Secure Database Access and Transfer Using Public Key Cryptography

M.Princy
Lecturer / MCA
Muthayammal Engineering College,
Rasipuram, Tamilnadu, India
prinzmanohar@gmail.com

C.Karthikeyan
Lecturer / MCA
Muthayammal Engineering College,
Rasipuram, Tamilnadu, India
karthi_mca87@yahoo.co.in

Fenella Ann Fowler
Lecturer / MCA
GanathipathiThulsi's Jain Engineering College,
Vellore, Tamilnadu, India
fenellafowler@gmail.com

ABSTRACT : Nowadays many transactions on internet are implemented by security mechanisms.so authentication plays a vital role in securing data, not only in a single process but with varioustransactions.Many security initiatives are defensive strategies — aimed at protectingthe perimeter of the network. But these works may ignore a crucial Things — sensitive data stored on networked servers are at risk from attackers who only need to find one way inside the network to access this confidential information. Additionally, perimeter defenseslike firewalls cannot protect stored sensitive data from the internal threat — employees with the means to access and exploit this data.Encryption can provide strong security for data at rest, but developing a database encryption strategy must take many factors into consideration.RSA is a rather mature public key algorithm in that itcan be used to encrypt and sign. This paper examines the issues of implementing access and transferring the data using public key cryptography.

Keywords: RSA, DES, Public Key,PKCS.

1. INTRODUCTION:

In this paper ―Secure Data Access and Transfer using Public Key Cryptography‖, using secure database access using authentication to access the data to database and then to transfer the data using public key cryptography algorithm RSA. The RSA algorithm used to encryption and decryption process. The Rivest- Shamir- Adelman (RSA) cryptosystem is a well-known public-key encryption method that is applied to many systems for encryption and decryption . RSA is one of the oldest and most widely used public key cryptographic systems. It was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography . RSA is still widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys. The RSA method is mainly based on integer and factoring as a one way function . Asymmetric cryptography: Unlike the symmetric cryptography, asymmetric cryptography uses a pair of keys to encrypt and decrypt message. One of these two keys is known as public key as it is distributed to others and the other is called private key which is kept secret. Normally public key is used to encrypt any message which can only be decrypted by the corresponding private key. There are essential properties that must be satisfied by the asymmetric cryptography. Thealgorithm used to encrypt the data to the sender using public key. The original data should be changed to coded data or encrypted data. The encipher data to be transfer to the receiver. The receiver generates the key to decrypt the coded text. The public key used to decrypt the coded message into original message. The public key cannot be match the data can't be decrypted. The original data should be stored on a persistent storage.

2. LITERATURE REVIEW

RSA Algorithm

RSA is a public key algorithm based on difficulty of prime factorization. Similar to most public keys password features, RSA password is block encrypted, but different from block encryption used in a secret key algorithm such as DES (Data Encryption Standard) in the sense that a length of a plain text and a key is variable; in other words, a relatively long length of a key can be used in consideration of the secure and reliable system, and a relatively short length of a key can be used for efficient system.The coded data shold be encrypted and it is automatically decrypt by the receiver. In an RSA algorithm, receiver's public key is used to encrypt messages, and the receiver decrypts encrypted messages with its own private key. In an RSA-based signature algorithm, a sender signs messages with its own private key, and a receiver

verifies the signed message with sender's public key; this is how an authentication service is guaranteed through an RSA-based signature algorithm. In many business sectors secure andefficient data transfer is essential. To ensure the security to the applications of business, the business sectors use Public Key Cryptographic Systems (PKCS). An RSA system generally belongs to the category of PKCS. RSA encryption is one of the public-key methods that have been popular in last decade.

In particular, the RSA algorithm is used in many applications. Although the security of RSA is beyond doubt, the evolution in computing power has caused a growth in the necessary key length. The performance characteristics of RSA are observed by implementing the algorithms for computation. In this paper, RSA was implemented through an encryption and decryption procedures over different key sizes. Because of wide uses of networks during the last decade and growing security requirements in communication, public-key cryptosystems have been regarded highly. The concept of public-key cryptography evolved from an attempt to attack two of the most difficult problems associated with symmetric encryption. A key distribution under symmetric encryption requires either (1) that two communicants already share a key, which somehow has been distributed to them; or (2) the use of a key distribution center. .

(*i*) The key generation process should be computationally effective and efficient.

(*ii*) Sender should be able to compute the cipher text by using the public key of the receiver for all themessage,which he sends.

(*iii*) The receiver should be able to decrypt the cipher easily to plain text by using his own private key,which he recieves.

(*iv*) It is impossible or at least impractical to compute the private key from the corresponding public key.

(*v*) It is computationally infeasible to compute the plain text form the public key and cipher text. RSA is the mostwidely used asymmetric encryption system or a public key encryption standard, the private key is kept secret but thepublic key is revealed to everybody in RSA.

OVERVIEW OF RSA CRYPTOSYSTEM

A public-key encryption scheme has six ingredients

• **Plaintext:** This is the readable message or data that is fed into the algorithm as input.

• **Encryption algorithm:** The encryption algorithm performs various transformations on the plaintext.

• **Public and private keys:** This is a pair of keys that have been selected so that if one is used for encryption, the otheris used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.

• **Cipher text:** This is the scrambled message produced as output. It depends on the plaintext and the key. For a givenmessage, two different keys will produce two different cipher texts.

• **Decryption algorithm:** This algorithm accepts the cipher text and the matching key and produces the originalplaintext. In RSA, the plaintext and the cipher text are considered as integers between 0 and n-1, where n is themodulus. The typical size of n is 1024 bits. However, the recommended length of n is 2048 bits as 640 bits key is nomore secure by now. The RSA algorithm is comprised of three sub algorithms that are described below:

Key Generation Algorithm

RSA public and private key pair can be generated by the following procedure. Choose two random prime numbers *p*and *q* such that the bit length of *p* is approximately equal to the bit length of *q*.

The key set is generated by using the following algorithm:

1. Select two large prime numbers *p* and *q* such that *p q*.

2. Compute modulus $n = p*q$

3. Compute (n) such that $(n) = (p–1)* (q–1)$.

4. Choose a random integer e satisfying $1<e < (n)$ and $gcd(e, (n)) =1$

5. Compute the integer d, such that $e*d = 1 \bmod (n)$. (n, e) is the public key, and (n, d) is the private Key

• *n*is known as the modulus.
• *e*is known as the public exponent or encryption exponent or just the exponent.

• *d*is known as the secret exponent or decryption exponent.

Encryption

Encryption refers to algorithmic schemes that encode plain text into non-readable form or cipher text, providingprivacy. Encryption is done by using the following steps:

1. Getting the recipient's public key (*n*, *e*).

2. Representing the plaintext message as a positive integer *m*.

3. Compute the cipher text *c* = *me* mod *n*.

4. Sending the cipher text *c* to receiver.

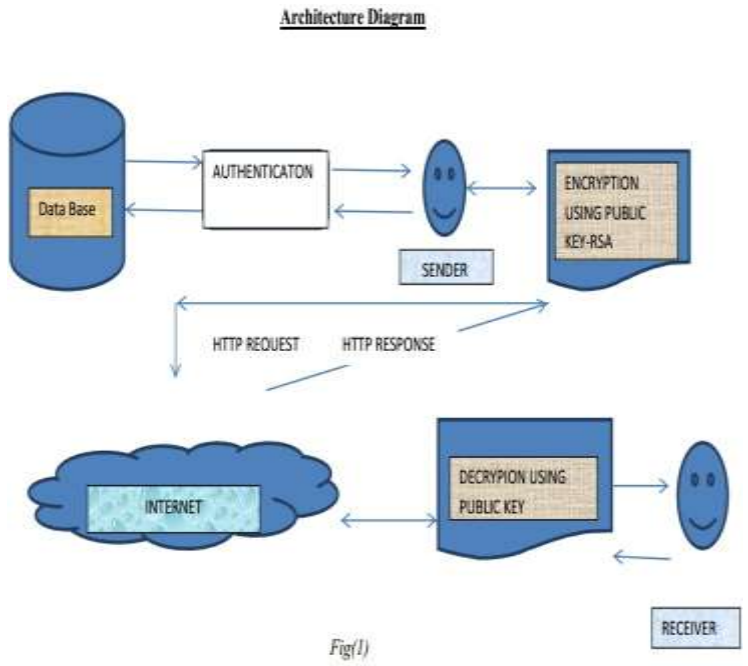
Decryption

Decryption refers to the algorithmic schemes that decode cipher text or non-readable text into readable form or pain text.Message is decrypted by using the following steps:

1. Receiver uses his own private key (*n*, *d*) to compute *m* = *cd* mod *n*.

2. Decrypting the plaintext from the integer representative *m*.

Architecture Diagram



Fig(1)

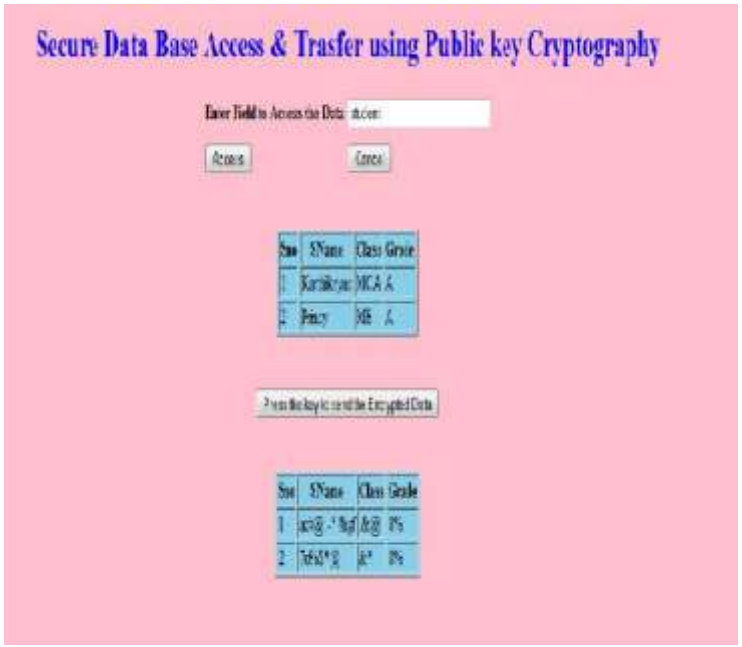
Encryption is a process of converting information in hidden form. So that it is intelligible only to some one who knows how to decrypt it. For encryption and decryption there are two aspects: algorithm and key used. Key is similar to one time pad used in vernam cipher. If same key is used for encryption and decryption then this is called cryptography.[Fig(1) shows that how the message is trasfering from the snder to the receiver using public key cryptography.]And if different keys are used and decryption we call this public key cryptography. In secret key cryptography single key is used. So as before distributing the data between entities the key must be transferred.

RSAconsumes large amount of time to perform encryption and decryption operation

Simulationresult. In this the sender authenticates the message from the database and encrypt it and sends the content to the receiver where he uses a key to decrypt the message.

Data Flow Diagram

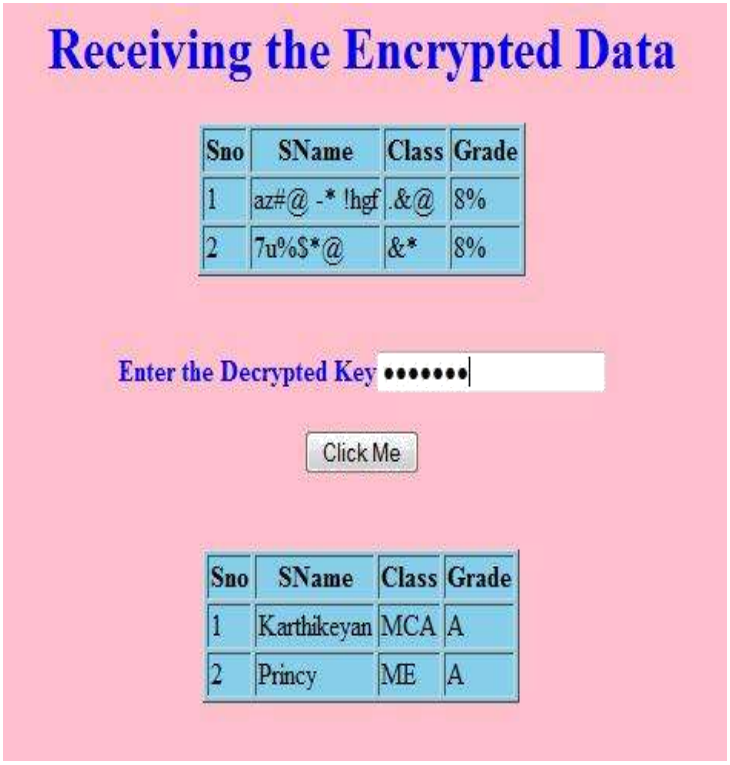
SCREENSHOTS:



Authentication:

RSA SecurID® tokens and smart card solutions are designed to deliver strong two-factor authentication that interoperate with a wide variety of products and applications. These products are easy for the receiver interfacing with a client/server application and they positively identify the user with a higher level of trust than using a simple password.

RSA SecurID authenticators are as simple to use as entering a password, but much more secure. Each end user is assigned an RSA SecurID authenticator which generates a new, unpredictable code every 60 seconds. The user combines thisnumber with a secret PIN to log into protected resources. The authenticator is tied to a powerful algorithm generating a new code every 60 seconds in the RSA SecurID authentication server known as the RSA ACE/Server,® solution. Only it knowswhich number is valid at that moment in time for that user/authenticator combination.Though authentication is important,the method we are using to secure the data also plays a major role.



Conclusion:

Database attacks are on the rise even as the risks of data disclosure are increasing. Already the financial services and health care industries must deal with legislation and regulation on data privacy. Consumer concerns about data disclosure and misuse will inevitably expand the responsibility of your enterprise to secure customer information. The goal of encryption is to make data unintelligible tounauthorized readers and extremely difficult to decipherwhen attacked.This paper discuss how to secure the database using public key cryptography.In this paper a data is encrypted and send to the receiver,the receiver receives the message and decrypt it for his use.Giving answer Using RSA algorithm, how to secure a database?

References:

[1] Dan Boneh and Glenn Durfee ―Cryptanalysis of low exponent RSA.
[2] W. Diffie,M.E Hellman‖ New Directions inCryptography.
[3] Schweighofer E (1997) Downloading information Info I & Common Technology