Improving Security by Comparing Symmetric and Asymmetric Encryption using DSC Algorithm

Sonal Rana[1], Aditi Sharma[2]
Department of Computer Science, Shaheed Udham Singh College of Engineering and Technology, Tangori, Punjab

Abstract- Digital Signature is basically used in banking, stock trading, and the sale and purchase. As merchandise are using electronic transactions to minimize operational costs and provide enhanced services. This has led to phenomenal increases in the amounts of electronic documents that are generated, processed, and stored in computers and transmitted over networks. This electronic information handled in these applications is valuable and sensitive and must be protected against tampering by malicious third parties. Digital signatures, which are nothing but a string of ones and zeroes generated by using a digital signature algorithm, serve the purpose of validation and authentication of electronic documents. Validation refers to the process of certifying the contents of the document, while authentication refers to the process of certifying the sender of the document. Comparing the different encryptions system by analysing message to take security risk of key sharing.

Keywords- *Hashing, Symmetric and Asymmetric Encryption, DSC Algorithm*

I. INTRODUCTION

Digital signature is just a sequence of zeroes and ones; it is desirable for it to have the following properties: The signature must be a bit pattern that depends on the message being signed (thus, for the same originator, the digital signature is different for different documents),The signature must use some information that is unique to the sender to prevent both forgery and denial; it must be relatively easy to produce; it must be relatively easy to recognize and verify the authenticity of digital signature; it must be computationally infeasible to forge a digital signature either by constructing a new message for an existing digital sig-nature or constructing a fraudulent digital signature for a given message; and it must be practical to recopies of the digital signatures in storage for arbitrating possible disputes later. Digital signature certificates (DSC) are the digital equivalent (that is electronic format) of physical or paper certificates. Examples of physical certificates are drivers' licenses, passports or membership cards. Certificates serve as proof of identity of an individual for a certain purpose; for example, a driver's license identifies someone who can legally drive in a particular country. Likewise, a digital certificate can be presented electronically to prove your identity, to access information or services on the Internet or to sign certain documents digitally. Digital Certificates are used for signing web forms, e-tendering documents, filing income tax returns etc. The PKI is a framework of policies, services, and encryption software that provides the assurances, users need before they can confidently transmit sensitive information over the Internet and other networks. At the heart of a PKI is a "Certifying Authority" which issues to each individual a Digital Certificate linking that particular person to a known public key?

The principal elements of a digital certificate are as follows:

- Version number of the certificate format
- Serial number of the certificate
- Signature algorithm identifier
- Issuer of digital certificate: a certificate authority with URL
- Validity period
- Unique identification of certificate holder
- Public key information

II. DIGITAL SIGNATURES – TECHNICAL ISSUES

The Information Technology Act 2000 (IT Act) prescribes digital signatures as a means of authentication of electronic records. Digital signature has the same function as that of a handwritten signature. However, understanding how a digital signature is created and how it achieves the same functionality as that of a handwritten signature is by no means an easy task. This is because the technical concepts involved in creating a digital signature seem far removed from the realm of law, although the objective of affixing digital signature to an electronic record is purely legal! Digital signatures are an application of asymmetric key cryptography. Cryptography is primarily used as a tool to protect national secrets and strategies. It is extensively used by the military, the diplomatic services and the banking sector. One of the landmark developments in the history of cryptography was the introduction of the revolutionary concept of public-key cryptography. Cryptography is the transformation of readable and understandable data into a form which cannot be understood in order to secure data. Cryptography refers exactly to the methodology of concealing the content of messages, the word cryptography comes from the Greek word "Kryptos", that means hidden, and "graphikos" which means

writing The information that we need to hide, is called plaintext , It's the original text, It could be in a form of characters, numerical data, executable programs, pictures, or any other kind of information, The plaintext for example is the first draft of a message in the sender before encryption, or it is the text at the receiver after decryption. The data that will be transmitted is called cipher text, it's a term refers to the string of "meaningless" data, or unclear text that nobody must understand, except the recipients. It is the data that will be transmitted Exactly through network, Many algorithms are used to transform plaintext into cipher text .The Key is an input to the encryption algorithm, and this value must be independent of the plaintext, This input is used to transform the plaintext into cipher text, so different keys will yield different cipher text, In the decipher side, the inverse of the key will be used inside the algorithm instead of the key. Computer security it's a generic term for a collection of tools designed to protect any data from hackers, theft, corruption, or natural disaster while allowing these data to be available to the users at the same time. Network security refers to any activity designed to protect the usability, integrity, reliability, and safety of data during their transmission on a network, Network security deals with hardware and software, The activity can be one of the following anti-virus and anti-spyware, firewall, Intrusion prevention systems, and Virtual Private. Internet Security is measures and procedures used to protect data during their transmission over a Collection of interconnected networks .while information security is about how to prevent attacks, and to detect attacks on information-based systems. Cryptanalysis (code breaking) is the study of principles and methods of deciphering cipher text without knowing the key, typically this includes finding and guessing the secrete key, It's a complex process involving statistical analysis, analytical reasoning, math tools and pattern-finding, The field of both cryptography and cryptanalysis is called cryptology. Symmetric encryption refers to the process of converting plaintext into cipher text at the sender with the same key that will be used to retrieve plaintext from cipher text at the recipient. While asymmetric encryption refers to the process of converting plaintext into cipher text at the sender with different key that will be used to retrieve plaintext from cipher text at the recipient. Passive attacks mean that the attackers or the unauthorized parties just monitoring on the traffic or on the communication between the sender and the recipient, but not attempting to breach or shut down a service, This kind of attacks is very hard to discover, since the unauthorized party doesn't leave any traces. On the other hand active attacks mean that the attackers are actively attempting to cause harm to the network or the data. The attackers are not just monitoring on the traffic, but they also attempt to breach or shut down the service. Authentications the process of determining whether someone is the same person who really is, such as login and password in login pages while authorization is the process of ensuring that this person has the ability to do something. Brute force is the attackers who are trying all of the possible keys that may be used in either decrypt or encrypt information.

III. DIGITAL SIGNATURE ALGORITHM

The tools are now in place to describe digital signatures. Simply, to sign a document one just needs to run the document through a message digest algorithm creating a "fingerprint" of the document, and then use this bit sequence in the signing procedure of the public key algorithm selected. Signing a document encrypts using the private keys. The resulting bit sequence is transmitted right along with the original document. The receiver, wishing to verify the signature, will get the sender's public key from a server (or from a certificate as described above), calculate the message digest of the message the same way the sender did, and use this information in the verification procedure of the decryption algorithm. If the algorithm indicates successful verification, the signature is considered valid. Validity would mean:

1. The message was not altered or modified between the time it was signed and the time the signature was verified.
2. The private key associated with this public key is the only key that could have signed this document. If the public keys were retrieved from a digital certificate (a PKI is in place), the keys can be traced to an identity, given that the source of the certificate (the bank for instance) is trustworthy. One more item could then be known.
3. The owner of this private key is the person (or company) who signed this document. Unless the secret key was compromised, there would be no denying this.

A. Secure Hashes

A "checksum" is a simple way of taking a very long string of data, which could be (almost) any length, and reducing it down to a specific number of bits, such that changing any bit of the original data would change the checksum. Hashing is the same concept, and it has been part of computing for a very long time. Hashing takes a message of any length and condenses it, or digests it, into a specified number of bits. It is a one-way function –you cannot go backwards and find the message from the hash. If the sender of a message calculated a hash before transmission, and then sent the hash along with the message, the receiver of the message could verify that the message was not garbled in transmission if his own calculation of the hash matched that of the senders' calculation. A secure hash has additional properties. As you might guess, a message digest uses cryptographic algorithms to provide these additional properties:

1. Changing any bit of the original message will unpredictably change each and every bit of the message digest.

2. It is not practical to find two messages with the same message digest (called a collision).
3. It is not practical to find messages with a given message digest.

With hashes we do not care about finding the message again after we "digest" it. There are no keys to keep secret. The message just needs to be scrambled enough such that the hash is unrecognizable. The properties are important if we are to guarantee that no one has manipulated the messages. This is important to digital signatures. The message digest is always the same number of bits. One might wonder how a message digest can represent the message, since surely more messages can be created than can be represented in a finite number of bits. To create a digital signature from a message, create a hash value, also known as a message digest, from the message. Then, use the signer's private key to sign the hash value. The following illustration shows the process for creating a digital signature.

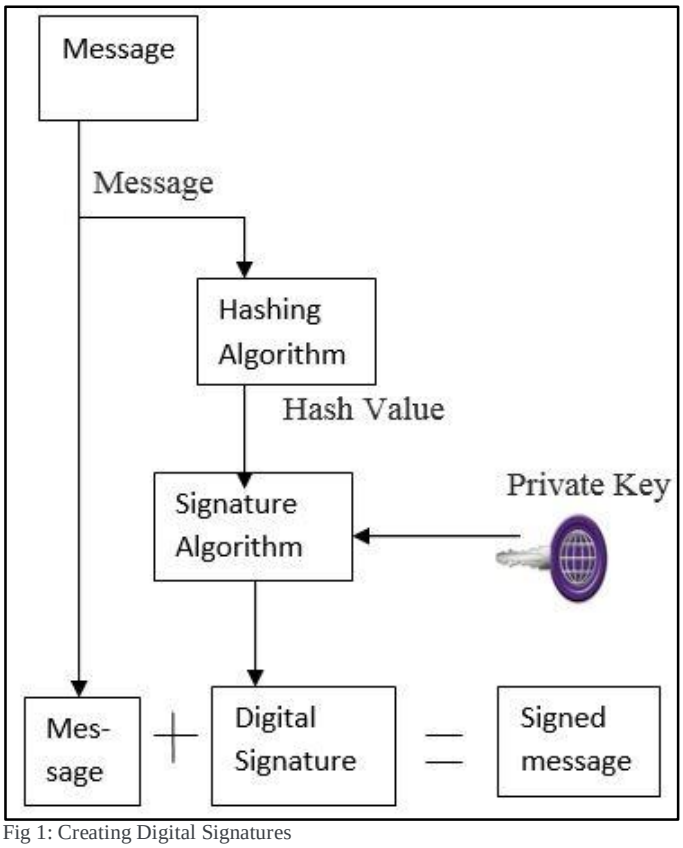

Fig 1: Creating Digital Signatures

B. Symmetric and Asymmetric Encryption

Encryption is the strongest and the safest way in securing data. Certainly, it is the most common one. Encryption systems are divided into two major types-Symmetric and Asymmetric. Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key. Symmetric encryption is known as secret key or single key, The receiver uses the same key which the sender uses to encrypt the data to decrypt the message,. This system was the only system used before discovering and developing the public key., A safe way of data transfer must be used to moving the secret key between the sender and the receiver in symmetric encryption. Symmetric encryption occurs either by substitution transposition technique, or by a mixture of both. Substitution maps each plaintext element into cipher text element, but transposition transposes the positions of plaintext elements.

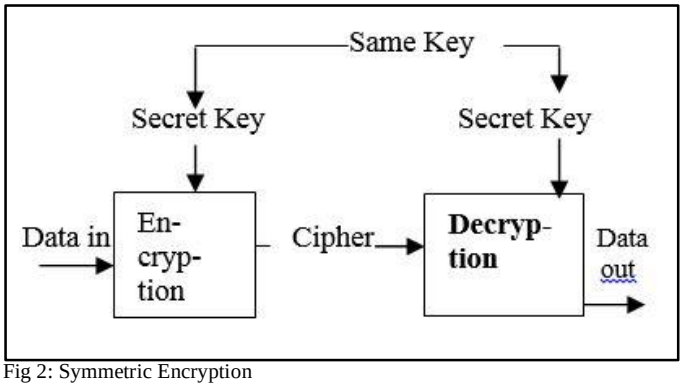

Fig 2: Symmetric Encryption

Asymmetric encryption is the opposite of symmetric encryption in safety, since it doesn't require sharing the secret key between the sender and the receiver. And this is the main difference between symmetric and asymmetric encryption, the sender has the public key of the receiver. Because the receiver has his own secret key which is extremely difficult or impossible to know through the public key, no shared key is needed; the receiver is responsible for establishing his private and public key, and the receiver sends the public key to all senders by any channel he needs, even unsecured channels to send his public key, asymmetric key can use either the public or secret key to encrypt the data. Also it can use any of the keys in decryption, asymmetric encryption can be used to implement the authentication and non-repudiation security services, and also it can be used for digital signature and other application that never be implemented using symmetric encryption Asymmetric

encryption is slower and very complicated in calculations than symmetric encryption. Therefore, asymmetric encryption deals with plaintext as a group of numbers which are manipulated in mathematics, while the plaintext in symmetric encryption deal as group of symbols and characters, the encryption process may permute these symbols, or may substitute one symbol by another. Asymmetric encryption is the opposite of symmetric encryption in safety, since it doesn't require sharing the secret key between the sender and the receiver. And this is the main difference between symmetric and asymmetric encryption, the sender has the public key of the receiver. Because the receiver has his own secret key which is extremely difficult or impossible to know through the public key, no shared key is needed; the receiver is responsible for establishing his private and public key, and the receiver sends the public key to all senders by any channel he needs, even unsecured channels to send his public key, asymmetric key can use either the public or secret key to encrypt the data. Also it can use any of the keys in decryption, asymmetric encryption can be used to implement the authentication and non-repudiation security services, and also it can be used for digital signature and other application that never be implemented using symmetric encryption. Figure.5 shows how the system works. Asymmetric encryption is slower and very complicated in calculations than symmetric encryption. Therefore, asymmetric encryption deals with plaintext as a group of numbers which are manipulated in mathematics, while the plaintext in symmetric encryption deal as group of symbols and characters, the encryption process may permute these symbols, or may substitute one symbol by another.

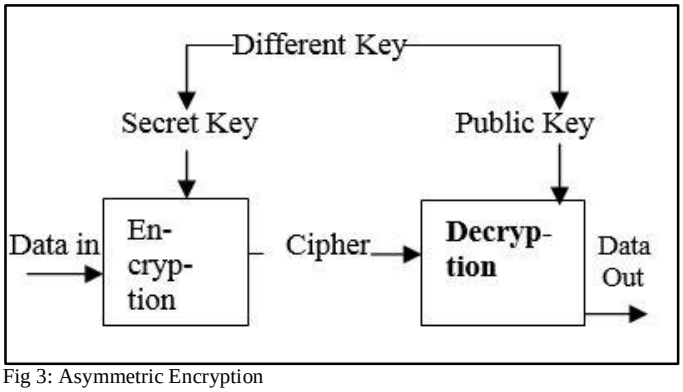

Fig 3: Asymmetric Encryption

IV. REASONS FOR USE OF SYMMETRIC APPROACH FOR ENCRYPTION AND DECRYPTION

1. The encryption process is simple.
2. Each trading partner can use the same encryption algorithm no need to develop and exchange secret algorithms.
3. Security is dependent on the length of the key.
4. High rates of data throughput.
5. Keys for symmetric-key ciphers are relatively short.
6. Symmetric-key ciphers can be used as primitives to construct various cryptographic mechanisms.
7. Symmetric-key ciphers can be composed to produce stronger ciphers
8. Symmetric-key encryption is perceived to have an extensive history.

V. CONCLUSIONS

Symmetric encryption uses the identical key to both encrypt and decrypt the data. Symmetric key algorithms are much faster computationally than asymmetric algorithms as the encryption process is less complicated. The length of the key size is critical for the strength of the security. There are inherent challenges with symmetric key encryption in that the key must somehow be managed. Distributing a shared key is a major security risk. Asymmetric encryption uses two related keys (public and private) for data encryption and decryption, and takes away the security risk of key sharing. The private key is never exposed. A message that is encrypted by using the public key can only be decrypted by applying the same algorithm and using the matching private key.

VI. REFERENCES

[1] Digital Certificate Used in Campuses and Internet Services J. Badeau., "The Genius of Arab Civilization", Second Edition. MIT Press,(1983), USA.
[2] D.Delfs. and K. Helmut.,: " Introduction To Cryptography: Principles and applications ", Second Edition. Springer Science & Business Media, (2007), Germany.
[3] A. Forouzan.: "Cryptography and Network Security ", First Edition.
[4] W .Stallings, " Cryptography and network security, Principles and practices ", Fourth Edition. Pearson Prentice Hall, (2006):, USA.