avalanche effect, balance and distortion parameters andResistance to collision attacks. .Likewise, this implementation needs lesstime so that the function would be more suitable for implementation ofHMAC

کلمات کلیدی:

hash functions, authentication code, the hashed message authentication code (HMAC), distortion parameters

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/535947