ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.5

A Survey Paper on All Cryptographic Techniques

Smruti .P. Patil[1], Prerna .B. Solanke[2], Darshana .N. Tambe[3]
Assistant Professor[1, 2, 3]
Department of Information Technology
PVPPCOE, Mumbai, Maharashtra, India

Abstract:
Cryptography has very long history, from ancient ciphers, such as Ceaser cipher, machine (or rotor) cipherx during WWI and WWII, and modern ciphers, which play a fundamental role in providing Confidentiality, Integrity, and Authentication services during transmission, processing, and storage of the sensitive data over the open or public networks. The cryptographic protocols that makes some agreements or decisions between two parties or multiple parties over the Internet using cryptosystems and hash functions provides key management, authentication, verification, and identification protocols into the practice. The security of the cryptographic protocols must be proved in detail under some theoretical assumptions before practical use. Nowadays, new types of secure or private protocols are becoming practical. New types of cyber businesses are available. Every day, we can enjoy cryptography to send a secure message over SNS (Social Network Service) to your friends, to secure financial transactions over the Internet, etc. Everyone can understand that security and privacy, as well as cryptography, are everywhere.

Keywords: Public Key encryption, Data Encryption Standard, Authentication Key Exchange.

I. INTRODUCTION:

Public key cryptography has various useful applications and the technique employed depends on the requirements of the application to be designed for. The rapid development in information technology, the secure transmission of confidential data herewith gets a great deal of attention. The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized user for malicious purpose. Therefore, it is necessary to apply effective encryption decryption methods to enhance data security. In 1949, Shannon [1], known as the father of information theory, introduced the seminal idea to construct secure block cipher using iterating cryptographically weak and simple functions ,such as confusion and diffusion, as many times, even though each functions are popularly used in classical ciphers and are easily cryptanalyzed by cipher text-only attacks. Based on Shannon's idea, DES (Data Encryption Standard) was developed in 1977 by the joint team of IBM and NSA as NIST (National Institute of Standards and Technology). DES is 64-bit plaintext and 56-bit key, of which security depends on Kerckhoff's principle—any secure system must be secure even if the system can be completely known to attackers, except for the secret key. NIST believed that DES could not be broken by key-exhaustive search attacks, which requires 256 operations. However, Biham and Shamir [2], in 1990, suggested the very clever DC (Differential Cryptanalysis), which utilizes the probabilistic significant distribution of bit-by-bit Exclusive Oring between subsets of plaintext and ciphertext iteratively. They found that the complexity to break DES using DC requires 247 operations. In 1992, Matsui [3] developed a more sophisticated breaking method of DES than DC, called LC (Linear Cryptanalysis), which requires 243 operations by utilizing probabilistic significant distribution between linear subsum of plaintext and ciphertext. This is a dramatic contribution to the breaking of DES in the sense that DC and LC require less complexity than a key-exhaustive search attack. Due to these notorious attacks, DES was deleted from the federal standard, and changed to use DES 3-times to increase the size of the key to a 112-bit for 128-bit block cipher. In 1999, Kocher et al. [4] introduced a very powerful attacking method called SCA (Side Channel Attack) by monitoring the timing or the power consumption during an encrypting operation to derive a part of the secret key with 100% accuracy, correctly embedded into the secure device. The designer must check the security of a block cipher from this type of powerful attack, in addition to the complexity of a key-exhaustive search attack. NIST changed the policy for standard algorithms by announcing a call-for-algorithm, all over the world, in 1997. After a three-year public debate, AES (Advanced Encryption Standard) [5] was chosen from the Rijndael block cipher with variable key size from 128-bit to 256-bit in 2000. AES was proved to be secure against DC and LC. In 2000, Berson [6] gave the IACR (International Association for Cryptologic Research) distinguished lecture entitled "Cryptography Everywhere" at Asiacrypt2000. There is a strong demand to apply cryptographic techniques to, not only ICT (Information Communication Technologies), but also merged applications it ICT, such as smart cars, smart embedded devices, smart grids, service robots, etc. Cryptography (ISSN 2410-387X) was established to provide a state-of-the-art forum for original results in all areas of modern cryptography, we focus mainly on areas that include, but are not limited to:

Theory of Cryptography

- Secret-key cryptograph
- Public-key cryptography
- Hash Functions
- Cryptanalysis
- Cryptographic Protocols

- Quantum Safe Cryptography

Practice of Cryptography

- Cryptographic Hardware/Engineering
- Applied Cryptography
- Secure Smart System/Device
- Digital Forensics
- Digital Rights Management

In 1976, Diffie and Hellman [2] proposed the influential idea to generate a common secret key over the public channel, between any two parties in a network, by exchanging their public keys to other party derived from their private keys. This was the historical birth of PKC (Public Key Cryptosystem), of which security depends on the difficult problems from the number theory. If public parameters, including the public keys are known (or public) to anyone, the complexity to derive the corresponding private key is computationally difficult, even if using the best-known algorithms by massively parallel digital computers. The security of DH (Diffie Hellman) key distribution depends on DLP (Discrete Logarithm Problem). In1978, RSA (Rivest, Shamir and Adelmann) [2] extended DH' side a to construct a one-way trapdoor function under the composite number, which is a product of large prime numbers. The security of RSA depends on the computational difficulty of IFP (Integer Factorization Problem). DLP and IFP are found to have almost similar sub-exponential complexity. PKC can provide a digital signing capability to make secure transactions over a public network to be feasible, such as secure electronic payment, secure electronic voting, auctions, etc. Miller and Koblitz, coincidently, suggested the idea to use an elliptic curve instead of a number field in 1985 and 1987, respectively. This was the birth of Elliptic Curve Cryptosystem (ECC) which uses 1/6 key size of RSA to guarantee the equivalent security. When we generate a digital signature of arbitrary length for a message, we need to compress the message, using the cryptographically hash function. Merkle and Damgard suggested an efficient construct collision resistant hash function from collision-resistant one-way compression function. In 1995, NIST adopted the standard of hash function SHA-1, which was cryptographically secure for 10 years. In2004, Wangetal [2] found an efficient algorithm to find a collision of previous hash functions. In 2009, Steven etal. showed how to make a rogue certificate of any issued certificate if the MD (Message Digest) 5 hash function is used to generate the digital signature. NIST was very anxious of these kinds of collision attacks and initiated the SHA-3 project, very similar as AES in 2007. Many proposals for SHA-3 candidates were submitted in 2008. The finalist of SHA-3 was Keccak [6], which can meet all the security requirements of SHA-3 and has a very unique sponge function. The cryptographic protocols that makes some agreements or decisions between two parties or multiple parties over the Internet using cryptosystems and hash functions provides key management, authentication, verification, and identification protocols into the practice. The security of the cryptographic protocols must be proved in detail under some theoretical assumptions before practical use. In 1984, Shor [6] proposed a polynomial time algorithm to solve IFP or DLP if the attackers have access to quantum computers, which have quite different computing architectures compared to digital computers. If a quantum computer, with a sufficient number of qubits, could operate without succumbing to noise and other quantum decoherence phenomena, Shor's algorithm could be used to break PKC, such as the widely-used RSA or ECC. It was also a powerful motivator for the design and construction of quantum computers, and for the study of new quantum computer algorithms. It has also facilitated research on new cryptosystems, which are secure from quantum computers, collectively called post-quantum cryptography or quantum-safe cryptography.

II. NETWORK SECURITY

Cryptography is an emerging technology, which is important for network security. Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security along with Cryptography is a concept to protect network and data transmission over a wireless network. Data Security is a perplexing issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The conventional methods of encryption can only maintain the data security. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. [7] The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password [1]. Network security starts with authenticating the user, commonly with a username and a password. Since this requires just one detail authenticating the user name —i.e. the password, which is something the user 'knows'— this is sometimes termed one factor authentication. With two-factor authentication, something the user 'has' is also used (e.g. a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g. a fingerprint or retinal scan). Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users [1]. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) helps detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network and traffic for unexpected (i.e. suspicious) content or behavior and other anomalies to protect resources, e.g. from denial of service attacks or an employee accessing files at strange times. Network Security is achieved by the implementation of different algorithms like Diffie Hellman key exchange, AES, Hash etc. All are compared using simple RISC style processor with ALU and shifter and workload characteristics can be determined. Aameer Nadeem et.al presented, performance of 4 secret key algorithms (DES, 3DES, AES, Blowfish) were compared by encrypting input files of various contents and sized on different hardware program. The algorithms have been implemented in a uniform language, using their standard specifications, to allow a fair comparison of execution speeds. Pentium-II having frequency 266MHz (running Microsoft Windows OS) and Pentium-IV with 2.4 MHz machine (running Windows XP OS) are the basis for time

measurement with their goal to measure the encryption times of considered algorithms.[8] The performance results have been summarized and discussed a tradeoff between performance and security and a conclusion has been presented. The performance measurement approach was JAVA in which Blowfish was the fastest algorithm among DES, 3-DES, AES and Execution results are presented in ECB mode (for block ciphers) and CFB (for stream ciphers) and concluded on the basis that an algorithm having more complex rounds and a larger number of rounds is generally considered more secure. So, concluded Blowfish as the fastest one among all. Kyung Jun Choi et.al investigated various cryptographic algorithms suitable for used in wireless sensor network utilizing MICA z-type motes & Tiny OS is investigated. Usage of resources including memory, computational time and power for each cryptographic algorithm was characterized experimentally. MD5 and RC4 showed best performance in terms of power dissipation and in terms of cryptographic processing time used. Neetu Settia et.al discussed the security and attack aspects of cryptographic techniques and also discussed the dominant issues of security and various attacks. Finally, bench marked some well-known modern cryptographic algorithms in search for the best compromise in security. In this paper, CrypTool was used as a simulator to conduct the experiments and to get the result. Only alphanumeric and special characters are used for analysis of cryptographic techniques. These specifications are selected in option menu of the CrypTool and visual results are set in window option of the CrypTool. For the input plaintext, around 25-sample text are taken and encrypted with various algorithms. The output of above plaintext is cipher text, analyzed with analysis option in CrypTool. Some of the cryptographic algorithms are implemented in C, and their output is taken as cipher text, which is then copied in some text file and that text file is used for the analysis with CrypTool [9]. Most of the network security methods adopts symmetric key cryptography for providing protection schemes for guaranteeing identity hiding. After the research by the scientists of CHINA named as Hongfeng Zhu, Yifeng Zhang, and Yang Sun, they wiped out the symmetric cryptography, and only use chaotic maps, a secure one-way hash function to construct a provable privacy-protection system (PPS) which can achieve two kinds of privacy protection and switch between them optionally by users: The first is anonymous scheme which can make nobody know the user's identity, including the server and the registration center (RC), and they only know these users are legal or paying members. The other is hiding scheme which owns also privacy-protection property, because the user's identity is not transferred during the process of the proposed protocol, and only the server and the RC know the user's identity. About practical environment, we adopt multi-server architecture which can allow the user to register at the RC once and can access all the permitted services provided by the eligible servers. Then a new PPS authenticated key agreement protocol is given based on chaotic maps. Security of the scheme is based on chaotic maps hard problems and a secure one way hash function.[10]

III. AUTHENTICATED KEY EXCHANGE (AKE)

It is one of the most important cryptographic components which is used for establishing an authenticated and confidential communication channel. Based on the number of participants, we can divide AKE protocols into three categories: two-party AKE protocols [10], three-party AKE protocols and N-party AKE protocols [11, 12]. Furthermore, based on the respective features in detail, the previous AKE protocols [10] can be classified into many categories, we use two-party AKE protocols to set an example: such as password-based [10], chaotic map-based [13], ID-based, anonymity[10], secret sharing and so on. Recently many researchers achieve AKE in the multi-server environment called multi-server authenticated key agreement (MSAKA) protocols. MSAKA protocols allow the user to register at the registration center (RC) once and can access all the permitted services provided by the eligible servers. In other words, users do not need to register at numerous servers repeatedly. MSAKA protocols mainly want to solve the problems in a traditional single server with authentication schemes [11] which lead to the fact that user has to register to different servers separately. About MSAKA protocols, the pioneer work in the field was proposed by Li et al. in 2001. However, Lin et al. pointed out that Li et al. s scheme takes long time to train neural networks and an improved scheme based on ElGamal digital signature and geometric properties on the Euclidean plane has also been given. At the present stage, the research emphasis shifts to functionality and user experience. Therefore, identity-based MSAKA protocols, based on bilinear pairings or elliptic curve cryptosystem (ECC) MSAKA protocols, dynamic identity-based MSAKA protocols and other MSAKA protocols came up recently.

IV. MULTI-SERVER ARCHITECTURE

In the multi-server environment [14], each user must perform authentication procedure to login the server for a transaction. If the user is in single authentication architecture, then the user must register at various servers and memorize the corresponding identifications and passwords, which could not be convenient for a user. In order to make the registration to various servers easier for users, each user must register with the registration center to obtain a secure account. Then the user uses the secure account to perform the login and authentication procedures with various servers. Secure communication schemes for remote one-way authentication and session key agreement for the multiserver architecture should provide security requirements such as Authentication, Impersonation Attack, Man-in-the-Middle attack, Replay attack, Known Key Security, Perfect Forward Secrecy, and Session key Security.

V. KINDS OF AUTHENTICATION

Anonymity ensures that a user may use a resource or service without disclosing the user identity completely. **ID hiding** usually means that a user may use a resource or service without disclosing the user identity during the protocol interaction, which is a kind of privacy protection partly. A pseudonym is an identifier of a subject other than one of the subject real names. ID hiding usually uses pseudonym to realize. Because the server may store the user identity. **OTP (one-time password)** usually means that the password can be used only once but the ID is plaintext during the protocol interaction, so there is no privacy protection. The above-mentioned terms related with authentication called anonymous authentication, hiding identity authentication and OTP authentication.

Anonymous Authenticated Key Agreement Phase
In this phase, the anonymous authentication has three meanings: (1) The server and the RC authenticated each other (2) The RC will help the server to authenticate the premium user, but no one knows (including the server and the RC) the premium user's identity. (3) The RC will help the premium user to authenticate the server.

VI. CONCLUSION:

In this survey paper, we have seen the different cryptographic techniques and their approaches for providing security to the data. All the techniques have some or more advantages and disadvantages and therefore the new techniques have been evolved. This paper exposed the importance of different cryptographic techniques to provide the secure and fast transmission of data through the wireless medium.

VII. REFERENCES:

[1]. Shannon, C.E Communication Theory of Secrecy Systems, Bell System Tech J 1949 28, 656-715.

[2]. Cryptography: A New Open Access Journal . Editor i n Chief Journal Cryptography, School Of Computing, Korea Advanced Institute Of Science And Technology (KAIST). Published Feb 2016.

[3]. Matsui, M. Linear Cryptanalysis Method for DES Cipher. In Advances in Cryptology—EUROCRYPT '93, SPRINGER, BERLIN AND GERMANY, 1993.

[4]. Kocher, P.; Jaffe, J.; Jun, B. Differential Power Analysis. In Advances in Cryptology—CRYPTO' 99; Springer: Berlin, Germany,1999; pp. 388–397.

[5].Announcing the Advanced Encryption Standard (AES). Available online: http://csrc.nist.gov/ publications/ fips/fips 197/fips-197.

[6]. Bertoni, G.; Daemen, J.; Peeters, M.; van Assche, G. The KECCAK Sponge Function Family. Available online: http:// keccak.noekeon.org/ (accessed on 1 February 2016).

[7]. Network Security Using Cryptographic Techniques. IJARCSSE, Volume2, Issue 2, December 2012

[8]. Murat Fiskiran, Ruby B. Lee, ―Workload Characterization of Elliptic Curve Cryptography and other Network Security Algorithms for Constrained Environments‖, IEEE International Workshop on Workload Characterization, 2002. WWC-5. 2002.

[9]. Suhaila Orner Sharif, S.P. Mansoor, ―Performance analysis of Stream and Block cipher algorithms‖, 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010.

[10]. Hongfeng Zhu, Yifeng Zhang, and Yang Sun."Provably Secure Multi-server Privacy-Protection System Based on Chebyshev Chaotic Maps without Using Symmetric Cryptograph". International Journal of Network Security, Vol.18, No.5, PP.803-815, Sept. 2016.

[11]. H. Li, C. K. Wu, J. Sun, "A general compiler for password-authenticated group key exchange protocol," Information Processing Letters, vol. 110, no. 4, pp. 160–167, 2010.

[12]. T. Y. Wu, Y. M. Tseng, and T. T. Tsai, "A revocable ID-based authenticated group key exchange protocol with resistant to malicious participants," Computer Networks, vol. 56, no. 12, pp. 2994–3006, 2012

[13]. M. S. Baptista, "Cryptography with chaos," Physics Letters A, vol. 240, no. 1, pp. 50–54, 1998.

[14]. L. H. Li, I. C. Lin, and M. S. Hwang, "A remote password authentication scheme for multi-server architecture using neural networks," IEEE Transactions on Neural Networks, vol. 12, no. 6, pp. 1498–1504, 2001