International Journal of Electrical and Computer Engineering (IJECE)
Vol. 7, No. 4, August 2017, pp. 2232~2240
ISSN: 2088-8708, DOI: 10.11591/ijece.v7i4.pp2232-2240

A Survey on Comparisons of Cryptographic Algorithms Using Certain Parameters in WSN

Pooja Singh, R.K. Chauhan
Departement of Computer Science and Applications, Kurukshetra University, India

Article Info

Article history:

Received Feb 22, 2017
Revised May 31, 2017
Accepted Jun 14, 2017

Keyword:

Cryptographyalgorithms
Decryption
Encryption
Security

ABSTRACT

The Wireless Sensor Networks (WSNs) have spread its roots in almost every application. Owing to their scattered nature of sensor nodes, they are more prone to attacks. There are certain applications e.g. military, where sensor data's confidentiality requirement during transmission is essential. Cryptography has a vital role for achieving security in WSNs.WSN has resource constraints like memory size, processing speed and energy consumption which bounds the applicability of existing cryptographic algorithms for WSN. Any good security algorithms has higher energy consumption by the nodes, so it's a need to choose most energy-efficient cryptographic encryption algorithms for WSNs. This paper surveys different asymmetric algorithms such as RSA, Diffie-Hellman, DSA, ECC, hybrid and DNA cryptography. These algorithms are compared based on their key size, strength, weakness, attacks and possible countermeasures in the form of table.

Corresponding Author:

Pooja,
Departement of Computer Science and Applications,
Kurukshetra University,
Kurukshetra, 136118, Haryana, India.
Email: poojasingh59@ymail.com

1. INTRODUCTION

WSN consists of hundreds or even thousands of autonomous devices called sensor nodes. The main components of sensor network are: sensing field, sensor nodes, base station and internet. The main components of sensor node are: controller, transceiver, power supply, memory and one or more sensors. These nodes have the sensing, processing and communication capabilities to monitor the real-world environment. WSNs have the advantage over the traditional networks in terms of scalability, deployment, applications, robustness, etc. As they are ad-hoc in nature, hence can be deployed in any area like military, environmental observation, syndrome surveillance, supply chain management, fire detection, vision enabling, energy automation, building administration, gaming, health and other commercial and home applications [1].

Because of its broad usage in multifarious applications, security becomes the primary issue in WSN. When we provide security to sensor networks, it is more complicated than that of MANET because of the resource limitations of sensor nodes. There are some resource constraints such as energy and power supplies, limited memory, computation and communication capabilities. This is the reason that traditional cryptographic techniques cannot be applied on sensor networks, hence demand of more security in WSNs arises. The security requirements in WSN are authentication, confidentiality, availability, integrity and QoS. These conditions should be met while developing the security algorithm.

2. OVERVIEW OF CRYPTOGRAPHY

Cryptography is a Greek word which means to protect the information by converting it into an unreadable form. By doing so, an unwanted user cannot access information or data. In other words, we can say that it's a technique to hide the data over the communication channel [2]. When sender transforms the data using some cryptographic techniques and a specific key into other form then it is known as cipher text and sends it to the receiver. This process is known as Encryption. Receiver receives the cipher text as input and transforms it back to the plain text with the help of known key. This process is called Decryption. This process is shown in following Figure 1:

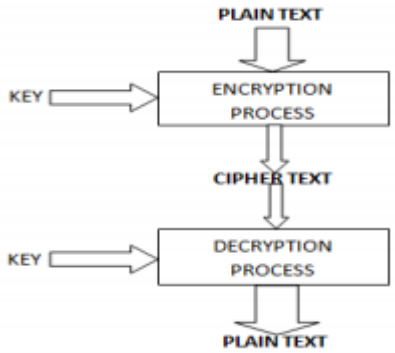

Figure 1. Process of cryptography

The two well-known categories of ciphers are symmetric (or secret) key ciphers and asymmetric (or public) key ciphers. Both of them uses different and unique mechanisms to achieve security. Symmetric key cryptography focuses on the structure of simple iterative cryptographic operations and asymmetric cryptography depends on the difficulty of a mathematical problem [3]. If network designers' priority is energy conservation, then symmetric key ciphers are preferred for use in the encryption of data transmitted by a sensor node [3]

The traditional cryptographic algorithms cannot be applied on sensor nodes because of their resource constraints. For these type of networks, key management scheme is best suitable to achieve security. For secure communication, key must be exchange securely between the nodes before the exchange of information. The key management is multi-operational technique in which first key is generated, then this key is distributed and exchanged among the nodes, then used by the sender and receiver, after successful and secure transfer of information keys are abolished and then refreshed. Hence, we can say that the main steps in key management scheme are: generation, distributed, exchanged, used, abolished and refreshed. There are many key management schemes for the WSNs [4].

Based on the encryption algorithms, the key management schemes are categorized into three types: symmetric key management, asymmetric management and hybrid key management techniques. Symmetric key (or private key) management scheme uses the same key at both sides i.e. sender and receiver use the common key for encryption and decryption. This technique is reliable and rapid fast, but it lacks resilience, scalability and connectivity. The main disadvantage of this scheme is that both parties should exchange the key securely [4]. Asymmetric key (or public key) management uses two different keys at both sides.The key used for encryption i.e. on sender side is called as public key and for decryption i.e. on receiver side is private key. The well-known public key cryptography techniques are: Ron Rivest, Adi Shamir and Leonard Adleman (RSA), Elliptic Curve Cryptography (ECC) and Hyperelliptic Curve Cryptography (HECC) [4]. Recently many researchers proved that the public key cryptography is suitable for resource constrain networks. Both the symmetric and asymmetric schemes have trade-off between the security and its resources are constraint [4]. The main problem ofconventional Public key Cryptosystems is that the Key size has to be sufficiently large in order to meet the high level security requirement, resulting in lower speed and consumption of more bandwidth [5].The third technique i.e hybrid key technique which is the combination of symmetric and public key cryptography. It merges the advantages of both schemes.The feasibility of public-key cryptography (PKC) has been proven [6]. PKC is getting more attention in WSNs due to the reason that it can easily resolve two fundamental and difficult problems, authentication and symmetric key distribution, with the help of Digital signature algorithm (DSA) and Diffie-Hellman key exchange [7][8]. Most researches applied ECC which has much smaller overhead than RSA, but ECC procedures are still heavy to resource-constrained sensor nodes [9]. ECC is best as compared to RSA [10].

The paper will now discuss and survey some of the public key cryptography schemes.

3. PUBLIC-KEY CRYPTOGRAPHY ALGORITHMS IN WSN

3.1. RSA Algorithm

RSA is one of the techniques for public key encryption. It was the first algorithm to be developed in public-key cryptography, and one of the first great achievements in public key encryption. It involves three steps: [11]

1. Key Generation
2. Encryption
3. Decryption

Phase 1: Key Generation

RSA uses two keys for its process. Encryption is done with receiver's public key and decryption is done with receiver's private key. To generate a key, it uses following steps:

1. Choose two distinct and large prime numbers say, P and Q.
2. Calculate N such that, N= P*Q.
3. Calculate z such that, z= (P-1)*(Q-1).
4. Choose public key exponent say, E such that 1 < E < z and E and z share no Divisors other than 1.
5. Determine D which satisfies the congruence relation. E*D = 1 (mod z).
   E is divisible by smallest of the series: z+1, 2z+1, 3z+1, 4z+1, ……..so on.
   Now, Public Key: (E, N) and Private Key: (D, N).

Phase 2: Encryption

This is the process of converting Plain Text into Cipher Text. This process requires two things: a key and encryption algorithm. Encryption occurs sender side and it uses the following equation to encrypt a message; C = M ^ E mod (N), where C is cipher text and M is plain text or message.

Phase 3: Decryption

This is the process of converting Cipher Text into Plain Text. This process require two things: Decryption algorithm and a key. Decryption occurs receiver side and it uses the following equation to decrypt a message; M = C ^ D mod (N). Encryption and Decryption processes are shown below in the Figure 2:

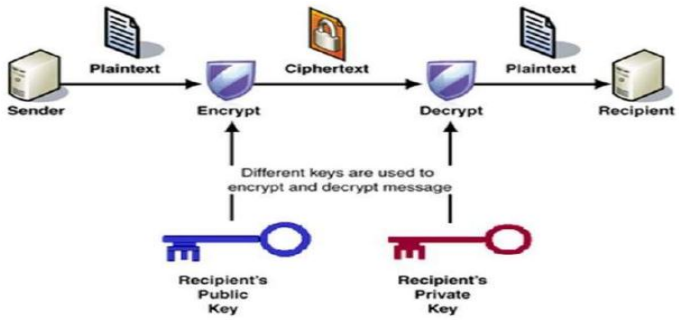

Figure 2. RSA Technique

3.2. Diffie-Hellman Algorithm

It is one of the earliest examples of key exchange implemented in the field of cryptography. The Diffie–Hellman algorithm allows both parties, which have no prior knowledge of each other, to mutually establish a shared secret key over an insecure communications channel. Diffie–Hellman key exchange is a symmetric cryptography because the shared secret key and session key are used for encryption and decryption [12], [13]. It is used by many protocols, like SSL, Secure Shell, and IPSec. Steps of this algorithm are as follows [2]:

1. Select two numbers 'p' (prime number) and 'g' (base).
2. Select two secret numbers 'x' for sender and 'y' for receiver.
3. Calculate public number R_1 = g^x mod p, And R_2 = g^y mod p.
4. Exchange their public numbers.
5. Computes First session key as K_s, K_s= R_2^x mod p.

6. Computes second session key as K_r, $K_r = R_1$^y mod p
7. Here $K_s = K_r = K$

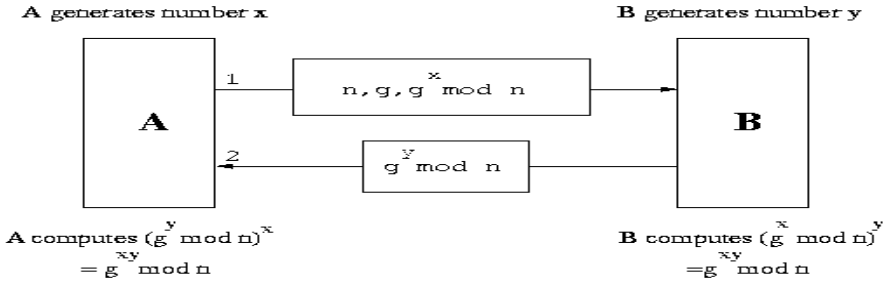

Figure 3.Diffie-Hellman algorithm

This algorithm can be explained via diagram as shown in figure 3 above. Sender A and Receiver B wants to share their secret keys over insecure channel. They are not sharing information, they just share keys.

The main disadvantage in this algorithm is that, man-in-the-middle-attack occurs in this algorithm. It occurs at the time of exchanging public numbers, i.e. R_1 and R_2. Intruder modifies the values of R_1 and R_2 and transfers it to both parties. Due to this reason, session key value comes to be unequal.

3.3. DSA Algorithm

Digital signatures are one of the best tools to implement security. A digital signature is electronic version of a written signature. It is a public-key cryptographic algorithm [14], which ensures authentication, authorization and non repudiation [15]. Digital certificate is a digital ID to show identity in the network. Encryption technology as the core of digital certificates can do encryption and decryption, and digital signature and signature verification for the information transmitted on the network to ensure confidentiality integrity and security of the information transmitted online [16].

Digital Signature is implemented by public and private key algorithms and hash functions. It is used at receiver side for message verification and sender's identity. The whole process of digital signature is shown in Figure 4. Digital signatures may also be generated for stored data and programs so that the integrity of the data and programs may be verified at any later time [17].

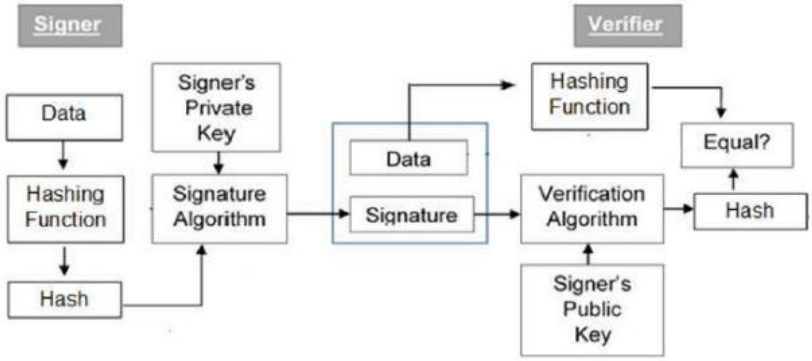

Figure 4. DSA process

Hash function follows some properties, which are given below:

1. Hash function should destroy all homomorphism structures in the underlying public key cryptosystem (be unable to compute hash value of 2 messages combined given their individual hash values) [18].
2. Hash function should be computed on the entire message [18].
3. Hash function should be a one way function so that messages are not disclosed by their signatures [18].
4. Hash function should be computationally infeasible given a message and its hash value to compute another message with the same hash value [18].

This algorithm works on ".doc, .pdf, .txt" and other types of files, and hash function can be used for dynamic size of data. The term dynamic means, results of hash function depends on size of the data [18] [19]. Applications of Digital signatures are in information security (authentication, data integrity, and non repudiation), e-commerce, banking, software distribution and in jurisdiction, and to detect forgery or tampering in data [14].

3.4. ECC Algorithm

This algorithm is mainly depend on the algebraic structure of elliptic curves [10]. ECC includes three steps in its operation, i.e., key agreement, encryption, and digital signature algorithms [20]. The first step is key distribution algorithm, which is used to share a secret key, second step is the encryption algorithm that enables confidential communication, and last is the digital signature algorithm which is used to authenticate the signer, i.e. sender and validate the integrity of the message [20]. An elliptic curve is a plane curve should satisfies the following equation [10] and the graph of the equation is shown in Figure 5.

$$y^2 = x^3 + ax + b$$

ECC is considered best for creating faster, smaller and more efficient keys [21]. ECC offers an equivalent amount of security for a far smaller key size and hence, it reduces processing and communication overhead. For example, RSA-1024 is equivalent in strength to ECC-160 [10], second example is RSA-2048 is equivalent to ECC-224 [10] and third example is RSA-3072 is equivalent to ECC-256 [10]. ECC is considered as best suitable technique for sensor networks which provides a good trade-off between key size and security [10]. It offers the maximum security with smaller bit key sizes that is why it consumes less power [21] and hence, Elliptic curve cryptography is good for battery backup also [21].
Following are the steps for ECC cryptography [21]:

1. The user must first encode any message M as a point on the elliptic curve Pm.
2. Select suitable curve & point G as in Diffie-Hellman.
3. Each user chooses private key $n_A < n$ and computes public key $P_A = n_A G$.
4. For encryption encrypt Pm, Cm={kG, Pm+kPb}, where k is a random number.
5. For decryption decrypt Cm, compute: $Pm+kPb-n_B(kG) = Pm+k(_{nBG})-n_B(kG) = Pm$

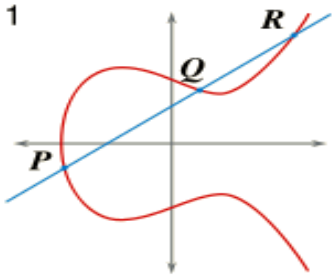

Figure 5. Elliptic Curve

3.5. Hybrid Algorithm

Hybrid means the combination of two or more things. Hybrid algorithm takes the advantages of symmetric and asymmetric algorithms. So many hybrid algorithms have been proposed. Some authors take only symmetric algorithms, some uses only asymmetric algorithms and some authors take combination of these two. Authors of [4], uses ECC and HECC techniques and inculcate with Genetics Algorithm. Authors of [2], uses RSA and Diffie-Hellman techniques to develop a hybrid algorithm. Authors of [22], uses DES and IDEA techniques for their proposed hybrid algorithm. Algorithm which is proposed by [2] is simple among all three. In this, authors uses the two times XOR operation to make the message more complex. Steps of this algorithm are as follows:

1. Encrypt the message using RSA and generate cipher text, C1.
2. Apply XOR operation between C1 and K_r. (K_r is the session key calculate by sender using Diffie-Hellman algorithm). This step produces cipher text, say C2.
3. Again apply XOR operation between C2 and K_s (K_s is the session key calculate by receiver using Diffie-Hellman algorithm). This step produces the final cipher text, C.

4. Decrypt the cipher text using RSA algorithm and obtain the original message.

3.6. DNA cryptography

DNA isa prolong polymer of compact units called nucleotides. Each DNA strand is composed of four nucleobases: A, G, C & T. The detail of any living thing is stored in DNA bases as shown in Figure 6[29].

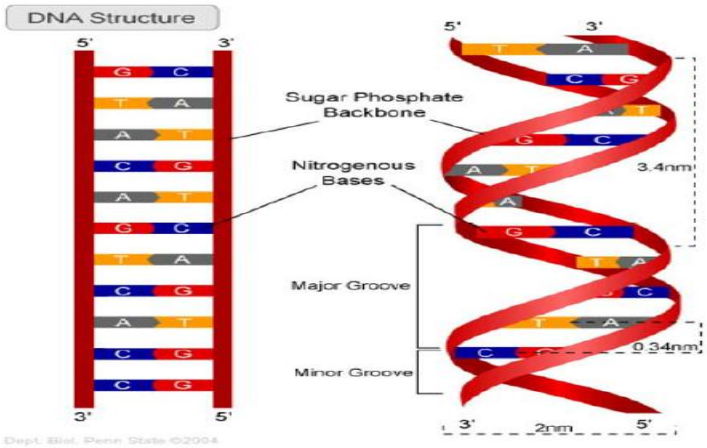

Figure 6. DNA structure

DNA cryptography uses DNA base pairs as the information carrier. Because of the processing power of DNA chips, it is more advanced technique. As we know traditional cryptographic algorithms (like DES, RSA etc.) may be break by an attacker, so there is a need of more secure cryptographic techniques. DNA computing algorithms have proposed for cryptography issues [23-25]. Several algorithms of DNA cryptography have been proposed which use secret and public keys for concealing the data [26-28]. For providing the security in WSN, the key pairs (i.e. public & private key) are used in the proposed algorithm of [29]. For the key pairgeneration, RSA algorithm is used. Their algorithm has three steps i.e. information, computation and biological [29]. In their proposed work, security is enhanced by using false data inculcated in the original data in the form of nucleotide bases [29-32].

4. COMPARISON USING VARIOUS PARAMETERS

The authors have categorized the algorithms according to their key size requirement, strength and weaknesses, possible attacks which can occur on sensor nodes by using these algorithms and then their countermeasures. Algorithms with small key sizes are breakable in the near future. So there is a need to use large key sizes in case of RSA algorithm. DH algorithm is based on dicrete logarithm problem and hences solves the challenges in these problems. ECC uses small sized keys as compared to RSA and is considered best. The all information is tabularized in Table 1.

Table 1. Comparison of various asymmetric algorithms

CRYPTOGRAPHIC ALGORITHM	KEY SIZE (in bits)	STRENGTH	WEAKNESS	POSSIBLE ATTACKS	PREFERABLE COUNTERMEASURES OF ATTACKS
RSA	• 1024 (can be breakable in near future) • 2048 • 3072 • 4096	• Less computation time.	• Small encryption exponent and small message. • Same key for encryption and signing. • Using a common modulus for different users	• Adaptive chosen cipher text attack • Side-channel analysis attacks • Power fault attack	• Optimal Asymmetric Encryption Padding
Diffie-Hellman	1024 or 3072 for p (the modulus)	• Solves challenging discrete logarithm. • Creating & sharing key, not information.	• Expensive exponential operation. • Lack of authenetication.	• Man in the middle attack	• Use authentication algorithm with D-H algorithm
DSA	Multiple of 64; between 512 & 1024 (inclusive)	• Authentication • Data Integrity • Non-repudiation	• Entropy, Secrecy, and Uniqueness of the random signature valueare critical.	• Key-recovery attack • Lattice Attacks	–
ECC	Smaller key sizes, i.e. • 160 • 224 • 256	• smaller key size • reducing storage • reduce transmission time • 15 times faster than RSA • less power consumption	• increases the size of encrypted text • Dependent on very complex equations which increases the complexity of algo	• Side-channel attacks • Backdoors • Quantum computing attacks	–
Hybrid	Based on chosen algorithms	–	• More execution time, because of two algorithms	• Adaptive chosen cipher text attacks	• Research is going on to prevent these attacks
DNA	Key size not required	• extraordinary storage capacity of DNA • low power consumption • high processing time • Dynamicity	–	–	–

5. CONCLUSION

Wireless sensor networksis a growing technology. It has applications in every field.Because of its roughly deployment in war field, it is vulnerable to many attacks. To protect it from attacks, several cryptography algorithms has developed. There are so many traditional techniques which are applied to sensors networks. But in recent years, researchers have developed so many other algorithms that are very hard to crack for any attacker. One of them is DNA cryptography, it is considered best among all others cryptographic techniques and it is still in research for study. All others techniques are surveyed in this paper and compared in terms of their key sizes, strength, weakness, possible attacks, and countermeasures of these attacks.

REFERENCES

[1] S. U. Rehman,*et al.,* "Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN)", *International Journal of Computer Science Issues*, vol. 9, Issue 1, No- 2, pp. 96-101, Jan 2012.

[2] G. R. Patel and K. Panchal, "Hybrid Encryption Algorithm", *International Journal of Engineering Development and Research (IJEDR)*, vol. 2, iss. 2, pp. 2064-2070, 2014.

[3] Xueying Zhang,*et al.*,"Energy efficiency of encryption schemes applied to wireless sensor networks", *Security and Communication Networks*, John Wiley & Sons, Ltd., 2011.

[4] R.Sharmila and V.Vijayalakshmi, "Hybrid Key Management Scheme for Wireless Sensor Networks", *International Journal of Security and Its Applications*, Vol.9, No.11, pp.125-132, 2015.

[5] S. Gajbiye, *et al.*, "A Survey Report on Elliptic Curve Cryptography", *International Journal of Electrical and Computer Engineering*, vol.1, no.2, pp.195-201, 2011.

[6] D. Malan, *et al.*, "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography", in Proc. *1st IEEE Int. Conf. Sensor Ad Hoc Communication Network*, pp. 71-80, 2004.

[7] Y. Liu,*et al.*, "PKC based broadcast authentication using signature amortization for WSNs", *IEEE Trans. Wireless Communications*, vol. 11, no. 6, pp. 2106-2115, 2012.

[8] P. Porambage, *et al.*,"Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed applications" *International Journal of Distributed Sensor Network*, vol. 2014.

[9] D. Kim and S. An, "PKC-based DoS Attacks-Resistant Scheme in Wireless Sensor Networks", *IEEE Sensors Journal*, 2016.

[10] M. Panda, "Security in Wireless Sensor Networks using Cryptographic Techniques", *American Journal of Engineering Research (AJER)*, vol.03, iss.01, pp-50-56, 2014.

[11] Al-Hamami, *et al.*,"Enhanced Method for RSA Cryptosystem Algorithm", *IEEE International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, pp. 402-408, Nov 2012.

[12] https://en.wikipedia.org/wiki/Diffie_Hellman_key_exchange.

[13] R. S.Dhakar, *et al.*,"Modified RSA Encryption Algorithm (MREA)", *Second IEEE International Conference on Advanced Computing & Communication Technologies (ACCT)*, pp. 426-429, Jan 2012.

[14] C. Dutta, *et al.*,"An Efficient Implementation of Digital Signature", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, iss. 2, pp. 452-457, Feb 2015.

[15] M. A. Nia, *et al.*,"An Introduction to Digital Signature Schemes", In Proceeding of *National Conference on Information*, Apr 2014.

[16] Z.Q. Ming, "Secure Digital Certificate Design based on the PublicKey Cryptography Algorithm", TELKOMNIKA, vol. 11, no. 12, pp. 7366-7372, Dec 2013.

[17] Vocal, "http://www.vocal.com/cryptography/dsadigitalsignaturealgorithm.

[18] William Stallings, http://williamstallings.com/Extras/Security Notes/lectures/authent.html.

[19] N. Jirwan, *et al.*,"Review and Analysis of Cryptography Techniques", *International Journal of Scientific & Engineering Research*, vol. 4, iss.3, Mar2013.

[20] F. Amin, *et al.*,"Analysis of Public-Key Cryptography for Wireless Sensor Networks Security", *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol. 2, no. 5, 2008.

[21] R. Bhanot and R. Hans, "A Review and Comparative Analysis of Various Encryption Algorithms", *International Journal of Security and Its Applications*, vol. 9, no. 4, pp. 289-306, 2015.

[22] M. Jain, "Implementation of Hybrid Cryptography Algorithm", *International Journal of Core Engineering & Management (IJCEM)*, vol.1, iss. 3, Jun 2014.

[23] T. Mandge andV. Choudhary, "A DNA Encryption Technique Based on Matrix Manipulation and Secure key Generation Scheme", *International Conference on Information Communication and Embedded Systems (ICICES)*, pp. 47-52, 2013.

[24] S. Sadeg, *et al.*, "An encryption algorithm inspired from DNA", *International Conference on Machine and Web Intelligence (ICMWI)*, pp. 344 – 349, 2010.

[25] X. Guozhen X,*et al.*, "New field of cryptography: DNA cryptography", *Chin. Sci. Bull*., 2006.

[26] Y. Zhang, *et al.*,"On the security of symmetric ciphers based on DNA coding*", Information Sciences*, pp. 254–261, 2014.

[27] G. Cui, et al., "An Encryption Scheme Using DNA Technology", *3rd International Conference on Bio-Inspired Computing: Theories and Applications (BICTA)*, pp. 37-42, 2008.

[28] S.P.N. Tripathi, *et al.*,"Securing DNA Information through Public Key Cryptography", *MIS Review*, vol. 19, iss. 1, pp. 45-59, 2013.

[29] M. and S. Upadhyaya, "Secure communication using DNA cryptography with secure socket layer (SSL) protocol in wireless sensor networks", *4th International Conference on Eco-friendly Computing and Communication Systems*, Elsevier, pp. 808 – 813, 2015.

[30] M. and S. Upadhyaya, "Improved Security using DNA Cryptography in Wireless Sensor Networks", *International Journal of Computer Applications*, vol. 155, no.13, Dec 2016.

[31] N. Saini, *et al.*,"Enhancement of security using cryptographic techniques" *4th IEEE International Conference*, pp. 1-5, 2015.

[32] X. Ren, "Security Methods for Wireless Sensor Networks", Proceedings of the *IEEE International Conference on Mechatronics and Automation*, pp. 1925-1930, 2006.

BIOGRAPHIES OF AUTHORS

Ms. Pooja is doing Ph.D from Kurukshetra University, Kurukshetra under the supervison of Dr. R.K.Chauhan. Her Research areas are MANET, WSN, security and cryptography. She has published papers in IEEE conference and in many other international journals also.

Dr. R.K.Chauhan is senior most faculty member of Department of Computer Science and Applications, Kurukshetra University, Kurukshetra. He has done excel in his field. He did MS from BITS, Pilani. He did doctorate from the Kurukshetra university.
He is the member of the Board of Directors of our university. He has attended many National and International Conferences, Seminarsand Workshops and presented many research papers in the field of Computer Science.