ABSTRACT

In the last few years, computer networks are becoming more dispersed and widespread, given the impact the internet has had on extending the network out to roaming users, business partners, to transfer various types of data with different confidentiality levels. So, it is extremely important to find more secure and confidential methods to ensure the integrity and confidentiality of transferred data. Internet Protocol Security or IPSec is a developed mechanism, has been in use for a number of years now to protect sensitive data as it flows from one location to another depending on a set of protocols and cryptographic algorithms. So, it is a need to develop new cryptographic systems to assure the integrity and confidentiality of transmitted data and withstood the attacks developed methods.

Studying the cryptographic systems and the new modified algorithms, among those modified algorisms, the signcryption algorithm which came to combine between the public cryptography algorithm and the signature algorisms in one step instead of the traditional approach, signature – then – encryption, with saving in the communication overhead reach 40% and saving in computation costs reach 58% with achieving the security goals. Discuss signcryption algorithm in broadcasting one message to multiply recipients.

In this thesis, introducing a new modified scheme "*Modified Elliptic Curve Signcryption*", this scheme based on Elliptic Curve Discrete Logarithm Problem (ECDLP) and in addition to achieve the functionality of the signcryption schemes, *unforgeability*, *confidentiality* and *non – repudiation*, it achieves *forward security and encrypted message authentication and public verifiability* .Also, using a strong session key encryption depends on using a random chosen value plus to the private key of the sender and it is used to encrypt the message twice to increase the confidentiality and integrity of the message. Although proposed scheme is slower than the Zheng's signcryption scheme, it achieves saving in communication overhead reach 50% with respect to the traditional approach signature – then – encryption. And applying the modified scheme on multiply recipients and compare it with Zheng's signcryption for multi – recipients. For future work, We can apply the modified scheme on the IPSec mechanism to save bandwidth and benefit with its security attributes.

LIST OF FIGURES

LIST OF TABLES

Appendix Tables

LIST OF ABBREVIATION

3DES	Triple Data Encryption Standard
AAA	Authentication, Authority And Accounting
AES	Advanced Encryption Standard
AH	Authentication Header
ANST	American National Standards Institute
CA	Certification Authority
CHAP	Challenge Hand Shake Authentication Protocol
DES	Data Encryption Standard
DHP	Differ–Hellman Protocol
DL	Discrete Logarithm
DLP	Discrete Logarithm Problem
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDSS	Elliptic Curve Digital Signature Standard
ECSCS	Elliptic Curve Signcryption Constructed form Shorten Digital Signature Algorithm
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
HMAC	Hash–Based Message Authentication Code
IEEE	Institute of Electrical and Electronics Engineers.
IETF	Internet Engineering Task Force

IFP	Integer Factorization Problem
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
ISAKMP	Internet Security Association And Key Management Protocol
LAN	Local Area Network
MD5	Message Digest Version 5
NIST	National Institute of Standards and Technology
OSI	Open System Interconnection
OTP	One Time Password
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RFC	Request For Comments
RSA	Rivest–Shamir–Adleman
S/KEY	Secure Key
SA	Security Association
SCS	Signcryption Constructed form Shorten Digital Signature Standard
SCSM	Signcryption Constructed form Shorten Digital Signature Algorithm For Multiple Recipients
SDSS	Shorten Digital Signature Standard
SHA	Secure Hash Algorithm
SKEME	Secure Key Exchange Mechanism
TAN	Transaction Authentication Number
TTL	Time To Live
VPN	Virtual Private Network
WAN	Wide Area Network
XAUTH	Extended Authentication