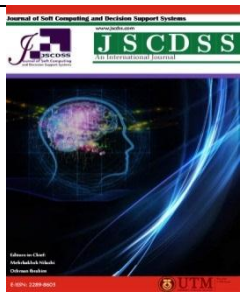
An International Journal
JSCDSS
http://www.jscdss.com
Vol.4 No.1 February 2017: 7-15
Article history:
Accepted 28 February 2017
Published online 28 February 2017

Journal of Soft Computing and Decision Support Systems



E-ISSN: 2289-8603

Encryption and Decryption Analysis of the RSA Digital Signature Based on MD5 and SHA Hash Functions Using Strong Prime

Abdelmajid Hassan Mansour [1,*]
[1] University of Jeddah, Faculty of Computers and Information Technology, Department of Information Technology, Khulais, Jeddah, Saudi Arabia, 21921

*** Corresponding author email address**: majidemam@gmail.com

Abstract

RSA digital signature is the most common public key crypto system that used widely on data security. The encryption and decryption time computation of the signature generation and verification is still a big problem an important issue that challenging the RSA security. This paper analyses the encryption and decryption time of the RSA Digital Signature based on the hash functions MD5, SHA-160, SHA-256, and SHA-512. The private key and public key of the RSA generated by using the "Strong prime", then compare it with the original RSA method. The main goal of the proposed scheme is to optimize and speed up the process of encrypting and decrypting time on a variable length of message, and different hash functions. This will overcome the problem of processing time and computational overheads of the RSA digital signature system.

Keywords: RSA digital signature, Private key, Public key, Encryption, Decryption, Strong prime, Hash function, Message digest.

1. Introduction

A digital signature is a cryptographic algorithm which includes the process of signature generation and signature verification. A signer uses the generation process to create a digital signature on the data, and the verifier verifies the authenticity of the signature by using the verification process. The private key is used to generate the signature and must remain secret, while the public key is on the verification process (Bhala et al., 2011). Digital signatures are widely used in various applications such as electronic commerce, banks, distributing software, and in detecting forgery or tampering. They are corresponds of handwritten signatures which can be transmitted within a computer network. Only the signer of the message can make the signature, and the other people can recognize easily as belonging to the signer. The digital signature has three types of services such as (Gola et al., 2014):

1.1 Authentication is the process of verifying the messages received is come from valid source.

1.2 Message integrity is process of authenticating the contents at the signature time and it did not altered during transfer.

1.3 Non-repudiation means the signer cannot claim they did not signed the message.

The digital signature provides an intermediary of integrity checking. This is done in order to provide assurance for the verifier that the data was in real was sent by the assumed entity (Ali, 2015). In the Digital signature verification they require the holder of the signature to have the private key for message signing and the public key for verification message of authenticity. The essential goal of the Digital signature is verifying that the message was not been altered during transit after it was signed and giving a confidence of sent by expected party to the receiver (Jafaar and Samsudin, 2010). Fig. 1 illustrates how the Digital Signature works from process of Signature Generation to Signature Verification.

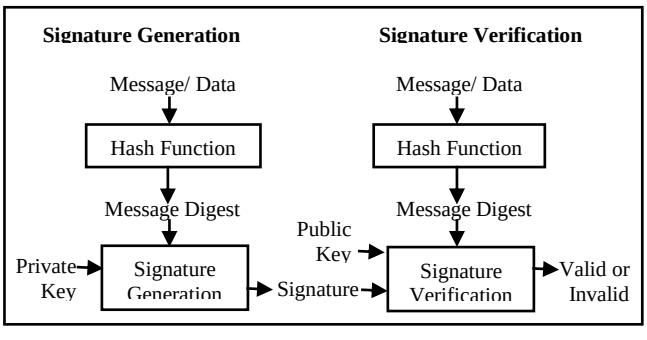


Fig. 1. Digital Signature Process

2. RSA Digital Signature

The RSA digital signature algorithm was developed by Ronald Rivest, Adi Shamir and Leonard Adelman at