Abstract

Any web security system should achieve three conceptual goals are; confidentiality, integrity and Non-repudiation, and authentication. Also any system of communication when it is designed with these security services are taken into account and these security services must be defined and can be shortened format as (CIA). In this paper, we are going to discuss the theoretical background on the objectives of web security, and it will be touched upon the other subjects such as symmetric cryptography, asymmetric cryptography, the hash function, confidentiality, integrity, non-repudiation, Authentication, Communication and Network Security and its types, and we will focus on the digital signature concepts.

References

6. Azaim MH, Sudiharto DW, Jadied EM. Design and implementation of encrypted SMS on Android smartphone combining ECDSA-ECDH and AES. InMultimedia and Broadcasting (APMediaCast), 2016 Asia Pacific Conference on 2016 Nov 17 (pp. 18-23). IEEE.

Index Terms

Computer Science  Security
Keywords

Symmetric cryptography, Asymmetric cryptography, Hash Function, Digital signature, Integrity.