

Digital securities in E-Governance in Uttarakhand

Mini Agarwal and Rajeev Kumar

Assistant Professor in Computer Science Department, College of Engineering
Teerthanker Mahaveer University
Moradabad (U.P.).

E-Mail: miniagarwal21@gmail.com, rajeev2009mca@gmail.com

Abstract: E-governance deals with the various businesses, governments and citizens. Now a days e-governance have every information related to business, government and citizens that's information is private information if any thief or hacker stolen or hack the data then he misuses the data because e-governance have various important information related to bank account , income tax, business transactions etc. Digital securities are a great technology that is using us for saving our data. Through this technology no one can hack, fetch or showing our data without the permission. At that time many citizens of Uttarakhand use the e-governance for banking, income tax, business purpose, in medical etc they don't know that any hacker hacks or stolen their data. They nothing knows about the digital security. So in this paper we discussing about the digital securities by RSA algorithm for stopping the hacking. In this e-governance helps the citizens in using the digital securities for saving the any conversation like money transaction, account number etc .In this in RSA algorithm we use the private and public key that gives by the e-governance for high security because if citizens forget their key then e-governance gives them again .

[Mini Agarwal, Rajeev Kumar, Digital securities in E-governance in Uttarakhand. Researcher, 2011; 3(9):12-14] (ISSN: 1553-9865). <http://www.sciencepub.net>.

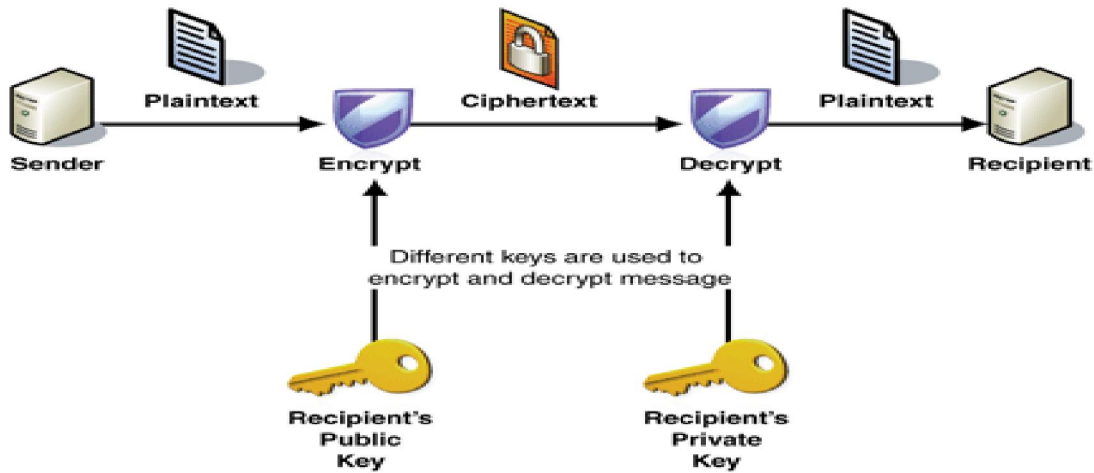
Key words: RSA, Encryption, Decryption, cipher text, Plain text, Key, Private key, Public Key.

1. Introduction:

E-governance provides the various the various IT services like data transaction, money transaction etc.

According the Ron Rivest, Adi Shamir, and Leonard Adleman RSA is a public- key cryptography algorithm. In RSA algorithm we use the two keys one for encryption the data and one for decryption the data. It use the two key public key for encryption the data that is know to all and other is private key for decryption the data that is known to only descriptors. So, in this paper we are using the RSA algorithm for stopping the hacking. The encryption key and decryption key will giving to the people for encrypting (convert the data in to cipher form or private form that is only known the user or e-governance) and the decrypting (convert the cipher means private form data in the original form). In this

when people of Uttarakhand encrypt the data then they have same keys but when they decrypt the data then different person have different key. A person who sends the data is called sender and he encrypts the data by public key and the person who receives the data is called recipient and receiver and he decrypts the data by private key . So, if people of Uttarakhand send the data then they called senders and they encrypt the data by public key and e-governance is called the receiver the decrypts the data by private key else Uttarakhand people are receiver and decrypts the data by private key and e-governance is the sender encrypts the data by public key. In this both keys are generate by the e-governance. E-governance gives the key to the people of Uttarakhand for encryption and decryption.



Fig(a): Encryption and decryption method.

2. Algorithm for Encryption and decryption the data:

RSA is an encryption and decryption algorithm. It is proposed by Ron Rivest, Adi Shamir, and Leonard Adleman. They give the encryption and decryption algorithm that is given below:

2.1 Algorithm used for encrypting the message is given below:

$$E = P^e \text{ mod } Q$$

Where,

E represented as Encryption text in numbers.

P represented as Plain text in numbers.

e represented as Encryption exponent in numbers.

Q represented as modulus in numbers.

2.2 Algorithm used for decrypting the message is given below:

$$P = E^d \text{ mod } Q$$

Where,

E represented as Encryption text in numbers.

P represented as Plain text in numbers.

d represented as decryption exponent in numbers.

Q represented as modulus in numbers.

3. How RSA uses in E-governance?

We use this algorithm in e-governance for stopping the hacking. In this both keys are generated by e-governance because if citizen forget his key then it again collect the key code to the e-governance through completing some inquiry. We describe this algorithm working with e-governance by diagram that is given below (fig (b) and (c)). In this fig (b) shows that citizen sends their data to the e-governance in cipher text form by using the public

key that is given by e-governance and then after receiving the data e-governance converts the cipher text in to the original or plain text by using the private key. In fig (c) shows that e-governance sends the data to the citizen's in the cipher text form by using the public key and after receiving the data citizen change the cipher text in to plain text by using the private key. No, one can steal the data if they don't have the encryption and decryption key.

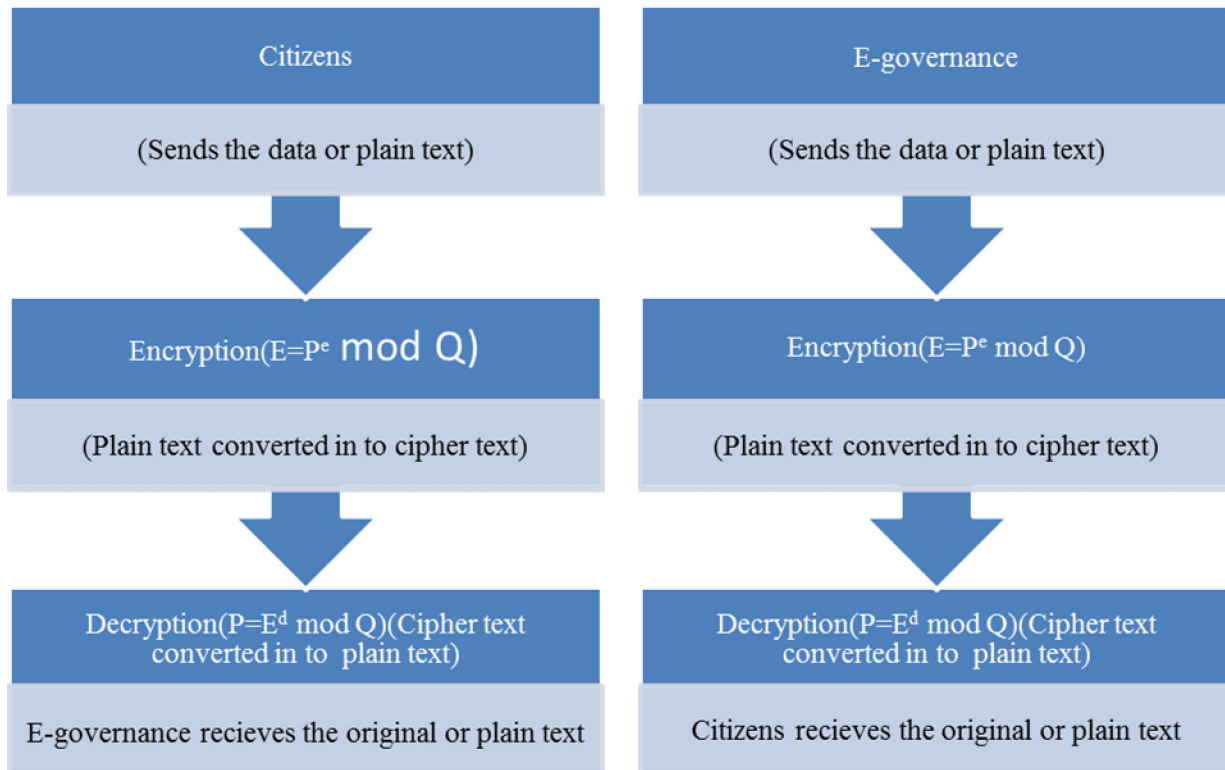


Fig (b) Encryption method by citizens and Decryption method by e-governance

Fig (b) Encryption method by e-governance and decryption method by citizens.

Advantages:

1. No one can fetch the information.
2. Increase security.
3. Use secret key no need for sending original key so, no one can change or hack the data.
4. High speed of Encryption and Decryption.
5. It creates the trust relationship between citizens and e-governance.

Disadvantages:

1. It's a very confidential method if any one hack the any key then he easily hack the data.
2. Increase time consumption in encryption and decryption method.
3. Lengthy process of key generation. E-governance wants many documents for their identity.

4. Conclusion:

At last we conclude the our paper through this paper we only want to say that user and e-governance will uses the digital securities for stopping the hacking or fetching the data. Because at that time e-governance and citizens deals on various important issues like money transaction by debit card, Income tax, Business proposals etc. So, we want no one can misuse the important information or data. Because misuse of data creates the untruthful relationship between e-governance and citizens. So, we want to create the strong relationship between the e-governance and citizens by using the digital securities.

References:

1. Fig(a) <http://msdn.microsoft.com/en-us/library/ff647097.aspx>

8/22/2011