CHAPTER - 4

MULTIPLE ENCRYPTION IN INFORMATION SECURITY

4.1 MULTIPLE ENCRYPTION IN SECURE ELECTRONIC TRANSACTIONS (SET)

Secure Electronic Transaction (SET) was developed by VISA and MasterCard with the help of other companies like Microsoft, GTE, IBM, Netscape, VeriSign and RSA in 1996 [DSET09]. Secure Electronic Transaction (SET) was based on X.509 certificates, which is a digital certificate used for authentication purpose. The first version of Secure Electronic Transaction was launched in May, 1997 [DSET09].

For SET, various encryption algorithms are used such as DES and RSA. As explained in the previous chapter DES is a 56-bit key algorithm, which is used to encrypt online transactions. This encryption technique is not much secure and can be easily cracked using modern software embedded hardware. In 1993, using a concept of brute force attack, a DES cracking machine was designed by a scientist Michael Wiener [USDE99]. In 1996, a great scientist Schneier proposed that a parallel machine can be designed that cracks DES system within a second [USDE99]. So, for the secure transaction the DES was replaced by a powerful and reliable system such as SET. SET permits to communicate parties to identify and authenticate each other in hidden manner and exchange sensitive information securely. The main advantage of SET is that all communication takes place in a hidden manner. In SET, the merchant cannot access the customer sensitive credit card information. Such strong protection is provided for the benefits of customers as well as credit/debit card companies to avoid any type of financial frauds.

4.1.1 Needs of Encryption in SET

The popularity of online shopping is increasing day by day, in which customers provide the credit card information to make payment for requested product. Secure Socket Layer (SSL) and Transport Layer Security (TLS) keeps records of credit card details safe from intruder and unauthorized users.
(a) Global e-commerce sales are growing at more than 19% per year  
(b) Global e-commerce sales in region 2010

Fig. 4.1: Status of E-Commerce Growth in Global Market

Research Survey conducted by a reputed organization i.e. JP Morgan is also screening accelerated growth in e-commerce of the predicted 19.4% of the United State e-commerce business in the year 2011. Though only building up the growth of e-commerce as approx. 3.9% of the US market in the year 2009, e-commerce is definitely staying here and continue to achieve more and more strength.

SET handles such type of situations by requiring merchants and credit/debit card holders to register themselves before any online transaction. A trusted certificate authority makes an important role to register cardholders and merchants and after final approval certificate authority issues the security details and a unique signature key for online transactions. These details and digital signature will be used for the authentication purpose. All order information and confirmations carry digital signatures, which provide non-repudiation and authentication services to avoid any fraud and can be used to resolve any dispute.

4.1.2 Working Principle of SET

A Secure Electronic Transaction involves three parties: the credit/debit cardholder, the merchant, and a bank as a payment gateway. The credit/debit cardholders share the order information with the merchant though merchant website but not with the bank (a payment gateway). But credit/debit cardholder shares the payment information to the payment gateway (bank) but not with the merchant. A set of dual digital signature establishes this partial sharing of information and allowing all communicating parties to confirm that they are performing the same transaction.
In this process, each communicating party receives the hash format of the required information. The cardholder signs the hashes of payment and order information. Each communicating party can verify and confirm that the hash in their possession matches with the hash signed by the cardholder. The cardholder and merchant compute equivalent hashes for the bank to compare. All communications between communicating parties are highly protected. Merchants cannot access the credit card information of customers.

Fig. 4.2: Secure Electronic Transaction Using Credit Card
In Fig. 4.2, the whole process of SET is shown. In this, SET involves three communicating parties as buyer, seller and the bank as a payment gateway. The online transaction is taking place over the wireless network as Internet in a secure manner.

Further, intruder or criminal is not able to make any transaction because it requires cardholder’s signature and a secret number received by trusted third party after registration. A merchant can be authorized to receive credit card numbers and has the option of accepting payments given a credit card number alone. Authentication is an important issue for online users who perform online transactions over unreliable and insecure wireless network. All communicating parties must have faith in the authenticity of each other through a trusted third party. In the absence of authentication, any intruder or unauthorized user could pose as a merchant and tarnish the merchant’s reputation by failing to deliver products and billing up the credit card bills in an illegal manner. So, authentication is a critical factor to achieve trust in electronic commerce.

According to the Data Security for electronic transaction, the general steps for the SET are:

❖ **Customer to Merchant**

1) A customer sends both the order and payment details to the merchant, together with his certificate.

2) The payment details will be encrypted; the merchant will not be able to read the payment details.

3) The merchant uses the customer’s certificate to verify the customer.

❖ **Merchant to Customer's Bank**

1. The merchant sends this payment details to his bank who will then forward it to the customer's bank to request authorization that the customer has sufficient available credit for the purchase.

❖ **Confirmation of Order**

1. Once the authorization is received, the merchant will send an order confirmation to the customer.

❖ **Shipping of Goods**
1. Upon confirmation by the customer, the merchant will deliver the goods to the customer

- Request for Payment By Merchant

1. Lastly, the bank makes a request to the customer's credit card bank for payment.

4.1.3 Overview of the Proposed Multiple Encryption Technique in SET

This idea differs with the existing data encryption technique used in Secure Electronic Transaction standards to provide better information security over the wireless network as the internet. It may enhance the data security enormously due to use of data encryption multiple times with different advance encryption keys. It increases the complexity in encryption as well as the decryption process in such a manner that a long time is required to analyze the correct keys to decrypt the encrypted data.

- Conventional Encryption Technique in SET

1. Take original confidential information as plain text.

2. Employ Simple Hash Algorithm, getting result as Message Digest.

3. Encrypt Message Digest with a private key to generate Digital Signature.

4. Transmit the data with Digital Signature to the receiver side.

However, as much as we encrypt the data multiple times we get stronger and secure encryption algorithm. So, using three encryptions in triple DES, we can achieve a greater level of security in comparison of single or double encryption. The use of double encryption does not provide the adequate security and cannot be recommended as a secure encryption technique. In triple DES, triple encryption can provide substantial improvements in data security.

- Multiple Encryption Technique in SET

1. Take original confidential information as plain text.

2. Employ Simple Hash Algorithm, getting result as Message Digest.

3. Encrypt Message Digest multiple times with different encryption keys to generate more
advance and complex Digital Signature.

4. Transmit the data with newly generated Digital Signature to the receiver side.

So, using multiple encryption we can get more secured and advanced digital signature which is very complicated to crack by any intruder or unauthorized party.

**4.2 MULTIPLE ENCRYPTION IN SECURE VOICE COMMUNICATION**

Voice encryption is a process of converting sound signal in a secure form by using encryption algorithm. In cryptography, secure voice is a term which is used for the encryption of voice communication over the insecure communication medium such as telephone, mobile or IP telephony.

![Fig. 4.3: Operations in Voice Encryption](image)

To implement this system, the army gave the contract to Bell Laboratories and they developed a system called as SIGSALY. In SIGSALY, ten channels were allocated to sample the voice frequency spectrum from 250 Hz to 3 KHz and two channels were allocated to sample background hiss and voice pitch. This system included radio transmitter and receiver with large precise phonograph turntables.
A secure voice communication system provides the secure transmission of voice communication between the sender and receiver through PSTN (Public Switched Telephone Network). This system implements the multiple encryption techniques to enhance the security of voice communication over insecure network. This system uses an encryption/decryption engine which is capable to execute a number of complex encryption algorithms. During the voice communication, the voice encryption algorithm may be changed session to session.

![Diagram of Secure Voice Communication System](image)

**Fig. 4.4: Voice Over Secure IP**

### 4.2.1 Description of Digital Secure Voice Communication

A digital secure voice generally includes two components, an encryption system to provide confidentiality and a digitizer to convert between speech and digital signals. Voice coder is used to achieve bandwidth compression of the speech signals. The old secure voice coder or voice compression standards include Mixed Excitation Linear Prediction (MELP), where the latest standard is the Enhanced Mixed Excitation Linear Prediction (MELPe) algorithm.

A) **Digital Methods Using Voice Compression**
The MELPe is a speech coding standard of the United States Department of Defense for military applications for secure voice and satellite communication. Its development was supported and led by NSA and NATO. The Enhanced-MELP was adopted in 2001 in the form of supplement and Annexure for secure voice communication.

In 2002, the MELPe was adopted as NATO standard and it was tested against old secure voice standards. Subsequently, the MELPe won the competition, surpassing the quality of all other secure voice standards. The NATO concluded that MELP substantially improved performance in terms of speech quality, intelligibility and noise immunity and reducing throughput requirements. In 2005, a new 600bit/s rate MELPe voice coder (vocoder) was added to the NATO standard by France, and there are more advance efforts made to lower the bit rates to 300 bit/s and even 150 bit/s.

![NATO’s MELPe Performance Index](image)

One of the greatest benefits of the MELPe is that it shares the same bit format as MELP, and hence can interoperate with existing MELP systems and delivers better quality at both ends. MELPe provides better performance and quality than older military standards, especially in noisy environments such as army vehicle, battlefield and aircraft.

**B) Multiple Encryption for Securing Voice**

Voice encryption is the process of converting sound signals or voice into a secure form. It provides high security for voice communication. There is the possibility of information theft during the conversation through insecure communication medium such as telephone, mobile and IP phone etc. Voice encryption can resolve this problem and enables to establish secure
communication between sender and receiver. In modern technology, most secure voice systems are using multiple encryption technique for secure communication without losing its quality and clarity. In this process, voice information is secured through multilayer security by number of encryptions using various advance and complex encryption algorithms.

Multiple encryption ensures high safety of voice information over an insecure wireless network. It offers telecommunication security that gives protection against eavesdropping and information theft for various forms of voice communication between 3G, GSM, 2.5 and IP network. In the modern age, mostly secure voice devices are implementing the concept of multiple encryption and using 256 bit AES encryption algorithm which is the most advanced encryption technique for voice communication and more advanced than the DES standard.

For secure voice communication multiple encryption provides the various benefits, which are followed as:

(a) High level security through number of encryption with different encryption keys for each session using Asymmetric Public key cryptography and Diffie-Hellman Key exchange algorithm.
(b) End-to-end secure data and voice communication over GSM network.
(c) Maintaining voice quality and clarity.
(d) Efficient implementation of encryption algorithms for minimum impact on battery life.

Fig. 4.6: Multiple Encryption of Voice Communication
Many IT companies are providing highly advanced voice encryption devices such as Snapshield, Snapfone, Snapgate and Snapmaster, which have the capabilities of voice encryption. These voice encryption devices are trusted by government offices or organizations, private enterprises and individuals.

### 4.2.2 SecureGSM: An Implementation of Secure Voice Communication

The techniques of secure voice communication are implemented successfully to provide reliable voice communication over wireless media. SecureGSM is one popular application in the market, which provides a secure voice communication over wireless networks.

SecureGSM products encrypt the phone call in both directions, end-to-end, to Military Grade encryption standards and beyond. In the connection between parties, SecureGSM products use strict verification procedures to ensure the identity of calling parties, backed up by widely endorsed encryption technologies.

*SecureGSM In-Confidence* is a next generation product designed to deliver SecureGSM's famous triple-layer encryption to secure Voice over IP (VoIP) communications. In-Confidence is the only dedicated multi-party conferencing product with triple layer encryption capabilities available in the market today.

This product is very popular for secure voice communication due to its advanced features of voice security and encryptions. It includes various advanced features such as:

*SecureGSM™ In-Confidence* features robust, triple cipher (3 x 256 bits), cascading encryption based on AES, Twofish and Serpent ciphers. Any one of these encryption algorithms is considered unbreakable by today’s standards and the triple layer ensures that encrypted data is future proof.

*If any one of the encryption algorithms is broken, or found flawed in the future, it is not possible to obtain data to decrypt or compromise the remaining layers or chains.*

*Robust, high performance, asymmetric key generation engine. Private and public keys are generated per session and subsequently destroyed upon termination of the call.*
*Calling party identity verification procedures as protection from “man in the middle” attack and comprehensive procedures to ensure keys or foreign data have not been injected or substituted by a third party.

*Triple ECDH - Elliptic Curves Diffie-Hellman (3 x 571 bits) * Public Key Infrastructure.

*Unique Party Authentication Module.

(a) SecureGSM Dialing  
(b) Identity Verification

(c) Incoming Call  
(d) Confirmation Message
During installation, signature files corresponding to each of the program files, along with a list of all files that belong to a SecureGSM product installation are placed in the installation folder. The signature files contain verification checksums of each file required to be verified. If the product or a component of the product is modified, corrupted or does not belong to that particular installation, its checksum will be different from what was recorded in its signature file. SecureGSM products stop phone tapping and interception by using unbreakable encryption and offer unparalleled ease of use.

4.3 MULTIPLE ENCRYPTION IN VIRTUAL PRIVATE NETWORK (VPN)

Virtual Private Network (VPN) is an effective technology to provide the secure data communication over unreliable and unsecure wireless network. It fulfills the requirement of private and secure point-to-point networking using a low cost public network as the internet.

4.3.1 Functionality of Virtual Private Network

A Virtual Private Network (VPN) creates a virtual and private network using the internet. Two remote locations can be connected through VPN with establishing a private connection between them. In Virtual Private Network, a concept of tunneling is used, in which each data packet is encrypted and then transmitted to remote locations. The VPN tunnel has only two endpoints as source point and destination point between which actual communication is
established. For example, one office can be connected to another office situated at remote location through a secure VPN tunnel. A secure and private communication can take place through a connected link from one location to another location.

After successful establishment of VPN network between two communicating parties, other users access the services of the internet independently and all internet traffic passes outside the VPN tunnel. In such a manner, we can establish number of VPN tunnels for multiple private and secure communications. The VPN tunnel is very secure and cannot be intercepted by any intruder or attacker in the mid way.

4.3.2 Multiple Encryption in Virtual Private Network

The process of encryption/decryption takes place at the end points of VPN tunnel. The VPN router has the ability to determine the VPN credentials like as remote locations, passwords, encryption keys and network addresses of remote networks. In the VPN, the process of encryption and encapsulation are integrated for secure communication. The use of point-to-point tunneling protocol provides an optional encryption, which is not considered as very secure. So, multiple encryption is used in VPN to enhance the security at the large extent. For this purpose, 3DES and AES are used as multiple encryption algorithm to provide high level security.
In current scenario, in mostly VPNs multiple encryption are used instead of conventional or simple encryption to provide high level security. 3DES and AES both are considered as highly secured encryption algorithms, but AES encryption algorithm provides better security in comparison of 3DES algorithm. In a VPN, the authentication process provides the additional security by protecting the communication from unauthorized user. To provide authentication facility in VPN, we can use SHA1 or MD5 as an authentication technique. The authentication process in VPN ensures the integrity of the key exchange mechanism.

![How VPNs Work](image)

Fig. 4.9: Working Criteria of VPN Technology

A VPN tunnel provides a link between one end and remote end through which data can flow freely in both directions. To create a secure tunnel between two ends, following requirements should be fulfilled.
Table 4.1: Requirements of Secure VPN

If above mentioned requirements are fulfilled then we can establish highly secure VPN through which data can be transmitted from one location to another location safely.

### 4.4 MULTIPLE ENCRYPTION FOR SECURE ACCESS TO XML DOCUMENTS

Extensible Markup Language (XML) encryption was specified and developed by W3C Consortium or World Wide Web (WWW) in the year 2002. The concept of XML Encryption was proposed to provide the security for web documents. XML Encryption consists a sequence of steps, which can be described in following manner.

1. Encryption of XML Data
2. Decryption of encrypted XMLData
3. XML Syntax to represent the encrypted data
4. Use of appropriate encryption algorithm from the list of secure encryption algorithms

#### 4.4.1 Overview of XML Encryption

XML Encryption is an ideal way to exchange the XML data in such a manner that confidentiality of XML data is maintained effectively during the transmission over insecure wireless network. In XML Encryption, the actual content of an XML document cannot be read or accessed by any
intruder during the transmission. In Pic. 4.11, overview of XML Encryption is described in a simple manner.

![Image of XML Encryption]

**Fig. 4.10: Overview of XML Encryption**

The XML data can be encrypted by secure encryption algorithm and stored using an XML element as `<Encrypted Data>`. It contains the encrypted XML data. This element consists number of supplements to include the information of encryption keys and other processes used during the encryption process. In a recent trend, XML documents are encrypted using multiple encryption instead of simple encryption to provide high security. XML Encryption permits any document to be encrypted multiple times.

### 4.4.2 Working Principle of Multiple Encryption in XMLDocument

In the multiple encryption of XML document, XML data is encrypted using two encryption keys as a pair of public/private key and separate session key. In the first phase of XML encryption, an asymmetric key pair through RSA algorithm is generated and this key pair is saved in a secure key container. In the second phase of XML encryption, a separate session key is created using AES encryption algorithm. This session key is used to encrypt the XML data and then RSA generated public key is used to encrypt the session key. Finally, encrypted session key and encrypted XML data are saved within a new XML element `<Encrypted Data>`.
To decrypt the XML data, first we retrieve the private key from key container and this key is used to decrypt the AES session key. Now this AES session key is used to decrypt the encrypted XML data.

**Fig. 4.11: Multiple Encryption of XML Data**

### 4.4.3. A Program for Multiple Encryption of XMLDocument

A program for multiple encryption of XML data can be written in any supportable programming language. An example of this program written in Visual Basic (VB) can be described in following manner.

**Program of XML Encryption:**

```vbnet
Imports System
Imports System.Xml
Imports System.Security.Cryptography

Class Program
    Shared Sub Main(ByVal args() As String)

        ' Create an XmlDocument object.

    End Sub
End Class
```

102  |  Designing Some Multiple and Multiphase Encryption Techniques for the Enhancement of Data Security
Dim xmlDoc As New XmlDocument()
' Load an XML file into the XmlDocument object.
Try
    xmlDoc.PreserveWhitespace = True
    xmlDoc.Load("test.xml")
Catch e As Exception
    Console.WriteLine(e.Message)
End Try
' Create a new CspParameters object to specify a key container.
Dim cspParams As New CspParameters()
cspParams.KeyContainerName = "XML_ENC_RSA_KEY"
' Create a new RSA key and save it in the container. This key will encrypt
' a symmetric key, which will then be encrypted in the XML document.
Dim rsaKey As New RSACryptoServiceProvider(cspParams)
Try
    ' Encrypt the "creditcard" element.
    Encrypt(xmlDoc, "creditcard", "EncryptedElement1", rsaKey, "rsaKey")
    ' Save the XML document.
    xmlDoc.Save("test.xml")
    ' Display the encrypted XML to the console.
    Console.WriteLine("Encrypted XML:")
    Console.WriteLine()
    Console.WriteLine(xmlDoc.OuterXml)
    Decrypt(xmlDoc, rsaKey, "rsaKey")
    xmlDoc.Save("test.xml")
    ' Display the encrypted XML to the console.
    Console.WriteLine()
    Console.WriteLine("Decrypted XML:")
    Console.WriteLine()
    Console.WriteLine(xmlDoc.OuterXml)
Catch e As Exception
    Console.WriteLine(e.Message)
Finally
    ' Clear the RSA key.
    rsaKey.Clear()
End Try
Console.ReadLine()
Public Shared Sub Encrypt(ByVal Doc As XmlDocument, ByVal EncryptionElement As String, ByVal EncryptionElementID As String, ByVal Alg As RSA, ByVal KeyName As String)
    ' Check the arguments.
    If Doc Is Nothing Then
        Throw New ArgumentNullException("Doc")
    End If
    If EncryptionElement Is Nothing Then
        Throw New ArgumentNullException("EncryptionElement")
    End If
    If EncryptionElementID Is Nothing Then
        Throw New ArgumentNullException("EncryptionElementID")
    End If
    If Alg Is Nothing Then
        Throw New ArgumentNullException("Alg")
    End If
    If KeyName Is Nothing Then
        Throw New ArgumentNullException("KeyName")
    End If

    '/////////////////////////////////////////////
    ' Find the specified element in the XmlDocument object and create a new XmlElement object.
    '/////////////////////////////////////////////
    Dim elementToEncrypt As XmlElement = Doc.GetElementsByTagName(EncryptionElement)(0) ' Throw an XmlException if the element was not found.
    If elementToEncrypt Is Nothing Then
        Throw New XmlException("The specified element was not found")
    End If

    Dim sessionKey As RijndaelManaged = Nothing
    Try
        '////////////////////////////////////////////////////////
        ' Create a new instance of the EncryptedXml class and use it to encrypt the XmlElement with the
        ' a new random symmetric key.
        '////////////////////////////////////////////////////////
        ' Create a 256 bit Rijndael key.
        sessionKey = New RijndaelManaged()
        sessionKey.KeySize = 256
        Dim eXml As New EncryptedXml()
Dim encryptedElement As Byte() = eXml.EncryptData(elementToEncrypt, sessionKey, False)

' Construct an EncryptedData object and populate it with the desired encryption information.

Dim edElement As New EncryptedData()
edElement.Type = EncryptedXml.XmlEncElementUrl
edElement.Id = EncryptionElementID

' Create an EncryptionMethod element so that the receiver knows which algorithm to use for decryption.
edElement.EncryptionMethod = New EncryptionMethod(EncryptedXml.XmlEncAES256Url)

' Encrypt the session key and add it to an EncryptedKey element.
Dim ek As New EncryptedKey()
Dim encryptedKey As Byte() = EncryptedXml.EncryptKey(sessionKey.Key, Alg, False)
ek.CipherData = New CipherData(encryptedKey)
ek.EncryptionMethod = New EncryptionMethod(EncryptedXml.XmlEncRSA15Url)

' Create a new DataReference element for the KeyInfo element. This optional element specifies which EncryptedData uses this key. An XML document can have multiple EncryptedData elements that use different keys.
Dim dRef As New DataReference()

dRef.Uri = "#" + EncryptionElementID

' Add the DataReference to the EncryptedKey.
ek.AddReference(dRef)

' Add the encrypted key to the EncryptedData object.
edElement.KeyInfo.AddClause(New KeyInfoEncryptedKey(ek))

' Set the KeyInfo element to specify the name of the RSA key.
' Create a new KeyInfoName element.
Dim kin As New KeyInfoName()

' Specify a name for the key.
kin.Value = KeyName

' Add the KeyInfoName element to the EncryptedKey object.
ek.KeyInfo.AddClause(kin)
' Add the encrypted element data to the EncryptedData object.
edElement.CipherData.CipherValue = encryptedElement

'///////////////////////////////////////////////////////
' Replace the element from the original XmlDocument object with the EncryptedData element.
'///////////////////////////////////////////////////////
EncryptedXml.ReplaceElement(elementToEncrypt, edElement, False)

Catch e As Exception
  ' re-throw the exception.
  Throw e
Finally
  If Not (sessionKey Is Nothing) Then
    sessionKey.Clear()
  End If
End Try
End Sub 'Encrypt

Public Shared Sub Decrypt(ByVal Doc As XmlDocument, ByVal Alg As RSA, ByVal KeyName As String)
  ' Check the arguments.
  If Doc Is Nothing Then
    Throw New ArgumentNullException("Doc")
  End If
  If Alg Is Nothing Then
    Throw New ArgumentException("Alg")
  End If
  If KeyName Is Nothing Then
    Throw New ArgumentException("KeyName")
  End If

  ' Create a new EncryptedXml object.
  Dim exml As New EncryptedXml(Doc)
  ' Add a key-name mapping. This method can only decrypt documents that present the specified key name.
  exml.AddKeyNameMapping(KeyName, Alg)
  ' Decrypt the element.
  exml.DecryptDocument()

End Sub 'Decrypt
End Class 'Program
4.5. RESULTS AND CONCLUSION

Multiple encryption is an ambivalent encryption technique and it plays an important role in various areas such as secure electronic transactions, secure voice communication, VPN and XML Documents etc. The main advantage of multiple encryption is that it provides better security because even if some encryption or secret keys are cracked or some part of ciphertexts are broken, the confidentiality and privacy of original information can still be maintained.

Some concluding facts for the revolutionary role of multiple encryption in various domains may be summarized as:

1) Multiple encryption in Secure Electronic Transaction provides high level security which is required to earn the interest and trust of customers, merchants and financial organizations for online transaction over unreliable network as internet.

2) It plays an important role to enhance the security of voice communication enormously without losing voice quality and clarity.

3) It provides the better security for Virtual Private Network by protecting the communication from unauthorized user and establishes highly secure VPN through which data can be transferred from one place to another place safely.

4) It enhances the security of XML documents by using hybrid key encryption algorithm which generates high level security through multi-layer architecture.