Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 4, Issue 2; January-March, 2017, pp. 88-90

http://www.krishisanskriti.org/Publication.html

A Novel Approach for Verifiable Secret Sharing

[1]Riya Sharma, [2]Prachi Aggarwal, [3]Adarsh Yadav and [4]Dayanand Sharma

[1,2,3,4]Department of Computer Science, HMR Institute of Technology and Management

Abstract – *VSS has been widely used in the field of information security for cloud storage, secure parallel communication, wireless multipath routing protocol. In recent years VSS has been used as a cryptographic tool in the applications of information security. In this paper we consider perfect verifiable secret sharing (VSS) in an existing network of n processors where a designated processor (dealer) wishes to share out a secret s among the processor in a way that none of them get any information, but any t + 1 processor acquire full information about the secret. Our proposed VSS overcomes the weakness of threshold SS which cannot detect any fraud among the dealer and the processors, but this proposed method can identify cheaters by verifying the validity of shares or the correctness of the recovered secret under the condition that both shares and the secret are not compromised.*

Keyword*: Decryption, Encryption, Verifiable Secret Sharing, Secret sharing (SS), RSA.*

Introduction – Network environment is the key essence to the applications running in any organization. So to preserve security in those applications, it involve more than one algorithm or protocol for encryption & decryption and for generation of sub-keys to be mapped to the plain text to generate cipher text. The main aim of this project is to provide an efficient way to the processors for secret reconstruction. Today the RSA algorithm is the foremost mode used for public-key cryptography. This paper evaluate many threshold RSA systems, which can be used for signing documents and for decryption purposes.

Verifiability is the resource of VSS, which confirms that each processor has received a valid share. Invalid shares may be caused either by the dealer or by any error. VSS is run by processors after receiving their own shares from the dealer but before using their shares to rebuild the secret. If VSS has identified some wrong shares, processors can request the dealer to reconstruct new shares. Thus, VSS can ensure processors that their shares can be used to build a secret when the secret reconstruction is needed in future. In a VSS, processors work together to ensure that their shares are created by the dealer consistently without disclosing the secrecy of both shares and the secret. The property of verifiability can check if the shares of shareholders are consistent before performing secret reconstruction. If shares are inconsistent, shareholders can request the dealer to regenerate shares.

Our proposed VSS can check that the secret reconstructed by any t or more processors is the same as that of which dealer has generated. Some of the contributions of this VSS are

1. One way hash function is used to verify the correctness of the message passed or the secret which reduces the operation of analyzing the range of values
2. Provides perfect secrecy.
3. It can detect whether any deception exist between the dealer and processor or not.

Objectives –

- To evaluate public-key cryptography
- To indicate that confidentiality and sender-authentication can be achieved concurrently with public-key cryptography
- To examine the RSA algorithm for public-key cryptography
- For securing multiparty computation
- To go over the computational issues related to RSA
- To confer about the vulnerabilities of RSA

Problem statement –

The major issue with existing cryptography system is that achievement of authentication and confidentiality along with integrity in one step is not possible. In PKI encryption and decryption perform with different key where private key is non-sharable entity. By the Asymmetric Key Cryptography if anyone cypher the message with public key, anyone can decode the message by its public key. Here, we can attain authentication but cannot preserve the confidentiality. Besides, if we cypher the message by public key, only intended person can decrypt the message. It helps to maintain the confidentiality but can't authorize sender. To overcome this problem we use to perform public key encryption after private key. So, only promised receiver would be able to decrypt the message and also authentic the sender by decrypting the received cipher message with public key.

Later on, there is a way to maintain authentication and confidentiality by carrying out digital envelope for communication. A digital envelope is a safe electronic data holder that is used to protect a message through encryption and data authentication. A digital envelope permits users to do coding with the speed of secret key encryption and the

convenience and security of public key encryption. A digital envelope has two layers for encryption: Secret (symmetric) key and public key encryption. Secret key encryption is used for message cypher and decipher

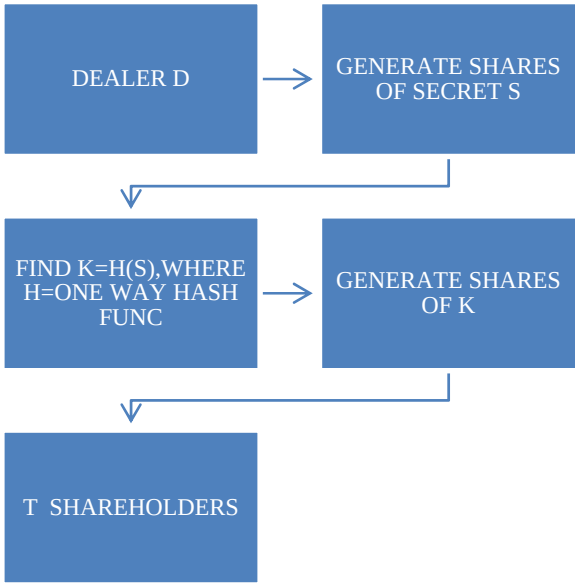
Public key encryption is used to send a secret key to a particular(promised) party over a network.

One of the following methods can be used to create a digital envelope:

- Secret key encryption algorithms, such as Rijndael or Twofish, for message encryption.

• Public key encryption algorithm from RSA for secret key encryption with a receiver's public key.

PROPOSED METHOD –



The proposed solution will not only provide a way for secure communication but also helps in improving level of encryption by reducing security issues.

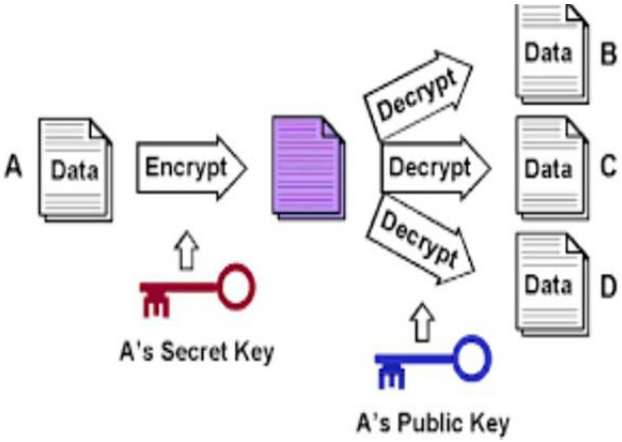
•Public-Key algorithms depend on two keys where:

– it is computationally impracticable to find decryption key knowing only algorithm & encryption key

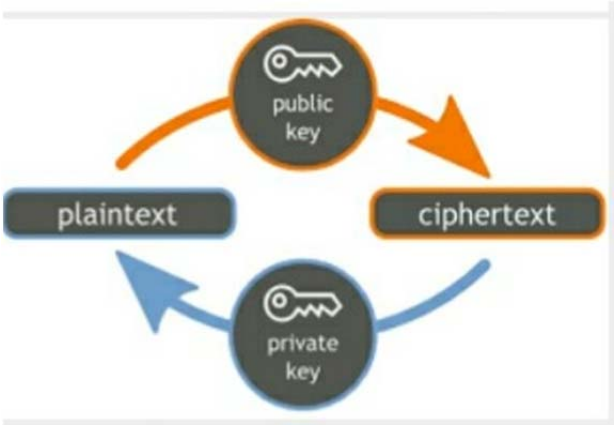
– it is computationally easy to en/decrypt messages when the relevant (en/decrypt) key is known

– Either of the two related keys can be used for encryption, with the other used for decryption only for some algorithm

Public-Key Cryptography: This scheme uses one key for encryption and another for decryption. Modern PKC was first described using a two-key crypto system in which two parties could merge in a secure communication over a non-secure communications channel without having to share a secret key. Here one of the two keys is designated as public key and another one as private key. RSA is one of the first and common public key cryptography implementation that is in use today for key exchange or for digital signatures.
Advantage of this scheme is the administration of the keys on a network requires the presence of only a functionally trusted TTP, as opposed to an unconditionally trusted TTP. And the key used to show the public verification function is typically much smaller than for the symmetric-key counterpart



Public-Key Cryptosystems –



Chosen Cipher text Attacks

• RSA is vulnerable to a chosen cipher text attack
• Attacker chooses cipher texts and gets decrypted plaintext back
• choose cipher text to exploit properties of RSA to provide info to help cryptanalysis

• can counter with random pad of plaintext

• use optimal asymmetric encryption padding

Conclusion and future scope –

The above given scheme is a simple but secured and efficient scheme as proved in this paper. Future work can look on acquiring some compression of data to make a real and very useful enterprise. Also these plan can be modified to add verification of dealer and other participants and also to deal with generalized threshold scheme with weighted participants. In summary, our scheme possesses the following abilities**:**

- The ability to identify the actual signers**.**
- Distributed key generation
- To share recovery scheme

References–

[1] Afolabi, A.O and E.R. Adagunodo, 2012. Implementation of an Improved data encryption algorithm in a web based learning system. International Journal of research and reviews in Computer Science. Vol. 3, No. 1.

[2] Bhoopendra, S.R., Prashanna, G. and S. Yadav, 2010. An Integrated encryption scheme used in Bluetooth communication mechanism. International Journal of Computer Tech. and Electronics Engineering (IJCTEE), vol. 1, issue 2.

[3] DI management (2005) “RSA algorithm”, available at: http://www.di-mgt.com.au/rsa_alg.html.

[4] Gaurav, S., 2012. Secure file transmission scheme based On hybrid encryption technique. International Journal of management, IT and Engineering. Vol. 2, issue 1.

[5] Hellman, M. and J. Diffie, 1976. New Directions in Cryptography. IEEE transactions on Information theory, vol. IT-22, pp:644-654.

[6] Shinde, G.N. and H.S. Fade War, 2008. Faster RSA algorithm for decryption using Chinese remainder theorem. ICCES, Vol. 5, No. 4, pp. 255-261.

[7] Yang L. and S.H. Yang. 2007. A frame work of security and safety checking for internet-based control systems. International Journal of Information and Computer security. Vol.1, No. 2.

[8] Washington, L.C. 2006. Introduction to Cryptography: with coding theory by Wade Trappe. Upper Saddle River, New Jersey, Pearson Prentice Hall.