Comprehensive Study of Symmetric Key and Asymmetric Key Encryption Algorithms

Muneer Bani Yassein
Jordan University of Science and Technology
Irbid, Jordan
masadeh@just.edu.jo

Shadi Aljawarneh
Jordan University of Science and Technology
Irbid, Jordan
saaljawarneh@just.edu.jo

Ethar Qawasmeh,
Jordan University of Science and Technology
Irbid, Jordan
Eaqawasmeh@just.edu.jo

Wail Mardini,
Jordan University of Science and Technology
Irbid, Jordan
mardini@just.edu.jo

Yaser Khamayseh
Jordan University of Science and Technology
Irbid, Jordan
yaser@just.edu.jo

***Abstract*—Cloud computing emerged in the last years to handle systems with large-scale services sharing between vast numbers of users. It provides enormous storage for data and computing power to users over the Internet. There are many issues with the high growth of data. Data security is one of the most important issues in cloud computing. There are many algorithms and implementation for data security. These algorithms provided various encryption methods. In this work, We present a comprehensive study between Symmetric key and Asymmetric key encryption algorithms that enhanced data security in cloud computing system. We discuss AES, DES, 3DES and Blowfish for symmetric encryption algorithms, and RSA, DSA, Diffie-Hellman and Elliptic Curve, for asymmetric encryption algorithms.**

Keywords—Cloud computing, Cryptography, Encryption, Decryption, private and public key encryption, AES, DES, 3DES, Blowfish, DSA, Elliptic Curve, Diffie-Hellman and RSA.

I. INTRODUCTION

Due to the extensive use and sharing of of data in the Internet, it is necessary to protect data from hacking, noise, and interference. Cryptography attracted many researchers [4]. It is used for protecting information during transmissions between users. It alters the content of transmitted data to unreadable form, once received by the receiver, it is converted back to its original form. Encrypting data results to an unreadable format called cipher-data. Reversion this cipher data to original data called decryption process. Cryptography had a set of security goals to ensure the privacy of data. These goals are confidentiality, authentication, data Integrity, non-repudiation and access control [2].

Cryptography is widely used to secure data in cloud computing. It is classified into Symmetric (private-key) and Asymmetric (public key) keys encryption. Examples of Symmetric algorithms are DES, 3DES, AES, Blowfish and DSA (Digital Signature Algorithm), Elliptic Curve, Diffie-Hellman (key exchange) and RSA are examples of Asymmetric algorithms.

In Symmetric key, encryption uses only one key for encrypting and decrypting data between the sender and the receiver, called secret key. On the other hand, Asymmetric key encryption uses public keys for encryption and different key for decryption it is also called private key. However, public key encryption is not very efficient for small mobile devices hence it based on mathematical functions and need more computations [6]. Symmetric encryption algorithms are almost 1000 times faster than asymmetric algorithms because they require less processing power for computations [7]. There are many protocols standard used in Asymmetric algorithms such as SSH, PGP, S/MIME, and SSL/TLS and GPG, ZRTP, Internet Key Exchange and SILC [5].

978-1-5386-1949-0/17/$31.00 ©2017 IEEE

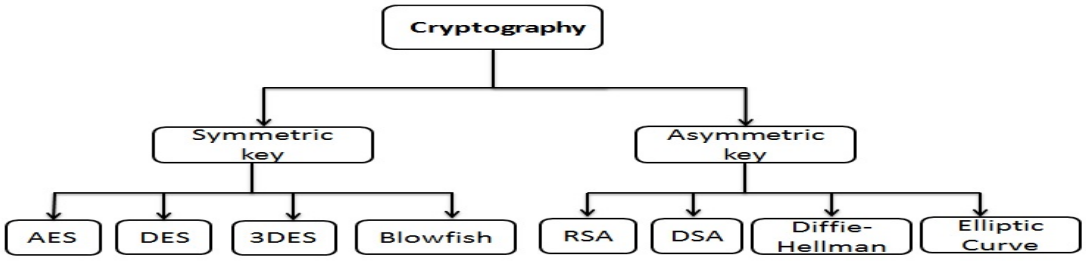

Fig 1: Classification of Encryption algorithms

II. SYMMETRIC ENCRYPTION ALGORITHMS

Encryption is a technique for protecting sensitive data. It hiddes the sensitive data of users by using the same key to cipher and decipher the data [8]. The following four algorithms uses symmetric encryption (see Fig. 1).

A. Data Encryption Standard (DES).

DES was the first encryption standards developed by National Institute of Standards and Technology (NIST). It was developed by an IBM team around 1974 and adopted as a national standard in 1997 [9]. DES provide a standard method for protecting sensitive and unclassified data [1]. DES used on the application was very popular in commercial, military, and other domains in the last decades [10] (see Fig. 2). DES uses 64 bit initially as input block,56-bit key and remaining 8 bits for odd parity check. Many attacks and methods have noticed weaknesses of DES Since that time, which made it insecure block cipher [11].

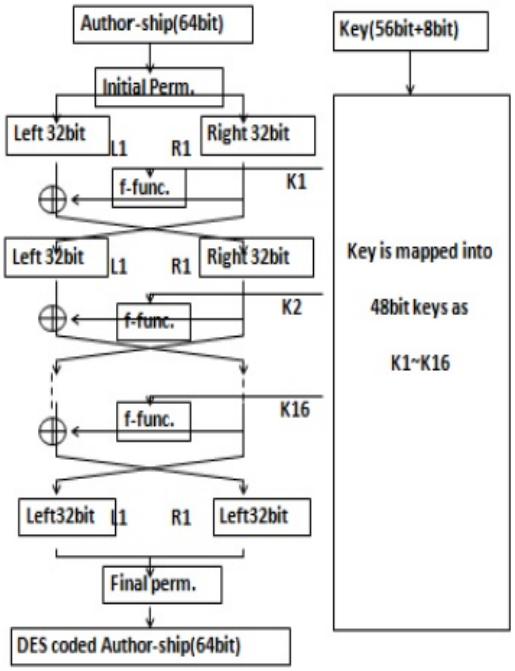

Fig. 2. DES algorithm. [10]

B. Triple Data Encryption Standard (3DES)

Brute-force attacks were more feasible with the availability of increasing computational power. The original DES cipher's key size of 56 bits had weakness of encryption, 3DES is an enhancement of DES was developed in 1998; It is 64-bit block size with increasing key size to 192 bits. this encryption method is similar to the original DES but applied 3 times, so 3DES is slower 3 times than DES, low performance in terms of power consumption and throughput but it is more secure [18]. In 3DES the plaintext is encrypted with the first key, decrypted with the second key, and third encrypted with the third key. Decryption executed in reverse as same as encryption procedure. This algorithm defines three options for the selection of keys in a bundle [12]:

- "Option 1, the preferred option, employs three mutually independent keys (K1 ≠ K2 ≠ K3 ≠ K1).It gives a keyspace of 3 x 56 = 168 bits" [12].
- "Option 2 employs two mutually independent keys and a third key that is the same as the first key (K1 ≠ K2 and K3 = K1). This gives keyspace of 2 × 56= 112 bits" [12].
- "Option 3 is a key bundle use same keys (K1 = K2 = K3).It is same DES Algorithm" [12].

C. Advanced Encryption Standard (AES)

AES is developed to be a new encryption standard recommended by NIST to replace DES. AES is a block cipher called Rijndael developed by Joan Daemen and Vincent Rijmen in 1997. It has different length of keys128, 192, or 256 bits; default 256. The encryption technique has variable rounds depending on key length, it needs 10 rounds for key length 128,12 round for key length 192 and 14 rounds for key length 256. Fig 3 shows AES encryption algorithm; the round step is performed iteratively a number of times based on length of the key. The process of decryption algorithm is as same as the sequence of encryption algorithm but with inverse each transformation step.

978-1-5386-1949-0/17/$31.00 ©2017 IEEE

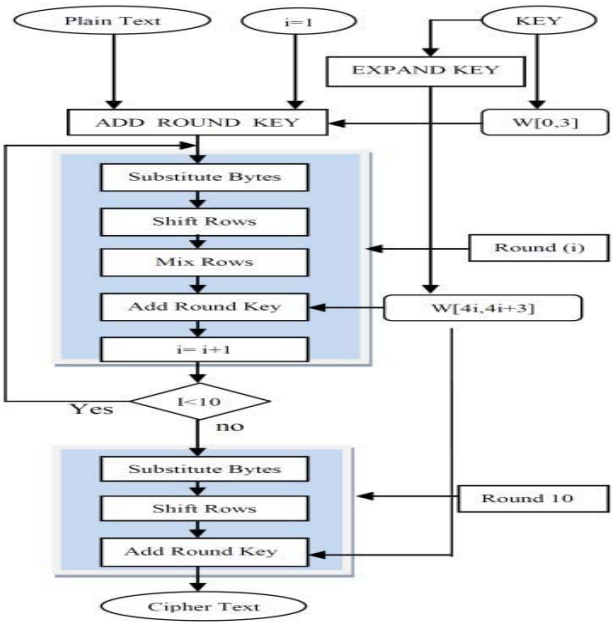

Fig. 3. AES (Advanced Encryption Standard) process [13]

D. Blowfish

Blowfish was developed by Bruce Schneier in 1993 [14]. Blowfish is a block cipher 64 bit can be taken variable length key 32 bits to 448 bits; default 128 bits. It was developed to replacement DES encryption algorithm, hence blowfish is faster encryption algorithm than another encryption algorithm that mentioned above. Blowfish is license-free and is available free for all uses [15]. Data encryption in blowfish algorithm performed commonly via a 16-round. Each round consists two parts: key dependent Permutation, and a key- and data-dependent substitution; all operations are XORs and additions on 32-bit words, the only additional operations are four indexed array data using S-boxes lookup per round [10].

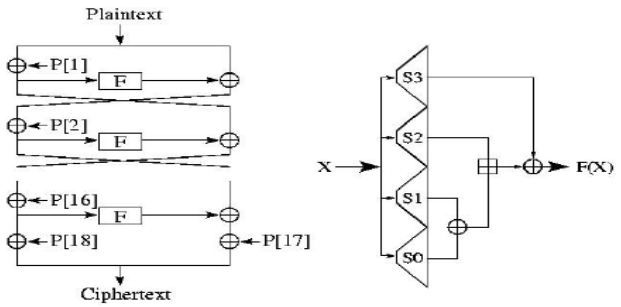

Fig. 4. Blowfish algorithm [10]

III. ASYMMETRIC ENCRYPTION ALGORITHMS

A. Rivest-Shamir-Adleman (RSA)

RSA algorithm using public key and private key. It was developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. It is a block cipher for digital signatures algorithms or key exchange algorithms. RSA uses variable length key and variable length block of encryption. A message is encrypted by cloud service provider (sender) and it's decrypted by cloud service consumer(receiver). Hence message is encrypted with a public key, it is decrypted with an appropriate private key that is owned by the receiver. RSA algorithm consists of three steps: Key Generation, encryption, and decryption. Fig 5 shows the process of RSA encryption algorithm. The main weakness in RSA is attacked by possible: Brute-Force Attacks, Mathematical attacks, Timing attacks and Chosen Ciphertext attacks [4].

B. Diffie-hellmann algorithm

The Diffie-hellman algorithm was the first public key algorithm constructed by Witfield Diffie and Martin Hellman in 1976 [16]. It is back to a Diffie-hellman problem related to discrete algorithm problem. Diffie-hellman is used for key exchange algorithm. It is constructed under insecure connection channel. Diffie-hellman consists of two keys:

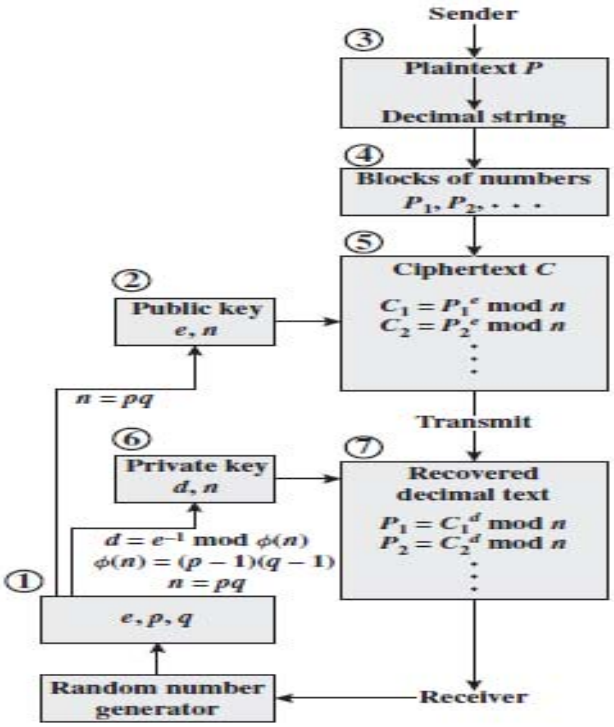

Fig. 5. RSA algorithm process [4].

a private key and secret key. Suppose sender wants to set up a connection with the receiver he encrypts the message

with his own private key and sender's public key. Once receiver gets the message he decrypts the message with his own private key and sender's public key [4].

C. Digital Signature Algorithm (DSA)

DSA was developed by the U.S. National Institute of Standards and Technology (NIST) in 1991 for used in their Digital Signature Standard(DSS) [11]. It based on the difficulty computing discrete algorithm problem [4]. DSA used for authentication and verifying the integrity of digital signatures. DSA performed to be able to generate and verify signatures using Secure Hash Algorithm (SHA). If the sender wants to send a message to the receiver the signature generation in sender uses its own private key to generate a digital signature, once the receiver gets the message the signature verification uses sender's public key [17]. DSA compatible with signing and verifying functions.

D. Elliptic Curve Cryptography (ECC)

ECC was developed by Koblitz and Miller in 1985 based on elliptic curve theory. Security of ECC due to use Discrete Logarithm Problem[19]. It uses complicated algebraic and geometric equations to generate public key[4]. It is a public key cryptography. ECC uses private key for decryption and generation signatures while it uses the public key for encryption and verification signatures.

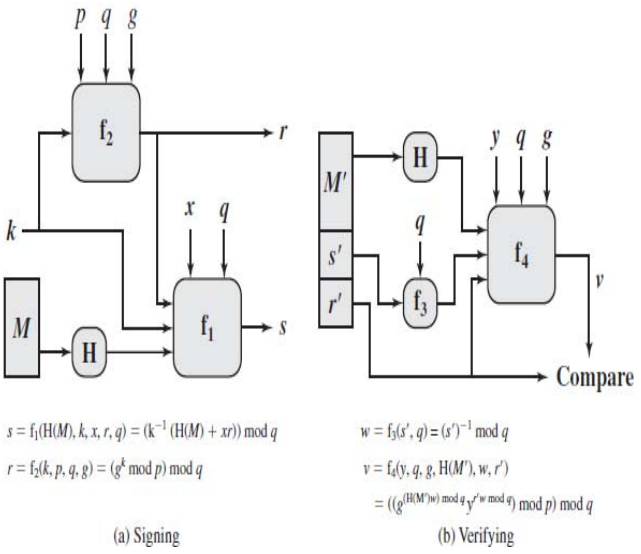

Fig. 6. Signing and verifying functions in DSA algorithm [4]

ECC can use as an enhancement for another encryption algorithm such as ECC- Diffie-Hellman and ECC-DSA [19]. ECC is designed to improve performance to reduce computing power and battery resource consuming [25]. This gives us chance for using ECC in mobile device application, hence it provided faster, efficient and secure model for secured application in the cloud [25].

IV. ANALYSIS AND COMPARISON OF SYMMETRIC AND ASYMMETRIC ALGORITHMS

Nadeem et al 2005 [20], made performance evaluation for symmetric algorithms DES, 3DES, AES and Blowfish that implemented in java and using two different hardware platforms. Algorithms were compared block cipher with different block size and different key size. They conclude when the block size is larger, speed time was faster; because large block size needs less execution time to encrypt data while small block size needs more execution for the same block cipher. They also conclude Blowfish is the fastest symmetric algorithm and 3DES is the slowest algorithm.

Elminaam et al 2010 [3], studied set of settings to evaluate six encryption algorithms (AES, DES, 3DES, RC2,Blowfish, and RC6),they used different factors for each algorithm to make comparison more accurate such as different sizes of data blocks, different data types ,battery power consumption, different key size and finally encryption/decryption speed[3]. They concluded that the blowfish is the fastest algorithm then RC6 followed it based on processing time when changing packet size. On other hand 3DES is the slowest algorithm hence it had the lower performance of power consumption and throughput than DES algorithm. When they used small key size they conclude RC2 had the lowest performance and lowest throughput compared with other algorithms. Also, they concluded that Blowfish had better performance of power consumption and throughput. AES is the best performance compared with RC2, DES and 3DES. Finally, when changing the key size the larger key size due to the utilization of battery consumption and time processing.

Verma et al 2011 [21], proposed performance evaluation for four encryption algorithms (DES, 3DES, Blowfish and AES). They used different settings to evaluate encryption algorithms such as different sizes of data blocks and decryption speed under different hardware and software platform. All codes implemented in C++, .NET(2003) and run on a Pentium- 4, 2.1 GHz processor under Windows XP SP1. They showed that Blowfish was the best algorithm in case processing time and it had strong key size(448 bit). AES needed more processing time when data block size was relatively large. 3DES required more time than DES. Also, they showed that AES was the best algorithm in cases number of request executed per second in different user loads, and in the response time in different user load situation performance results of stream cipher [21].

978-1-5386-1949-0/17/$31.00 ©2017 IEEE

Kumar et al 2016 [22], made a comparison of the performance of algorithms (DES, AES, and Blowfish). They concluded that Blowfish gives the best results in various block cipher modes with minimum weak points. AES showed poor performance compared with other algorithms. In general, symmetric encryption algorithms are faster than asymmetric encryption algorithm but it had only one weak point that it is shared its key with other parties involved in the process. Asymmetric encryption has a strength point that it is used two different keys but it's required more processing time than symmetric encryption.

Arora et al 2013 [23], proposed implementation of the algorithm using java to make cloud data secure by using different settings to make a comparison between algorithms(AES, DES, Blowfish, and RSA). They showed that AES used the least time of execution cloud data. Blowfish consumed least memory requirement. DES consumed the least time in encryption. RSA consumed the longest time in encryption and largest memory size.

Boni et al 2015 [24], proposed a new technique to improve the Diffie-Hellman algorithm, hence it requires complex computations that increasing time complexity when public keys are generated named "Multiplicative Key Exchange Algorithm". It used simple arithmetic equation when generated and exchanged keys over an insecure network. They showed that Multiplicative Key Exchange time complexity is ten times faster than a Diffie-Hellman algorithm, hence it needs fewer computations compared with the Diffie-Hellman algorithm. This technique used on the area which cares of the speed of generation keys rather than security where devices are not complex or have lower end configurations.

We make a comparison between all algorithms on Table 1 based on main characteristics and summarization of all performance evaluation of researchers that are considered above for symmetric and asymmetric encryption algorithms.

V. CONCLUSION

In this survey, we give a detailed study of symmetric like AES, DES, 3DES and Blowfish also for asymmetric algorithms such as RSA, DSA, Diffie-Hellman and Elliptic Curve. According to analysis section, we found that the efficiency of the various algorithm affected by the difference parameter. In the current state of increasing demand on cloud application, it became necessary to provide efficiency, robust and high-security algorithms that suitable with the large scale of data in the cloud. Speed and security are the most important rules play on cloud applications.

REFERENCES

[1] Mahajan, Prerna, and Abhishek Sachdeva. "A Study of Encryption Algorithms AES, DES and RSA for security." Global Journal of Computer Science and Technology (2013).

[2] Surya, E., and C. Diviya. "A Survey on Symmetric Key Encryption Algorithms." International Journal of Computer Science & Communication Networks 2.4 (2012): 475-477.

[3] Elminaam, Diaa Salama Abd, Hatem Mohamed Abdual-Kader, and Mohiy Mohamed Hadhoud. "Evaluating the performance of symmetric encryption algorithms." IJ Network Security 10.3 (2010): 216-222.

[4] Stallings, William, and Mohit P. Tahiliani. Cryptography and network security: principles and practice. Vol. 6. London: Pearson, 2014.

[5] Panda, S. N. "A PROPORTIONAL ANALYSIS ON CRYPTOGRAPHY TECHNIQUES, FUNCTIONS AND RELATIVE PERFORMANCE ISSUES." Journal of Global Research in Computer Science 2.6 (2011): 130-136.

[6] Ruangchaijatupon, N., and P. Krishnamurthy. "Encryption and Power Consumption in Wireless LANs-N,''." The Third IEEE workshop on wireless LANS. 2001.

[7] Hardjono, Thomas, and Lakshminath R. Dondeti. Security in Wireless LANS and MANS (Artech House Computer Security). Artech House, Inc., 2005.

[8] Padmapriya, A., and P. Subhasri. "Cloud computing: security challenges and encryption practices." International Journal of Advanced Research in Computer Science and Software Engineering 3.3 (2013).

[9] Standard, Data Encryption. "Federal information processing standards publication 46." National Bureau of Standards, US Department of Commerce (1977).

[10] Nie, Tingyuan, and Teng Zhang. "A study of DES and Blowfish encryption algorithm." Tencon 2009-2009 IEEE Region 10 Conference. IEEE, 2009.

[11] Kaur, Randeep, and Supriya Kinger. "Analysis of security algorithms in cloud computing." International Journal of Application or Innovation in Engineering and Management 3.3 (2014): 171-6.

[12] "3DES", http://www.cryptosys.net/3des.html. Last access: 1/2/2017.

[13] Mandal, Akash Kumar, Chandra Parakash, and Archana Tiwari. "Performance evaluation of cryptographic algorithms: DES and AES." Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on. IEEE, 2012.

[14] Nie, Tingyuan, and Teng Zhang. "A study of DES and Blowfish encryption algorithm." Tencon 2009-2009 IEEE Region 10 Conference. IEEE, 2009.

[15] Thakur, Jawahar, and Nagesh Kumar. "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis." International journal of emerging technology and advanced engineering 1.2 (2011): 6-12.

[16] Diffie, Whitfield, and Martin Hellman. "New directions in cryptography." IEEE transactions on Information Theory 22.6 (1976): 644-654.

[17] Gallagher, Patrick. "Digital signature standard (DSS)." Federal Information Processing Standards Publications, volume FIPS (2013): 186-3.

[18] Minaam, Diaa Salama Abdul, Hatem Mohamed Abdual-Kader, and Mohiy Mohamed Hadhoud. "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types." IJ Network Security 11.2 (2010): 78-87.

[19] Tirthani, Neha, and R. Ganesan. "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography." IACR Cryptology ePrint Archive 2014 (2014): 49.

[20] Nadeem, Aamer, and M. Younus Javed. "A performance comparison of data encryption algorithms." Information and communication technologies, 2005. ICICT 2005. First international conference on. IEEE, 2005.

978-1-5386-1949-0/17/$31.00 ©2017 IEEE

[21] Verma, Om Prakash, et al. "Peformance analysis of data encryption algorithms." Electronics Computer Technology (ICECT), 2011 3rd International Conference on. Vol. 5. IEEE, 2011.

[22] Kumar, Praveen, et al. "A performance based comparison of various symmetric cryptographic algorithms in run-time scenario." System Modeling & Advancement in Research Trends (SMART), International Conference. IEEE, 2016.

[23] Arora, Rachna, Anshu Parashar, and Cloud Computing Is Transforming. "Secure user data in cloud computing using encryption algorithms." International journal of engineering research and applications 3.4 (2013): 1922-1926.

[24] Boni, Sharad, Jaimik Bhatt, and Santosh Bhat. "Improving the Diffie-Hellman Key Exchange Algorithm by Proposing the Multiplicative Key Exchange Algorithm." International Journal of Computer Applications 130.15 (2015).

[25] Alowolodu, O. D., et al. "Elliptic curve cryptography for securing cloud computing applications." International Journal of Computer Applications 66.23 (2013).

978-1-5386-1949-0/17/$31.00 ©2017 IEEE

TABLE I. COMPARISON OF SYMMETRIC AND SYMMETRIC ENCRYPTION ALGORITHMS

Factors	AES	DES	3DES	BLOWFISH	RSA	Diffie-Hellman	ECC
Developed by	Joan Daemen and Vincent Rijmen in 1997	IBM in 1975	IBM in 1978	Bruce Schneier in 1993	Ron Rivest, Adi Shamir, and Leonard Adleman in 1977	Witfield Diffie and Martin Hellman in 1976	Koblitz and Miller in 1985
Key length	128,192, 256	56 bits	K1,k2,k3 168 bits	32-448 bits(128 by default)	1024 bits	2013,224 bits for q and 2048 bits for p	112 bit to 512 bit
Cipher type	Symmetric	Symmetric	Symmetric	Symmetric	Asymmetric	Asymmetric	Asymmetric
Scalability	Not scalable	It is scalable algorithm Due to varying the key Size and block size.	168,112 or 56	Scalable	Not scalable	Scalable	Scalable
Security	Secure for both provider and user.	Security applied to both providers and user	Security applied to both providers and user	Secure for both providers and user/client side	Secure for user only	Vulnerable and secure against eavesdropping	Based on difficulty Of generating key
Attack	Brute force	Brute force	Theoretically possible	Not yet	Brute forced and oracle attack	Denial of service attack	Timing or simple and power attack

978-1-5386-1949-0/17/$31.00 ©2017 IEEE