Rsa cryptographic algorithm research paper sample

Sociology, Communication

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Introduction

Cryptography algorithms broadly refer to the techniques that are used for securing communication in the presence of adversaries. It mainly involves the construction and analysis of protocols that are aimed at overwhelming the effects of the third parties in a communication environment with the principal objective of ensuring data integrity, confidentiality and authentication (Mutyaba, 2010). RSA is an example of a public key cryptographic algorithm that was developed by Rivest, Shamir and Adleman, whereby the key that is used for encrypting the message is not same with the key that is used for decrypting the message although they are related. The RSA cryptographic algorithm mainly used the concept of modular exponentiation. RSA cryptographic algorithm is the first algorithm that has been known to combine both signing and encryption. In addition, the RSA played an integral role in influencing the further advancements in the public key cryptography. Its application is mostly deployed in e-commerce

protocols and is considered to be satisfactorily secure due to the use of long keys and updated implementations (Mutyaba, 2010). This paper discusses the history of the RSA, its security considerations and the areas of its application.

History of the RSA

Public key cryptography makes use of two keys, which includes a public key and private key in order to encrypt messages in a secure manner that does not the communicating entities to exchange the key to ensure message security. For a long time, the cryptographic community consented that the only way for two entities to communicate securely was through an initial exchange of the secret key. With the growth of electronic networks, this approach to encryption key management presented diverse challenges, especially in the context of military communications, enterprise communications and financial transactions. Earlier algorithms of public key cryptography were developed by Whitfield Diffie and Martin Hellman during 1976 and laid emphasis on the development of digital signatures, with the only constraint being that the Diffie-Hellman-Merkle key exchange algorithm was a secure method of distributing the public key but they did not manage to successfully implement digital signatures. The RSA cryptographic algorithm was based on a mathematical function to develop complete public key cryptographic algorithm that was based on the Diffie-Hellman-Merkle algorithm (Mutyaba, 2010).

The invention of the RSA cryptographic algorithm was a significant milestone in the field of network security, which facilitated information security while

still implementing transparency during the exchange of encrypted messages between the users and business entities that do not know each other. The RSA cryptographic algorithm formed the basis of network and internet security and played an integral role in facilitating electronic commerce. The RSA is the most commonly used method when it comes to the the implementation of key public network applications globally. The time-synchronous authentication, which was an innovation of the RSA developed during 1986, has made significant contributions towards the reinforcement of network and information security. The time-synchronous authentication offers strong user authentication using the RSA SecurID tokens, which provides a framework through which enterprises can validate the identity of a user with high levels of certainty (Rhee, 2003).

Security considerations of the RSA cryptographic algorithm

The RSA cryptographic algorithm functions mainly by use of two mathematical problems that entails the problem of factoring large integers and the RSA problem. Decrypting an RSA cipher text is impractical basing on the underlying assumption that these problems are relatively hard in the sense that there is effective algorithm that can used for finding their solutions. Reinforcing security on a partial decryption poses the need to add a secure padding scheme. With regard to the RSA problem, as of 2010, the biggest known integer that could be factored using the general purpose algorithm was established to have a bit length of 768. The RSA keys on the other hand have a bit length of 1024-2048 bits, implying that current factoring algorithms have not been able to break the RSA keys (Mutyaba,

2010). The underlying assumption is the security of RSA depends on its composite n; a sufficiently large n makes it impractical to break the RSA keys. The composite n that is less than 300 is susceptible to being factored by the PC using application software that is already in the market. RSA keys of bit length 512 bits were broken during 1999. The current recommendation is that n should have a minimum bit length of 2048 for the RSA key to be considered sufficiently secure. During 1994, Peter Shor established that breaking the RSA keys can be practically possible in the event that quantum computer be developed in the future and dedicate it to this task using the polynomial time (Rhee, 2003).

Padding also serves to enhance the security of the RSA cryptographic algorithm. Currently, there are no known attacks that have managed to break the RSA keys on occasions that proper padding schemes have been implemented. Improper implementation of padding schemes however increases the susceptibility of breaking the RSA keys, a concept usually referred to as unpadded plain text visibility. The RSA cryptographic algorithm is of a security concern when it comes to the case of timing attacks. If an eavesdropper has sufficient information regarding the recipient’s hardware, one is able to evaluate the decryption times for most of the cipher texts that are known (Mutyaba, 2010).

Therefore, the eavesdropper can figure out the decryption key with ease. Timing attacks can also be implemented in the signature scheme adopted by the RSA. In order to eliminate such potential attacks, the RSA cryptographic algorithm makes use of cryptographic blinding, which deploys the

multiplicative property of the RSA. Most of the potential attacks that can be initiated to the RSA cryptographic algorithm such as the adaptive chosen cipher text attack and side channel analysis attacks can be eliminated by proper implementation of the padding schemes on the RSA. Padding schemes also serve to avoid attacks that can be initiated against the plain RSA such as the Coppersmith Attack (Mutyaba, 2010).

Application of the RSA cryptographic algorithm

The basic application of the RSA cryptographic algorithm is to facilitate secure communication through message encryption, which implies third parties in the communication environment cannot decipher the message. The RSA offers an effective approach towards key management to facilitate transparent and secure communication that encrypted among the people who had never communicated at an earlier time (Mutyaba, 2010).

The RSA is also used in identification and authentication, which are core requirements in facilitating secure communication over the internet. Identification simply entails a verification of an individual’s identity, while authentications serve to make sure that the person is who he/she claims to be. Another application of the RSA is secret sharing, which facilitates the distribution of secrets among a group of individuals. Electronic commerce is one of the wide applications of the RSA cryptographic algorithm with the main objective of ensuring security during business communications and online transactions (Katzenbeisser, 2001).

Conclusion

The increased use of computer networks as a means of communication brought into focus the issue of security and reliability of information and data. Cryptograph techniques provide the best avenues through data can be secured. Development of RSA served as a big milestone because it radically increased the level of security in e-commerce applications. The RSA cryptographic algorithm continues to serve as an integral part of ensuring that there is secure communication between networks.

References

Katzenbeisser, S. (2001). Recent advances in RSA cryptography. New York: Springer.

Mutyaba, R. (2010). Improving the Rsa Cryptographic Algorithm. New York: Lap Lambert

Academic Publishing.

Rhee, Y. (2003). Internet security: cryptographic principles, algorithms and protocols. New

York: John Wiley and Sons.