IRA-International Journal of Technology & Engineering
ISSN 2455-4480; Vol.05, Issue 03 (2016)
Pg. no. 70-76
Institute of Research Advances
http://research-advances.org/index.php/IRAJTE

A Study on Modern Cryptographic Primitives and Signature Schemes

Jyotirmoy Das[1] , Dr. Sangeeta Kakoty [2] , Dr. Majidul Ahmed [3]

[1] Research Scholar, Department of Computer Science and Engineering, Assam Down Town University, Guwahati, Assam, India.

[2] Associate Professor, Department of Computer Science and Engineering, Assam Down Town University, Guwahati, Assam, India.

[3] Assistant Professor, Department of Information Technology, Gauhati Commerce College, Guwahati, Assam, India.

Type of Reviewed: Peer Reviewed.
DOI: http://dx.doi.org/10.21013/jte.v5.n3.p3

How to cite this paper:
Das, J., Kakoty, S., & Ahmed, M. (2016). A Study on Modern Cryptographic Primitives and Signature Schemes. *IRA-International Journal of Technology & Engineering* (ISSN 2455-4480), 5(3), 70-76. doi:http://dx.doi.org/10.21013/jte.v5.n3.p3

ABSTRACT

The access to digital data by the users has increased in recent times with the advent of data communication technologies and its popularization. The data which is in digital form has to pass through insecure channels, for example when a user accesses the Internet, the privacy of data becomes a major issue. The area of Information Security has to play a crucial role when it comes to protecting the privacy of digital data. Cryptography is one such part of Information Security field where a sender's message gets encrypted and the message gets decrypted at the receiver's end. From time to time, various cryptographic schemes have been developed among which the Private Key Cryptography and Public Key Cryptography techniques are prominent. Moreover many special Signature Schemes which are part of cryptographic protocols have been providing security in dealing with digital transactions. This paper focuses on the use of modern cryptographic schemes and their importance in digital data communication system.

Keywords: Digital data, Information Security, Cryptography, Private key, Public key, Signature Schemes

1. INTRODUCTION :

In this age of Internet and digital data, people tend to keep their information in digital form rather than traditional files that maintained manually. Among all digital information, there may be some information which are confidential, which may have more value and more sensitive and thereby consequently not preferred to be known by others. This information might include their bank and other financial details, their geographical locations, as well as professional and network information. Similarly, business organizations and Government agencies also keep sensitive and critical information which they have value. Therefore, it can be said that when using Internet and digital data in various realms, the issues relating to the security of confidential data or information cannot be overlooked, thus framing the science of Information security in a more rigid and secured manner day by day. Computer scientists have come up with Cryptography as a solution to these problems where information gets encrypted from a sender's end on transaction and decrypted at the receiver's end [2]. Different cryptographic schemes have been developed at different times among which Private Key Cryptography, Public Key Cryptography and a few special Signature Schemes have been providing security in dealing with digital transactions.

2. CRYPTOGRAPHY :

Cryptography is considered as one of the oldest methods employed by ancient civilizations for secret communications. The Egyptians in particular is known to have used cryptography on the tombs of deceased kings and rulers. The Greeks of Classical times are said to have known of the methods of encrypting and decrypting information, for instance the scytale transposition cipher claimed to have been used by the Spartan military. Methods like Steganography was also first developed in ancient times, which hides even the existence of a message. One of the famous methods in the history of Cryptography was 'Caesar Cipher' which was invented by Julius Caesar. The 'Caesar Cipher' used the substitution cipher method where the alphabets were shifted by a constant number of steps. For example this cipher would shift an "A" to "D" or a "B" to "E". Also, we can perform a multiplication with a constant which will lead us to the 'Affine Cipher' method which was another most pospular historical ciphers used back in the early days and is still implemented in some legacy applications.

Modern cryptography is the scientific study of techniques for securing digital information, transactions, and distributed computations [1]. Historically, cryptography was mostly used by military and intelligence organizations. However, nowadays cryptography is used in almost every sphere. Most of the times when we access a secured application, we go through some process Cryptographic primitives. Complex scientific techniques are employed for designing an algorithm for a modern cryptosystem and these algorithms are based on computational hardness which makes it difficult for adversaries to break

into the system. A modern cryptosystem is all about the design and analysis of various methods that are related to data security, integrity and authentication [7][9]. To assure that a particular system is secure, Cryptanalysts try to break the methods used in building the system. Cryptography and Cryptanalysis together constitute to define what is known as "Cryptology". The following figure shows how a crypto-system works in general –

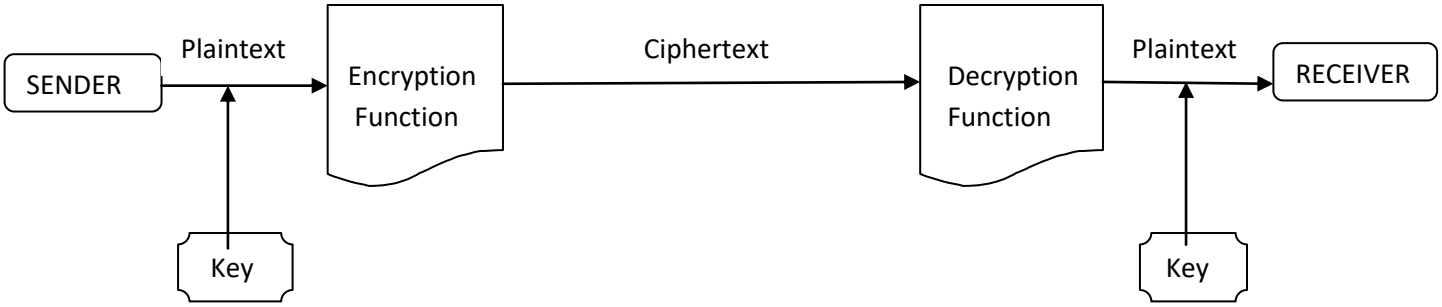

Fig 2.1: A typical crypto-system

A cryptographic system (or cryptosystem) has five components [5]:

1. A plaintext message space, ɱ
2. A ciphertext message space, ɕ
3. A key space, Ƙ
4. A family of enciphering transformations, E_K: ɱ -> ɕ, where K ∈ Ƙ
5. A family of deciphering transformations, D_K: ɕ -> ɱ, where K ∈ Ƙ

The field of Modern Cryptography is categorized into three main branches. The following figure shows the branches of Modern Cryptography :

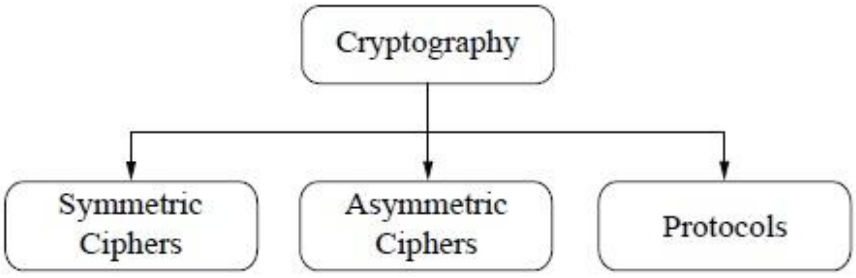

Fig 2.2: Branches of Modern Cryptography

2.1 Symmetric Key Cryptography :

Until the mid 1970s, cryptography was exclusively based on symmetric key algorithms. Here, a single key is used for both encryption and decryption process [12]. Both the parties must agree on the secret key before the actual exchange of data takes place. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data [10]. Symmetric Key Ciphers are broadly classified into two categories –Stream Ciphers and Block Ciphers. A stream cipher breaks the plaintext message 'm' into successive characters or bits m_1, m_2, . . . and enciphers each m_i with the i^{th} element k_i of a key stream K = k_1,k_2. . . whereas , a block

cipher breaks 'm' into successive blocks (each block is typically several characters long.) m_1, m_2 . . . . . and enciphers each m_i with the same key K; that is , $E_K(m) = E_K(m_1)E_K(m_2)$ . . . Symmetric ciphers are still in widespread use, especially for data encryption and integrity check of messages.

2.2 Asymmetric or Public-key cryptography :

The concept of two-key cryptosystems known as the Public key Cryptosystem or Asymmetric Key Cryptosystem was introduced in 1976 by Whitfield Diffie, Martin Hellman and Ralph Merkle [5]. In this scheme, each user requires a private key and a public key [8][15]. During the entire communication process, the public key can be known to all, but the private keys of each users should be kept secret by them. Asymmetric crypto-algorithms can be used for applications such as digital signatures and key establishment, and also for classical data encryption. Public key algorithms, unlike symmetric key algorithms, do not require a secure initial exchange of secret keys between the parties [13]. Public-key cryptography is used as a method of assuring the confidentiality, authenticity and non-repudiability of electronic communications and data storage.

2.3 Cryptographic Protocols :

Before cryptographic protocols were proposed, the field of cryptography was concerned only with encryption and decryption process. In recent times, the field of cryptography has expanded and many security services have been added to ensure security. Among them confidentiality, message authentication, message integrity and non-repudiation are among the few most important security services offered under cryptographic protocols.

Cryptographic protocols deal with the application of cryptographic algorithms [14] for ensuring the privacy, confidentiality, authentication of information. Symmetric and asymmetric algorithms can be viewed as primitives to develop various applications for secured Internet communication. Cryptographic protocols use these primitives as building blocks to build secure modern services. The Transport Layer Security scheme, which is used in every Web browser, is an example of a cryptographic protocol.

The introduction of cryptographic protocols such as signature schemes can be considered as one of the major development in the field of cryptography. In order to provide secure communication for various applications, protocols such as digital signatures have been employed in critical applications such as secure web browsing for e-commerce like applications and hence they have become an essential part of modern crypto-systems.

3. SIGNATURES SHEMES AS A SECURITY NEED :

Although Public Key Algorithms are secured enough when compared with Private Key Algorithms, they were still vulnerable to a few attacks among which the so-called man-in-the-middle attack is one most prominent attack. Here, we assume a person (S) is communicating with another person (R) in a public key environment. The person S publishes his public key, thereby enabling him to send and receive messages from his companion through a secure method. However, another person (T) in the middle, is making independent connections with the other two and sending messages between them, making both S and R believe that they are talking directly to each other. To solve this problem, the notion of Public Key Infrastructure (PKI) certificate was introduced enabling users of the system to combine their public key with a digital signature issued by some Certification Authority (CA), which shows that they indeed own the public keys they claim to. In other words, PKI certificate is a security mechanism for public keys.

A signature is accompanied by two essential information− the identity of the signer and the signed message. Various types of signatures schemes for privacy have been proposed based on different application demands.

3.1 Various Signature Schemes :

A Digital Signature is a cryptographic security scheme which demonstrates the authenticity of a message that is being transferred from a sender to a receiver over an insecure network such as the Internet [14]. A digital signature provides reasons for the receiver to believe that the message received, was really sent by the claimed sender which provides a way to detect forgery or tampering. Here, a signer S has a private key and a public key. A user U wants to get a message m signed by S. S generates the signature σ (***sigma)*** with an algorithm which takes input m and S's private key and sends σ (***sigma)*** to U. On the other end U can verify using a verification algorithm which uses S's public key.

There are many applications of Digital signatures in information security, which includes authentication, data integrity, and non-repudiation [14]. Among others, one of the significant applications of digital signatures is the certification of public keys in large networks. The first signature scheme was the RSA Signature scheme which was proposed by Rivest, Shamir and Adleman. The security of the RSA signature scheme was based on the well-known RSA assumption. The RSA scheme is subject to forgery and so it is not secured. In other words, it is easy to create a valid message-signature pair without asking the signer directly. Moreover, it is seen that if the message is too long then the signature takes a long time to be computed or the message does not remain in the domain of the signing function.

It has been found that by introducing a special method called hash function into the scene, the problems regarding RSA signature scheme can be solved. A hash function computes a short, fixed-length bit-string called a message-digest which can be used as a unique representation of the message. Now, by signing the message-digest instead of signing the message itself the security of the signature scheme is retained. The Digital Signature Algorithm (DSA) is an example of a hash enabled signature scheme which was published in early 1990s and is widely used. The DSA uses a public key of atleast 1024 bits. A variant of the DSA is the Elliptic Curve Digital Signature Algorithm (ECDSA), was later introduced, which uses elliptic curve cryptography. One of the advantages of ECDSA over DSA is that the ECDSA uses a public key of 160 bits.

Another variant of a Digital Signature is a Blind Signatures which have the functionalities of digital signatures and some additional features. A blind signature scheme is a protocol for obtaining a signature σ (***sigma)*** on ***m*** from the signer S such that S does not learn anything about σ (***sigma)*** and m. Here the user U generates a secret random number r, embeds it into m to obtain m' , the blinded message and sends m' to S. S generates signature σ' on m' and returns it to U. U then removes the random blinding factor to obtain σ (***sigma)***, the signature on m. Hence, both m and σ (***sigma)*** remains hidden from S [3]. In a Blind Digital Signature scheme, the signer does not know the content of message in the signing phase [4]. In general, a blind signature scheme should meet the following four requirements:

i. **Completeness** : Completeness means that if the signer S and the user U both agree with the blind signature algorithm, then the output of the blind signature verification algorithm will always accept the signature **σ,** thus always generating the output as *'true'*.

ii. **Blindness :** Blindness is the condition where it is not possible for the signer S to link any valid message-signature pair (**m, σ**) to any other instance of message / signature pair.

iii. **Unforgeability:** Unforgeability refers to the condition for an attacker who has no clue about sk, the only way for the attacker to obtain (**m, σ**) is to execute the signature generation algorithm with a signer holding private key *sk*.

iv. **Untraceability:** Untraceability means that the signer S of the blind signature is unable to link the message-signature pair (**m, σ**) even when the signature has been revealed to the public [11].

The first blind signature scheme, which was based on RSA and the hardness of the factoring problem, was proposed by David Chaum. He wanted to create an electronic version of money such that it

is secure against double-spending. Chaum proposed an RSA-based online e-system where the bank checks online whether a coin has been spent or not. This theory was not practical because the bank databases are quite large and real time searching takes a lot of time. Chaum then proposed an RSA-based offline version of the blind scheme which was able to solve the double-spending problem.

In 1994, Camenisch, Piveteau, and Stadler proposed two blind signature schemes in [13]; one was based on the modified Digital Signature Standard (DSA) and the other was based on Nyberg-Rueppel signature scheme [15]. E. Mohammed, A.E. Emarah, and K. El-Shennawy proposed a blind signature protocol based on El-Gamal signature scheme which has the advantage of being efficient, faster and simpler than RSA in the blinding procedure. The anonymity of the signatures generated by the new method is higher than that of RSA can be utilized to offer privacy enhancement and unlinkability in electronic banking operations and e-commerce transactions [6].

4. CONCLUSION :

This paper has reviewed Cryptography and its various types which include Symmetric Key Cryptography, Asymmetric Key Cryptography and Protocols which consists of cryptographic essentials such as Signature Schemes. It has been observed that both Symmetric key and Asymmetric Key Cryptography is concerned with encrypting the information that has been sent across insecure channels. On the other hand, Signature schemes are concerned with the authenticity, confidentiality, and data integrity during the communication process. Each technique is unique in its own way, which might be suitable for different applications. Everyday new schemes are emerging and hence fast and secure conventional techniques will always work out with high rate of security.

ACKNOWLEDGEMENT

The first author acknowledges the academic support given by Assam down town University (AdtU), Guwahati, Assam.

REFERENCES

[1] Ahmed Al-Vahed , Haddad Sahhavi , 2011, “An overview of modern cryptography”, World Applied Programming, Vol (1), No (1), April 2011. 55-61

[2] Ahmed M, Sazzad T. M., Mollah E., 2012, “Cryptography and State-of-the-art Techniques” IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, March 2012

[3] Asghar N., 2011, “A Survey on Blind Digital Signatures”

[4] D. Chaum,1982 “Blind signatures for untraceable payments,” in Advances in Cryptology, CRYPTO’82, pp. 199–203, 1982.

[5] Denning D.E.. 1982, “Cryptography and Data Security”, Addison-Wesley Publishing Company; 1st edition (June 1982)

[6] E. Mohammed, A.E. Emarah, and K. El-Shennawy. *A blind signature scheme based on ElGamal signature.* IEEE/AFCEA EUROCOMM 2000 Information Systems for Enhanced Public Safety and Security, pp. 51-53, 2000

[7] John Justin M, Manimurugan S, 2012, “A Survey on Various Encryption Techniques” International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012

[8] Kakkar A., Singh M. L, Bansal, P.K., 2012, "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network" International Journal of Engineering and Technology Volume 2 No. 1, January, 2012

[9] Kaushik S., Singhal A., 2012, "Network Security Using Cryptographic Techniques" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 12, December 2012

[10] Kumar Y., Munjal R., Sharma H., 2011, "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011

[11] Lee C.C., Yang W., Hwang M., 2003, "Untraceable Blind Signature Schemes Based on Discrete Logarithm Problem", Fundamenta Informaticae 55 (2003) 1–13, IOS Press

[12] Malhotra M, Singh A, 2013, "Study of Various Cryptographic Algorithms" International Journal of Scientific Engineering and Research (IJSER) Volume 1 Issue 3, November 2013

[13] Manakshe A., Dalu A.P., Mutkule R., 2014, "Survey on Various Cryptography Methods" International Journal of Research in Advent Technology, Vol.2, No.2, February 2014

[14] Paar C, Pelzl J., 2010, "Understanding Cryptography-A Textbook for Students and Practitioners", Springer; 1st ed. 2010 edition

[15] Singh M, Gupta S, Bhushan B, 2012, "Comparison of symmetric and asymmetric key cryptography: A study" , IJMRS's International Journal of Engineering Sciences, Paper from Proceeding of the National Conference "Science in Media 2012" Organized by YMCA University of Science and Technology, Faridabad, Haryana (India) December 3rd -4th 2012