Survey on Modern Cryptography

Mustafa M. Abd Zaid *Soukaena Hassan*

mustafamajeed2014@gmail.com *soukaena.hassan@yahoo.com*

Computer Sciences Department/ University of Technology, Baghdad, Iraq

DOI :http://dx.doi.org/10.31642/JoKMC/2018/070101

Received Sep. 1, 2019. Accepted for publication Mar. 11, 2020

Abstract. *Security is one of the significant difficulties that individuals are confronting when the information exchanged over the internet in today's world. Cryptography is the way to achieve security of network or data by hiding the important information from unauthorized individuals. Encryption is a mechanism of converting plain-text into cipher-text in order to be unreadable by unwanted people. In this review, we explain some important cryptography primitives (symmetric and asymmetric cryptography algorithms) with examples for each type. Comparative study is making among this cryptography primitives according to many parameters such as structure, speed, block size and others parameters.*

Keywords: Cryptography, encryption, decryption, AES, RC4, RSA.

I.Introduction

Cryptography implies "secret writing," which also represents their main objective as classified by this Greek term. Cryptography is a well-known field with a great impact over 2,000 years. The word "cryptography," known as the cryptography or cipher systems, has been connected with the issue of developing and evaluating encryption systems [1],[2].

Cryptography is the science of security-based algorithms and safeguards information integrity, information source authenticity algorithms, and information confidentiality algorithms (encryption algorithms). The core of cryptography is secrecy. Encryption is a convenient way of privacy of information[3].

Cryptographic algorithms are classified in various respects. For the basis of the current review, the keys used for encryption and decryption will be classified according to the amount and the specific application. The category of main encryption algorithms is illustrated in figure 1.

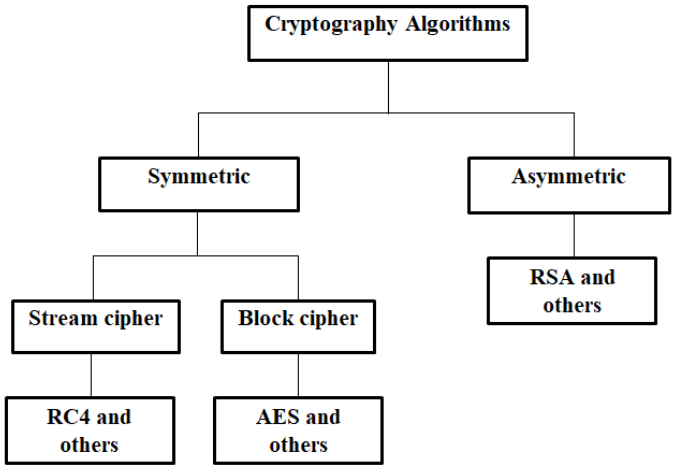

Fig1: Cryptography Algorithms

The secret key can be classified under the asymmetric cryptography into a public key (own for everyone) and a private key (own for only allowed people) [4].

Asymmetric encryption has two main usage instances: authentication and privacy. Messages may be signed with an asymmetric cryptographic key, and then everyone with the public key can check that a person has the respective personal key produced the signal. It can be coupled with an identification system evidence, to determine what entity (individual or group) really possesses, authenticating it [1].

Asymmetric encryption operates a little different from symmetrical encryption. The sender with the public key encrypt a message, and only the receiver with the private key decrypt it.

Symmetrical encryption allows the content of material to be encrypted or hidden where the recipient and sender both use the same secret key. Note that, for most applications symmetrical encryption is not enough, as it does not provide authenticity but only privacy. This means that an attacker cannot see the message but an assailant can create fake messages to force the applicant to be decoded [4],[5].

II.Security Services of Cryptography

The goal of modern cryptography is to ensure the preservation of information properties through mathematically sound means. There are many attributes of information that can be assured in this way[6], the following are the four major ones:

- Confidentiality: Ensures that the transmitting information are accessible only for reading by authorized parties.
- Data Integrity: It is a security service which is responsible for pinpointing any changes to the information. The information may be altered deliberately or accidentally by an unlawful entity. Integrity service demonstrates whether or not the information has been intact since an approved user last produced, transferred or stored those data. Data integrity does not protect the data from getting modified but provides the ability to uncover data that got altered in an unauthentic process.
- Authentication: Ensures that the original message is correctly identified, with an assurance that the identity is not false.
- Non-Repudiation: To make sure that only the intended endpoints have sent the message and later cannot deny it.

III.Symmetric Cryptography (Secret Key)

This type of algorithms uses the same key for encryption and decryption process. The sender has a specific key to encrypt the plain-text and the receiver relates the same key to decrypt the message and convalesce (recover) the plain-text. This key must save secretly.

A symmetric key encryption scheme ensures confidentiality when two sides communicate, sending and receiving. They meet on a specific key to establish a safe communication. Encrypted of a plain-text is performed by the sender to compute ciphertext that is sent to the receiver [5],[7],[1].

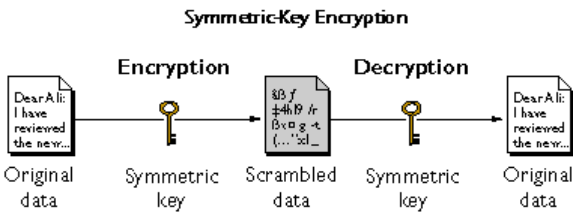

Fig2: A symmetric-key encryption scheme

By using the symmetric key encryption, each pair of the users who need to exchange the data must have two instances of the identical key. If 10 people expect the symmetrical keys to be used to interact safely, 45 keys should be kept informed. Then, there will be 4,950 keys if 100 persons are to interact. In order to verify the number of the symmetric keys required, the mathematical statement is n (n–1)/2. The safeguard key is the basis for the symmetrical encryption technique [8],[9].

Stream and block ciphers can be classified as the main parts of the symmetric algorithms. Stream ciphers encode one bit of plain-text at a moment; however, block ciphers encrypt amount of bits in one piece (such as 64 bit ciphers of nowadays). The symmetrical encoding algorithms Blowfish, AES, DES, RC5, and RC6 are popular examples [9].

A. Block Cipher

A block cipher name is given when each block has the same key to encrypt a block of information each time. In particular, if the same code key is used in a block cipher, the same plaint-text block will always encrypt the same chipper-text in a distinct stream cipher.

If the chip is calculated by the iterative application of a round function to the plain-text several times, a block cippher is called an iterated cipher. A round key is paired with the entered document in each round [1].

- **Advanced Encryption Standard (AES-128):**

In 2001, NIST (National Institute of Standards and Technology) determined (Advanced Encryption Standard (AES)), which is known by its unique name for the encryption of electronic information. Even the US government in the 1990s realized that Data Encryption Standard (DES) had survived its usefulness. The main problem with the DES is the 56 bit key length can be extensively searched for, and distributed assaults on the Internet using the pcs which can be carried out using the DES keys. In 1997, NIST began to look for the DES alternative NIST which is determined AES algorithm to replace DES. The AES must be a block cipher that fits for taking care of 128 bit blocks, utilizing the keys estimated at 128, 192, and 256 bits. For the symmetric block cipher AES can encode (encrypt) and decode (decrypt) data. The information is changed to an incomprehensible form called ciphertext by "the Encryption" Changing the information again into its original form is called plain-text by "the Decryption" [10],[11]. The number of rounds in the AES depends on the key length, therefore it is variable comparing to the DES. Here, for the 128 bit keys, AES utilizes 10 rounds, for the 192 bit keys, the AES utilizes 12 rounds, and for the 256 bit keys, the AES utilizes 14 rounds. An alternate 128 bit round key is used by every one of these rounds. The 128 bit key's round is figured from the standard key of the AES[12].

Four fundamental operation blocks separate AES where information is dealt with at either byte or bit level. "State" is used to store out the variety of bytes as a 4*4 array. The following four steps are the essential steps in the AES algorithm:

STEP 1: SubBytes & InvSubBytes Transformation: a non-linear substitution byte, using a substation table (S-Box). For byte-by-byte substitution amid the forward procedure, this step is known as SubBytes. InvSubBytes is the comparing substitution step utilized in the decryption step [1].

This process is used by substituting byte for a given byte in the input-state, utilizing a 16 × 16 query table. S-box is the AES-based byte matrix, Table1

- The sections in the query table are made by utilizing the thoughts of multiplicative inverses in GF(2^8) and bit mix to annihilate the bit-level relationships inside each byte. Figure 3 shows the substation byte operation

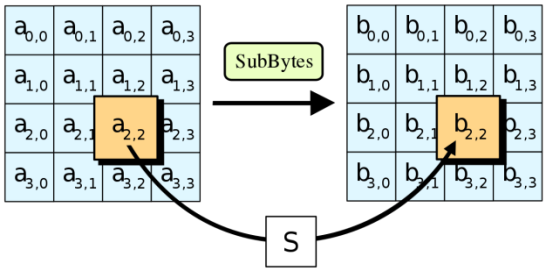

Fig3: The SubBytes operation

Table1: The S-box of the AES [1].

X \ Y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7c	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

The inversion byte replacement process uses the same byte substitution method for decoding purposes. The inverse S-box is indicated in Table (2).

Table2:The inverse S-box of the AES [1].

X \ Y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

STEP 2: The ShiftRow & InvShiftRow Transformation:

- To scramble the byte, arrangement inside each 128 bit block is the objective of this change
- (moving the rows of the state array amid the forward procedure). InvShiftRow (The relating change amid backward process). The ShiftRows transformation is a two-featured system that makes the algorithm linear. A simple byte transposition with episodically shifted bytes in the last three state rows episodically changed; the left shift offset is one to three bytes [1],[12].
- The Inverse ShiftRows transformation must switch encrypted message from the state matrix rows in the reverse direction using the data to perform the decryption phase. ShiftRow Transformation is shown in Figure 4.

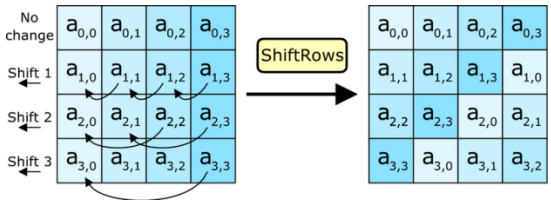

Fig4: The ShiftRow transformation.

STEP 3: (Mixcolumns & inverse MixColumns) Transformation: MixColumns for stirring up of the bytes in every column independently in the encryption step. InvMixColumns is the corresponding transformation during decryption step[12].

- The objective is to additionally mix up the 128 bit input block. The bits of the cipher-text are relied on the bits of the plain-text after 10 rounds of preparing by the ShifRows process along with the MixColumn process[1]. See Figure 5.

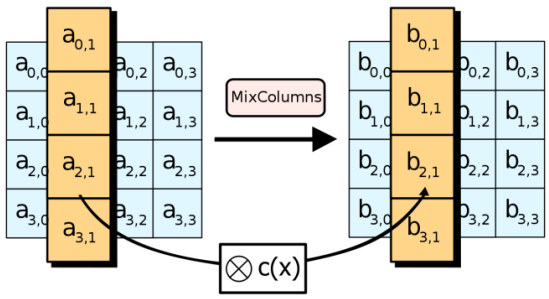

Fig5: The MixColumns operation

A linear conversion that blends each column of the state matrix is the phase of the MixColumn. The main diffusion component in the AES is the MixColumn operation. Each column of four bytes is regarded as a vector and multiplied by a specified matrix of four bytes. There are steady entries in the matrix. The inverse transformation of MixColumns utilizes the same conversion method for the decryption technique depending on the inverse matrix. Multiplication and addition of coefficients are carried out using the GF(2^8)[1],[13].

STEP 4: Add-round-key Transformation:

Key scheduling or round key expansion is a method used for producing round keys. This is an uncomplicated, straightforward XOR operation between the round-key and the working state [13].

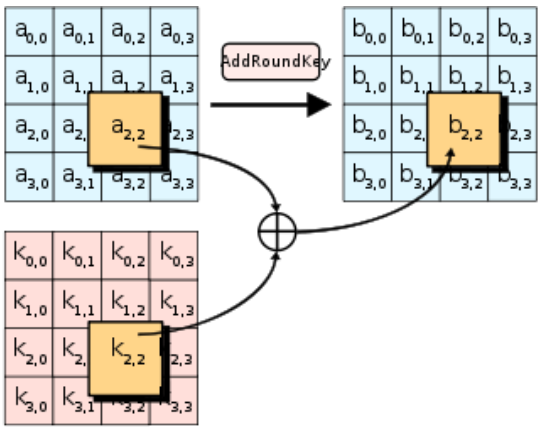

Fig6: The AddRoundKey operation

The figure of the standard AES system is shown below in Figure 7.

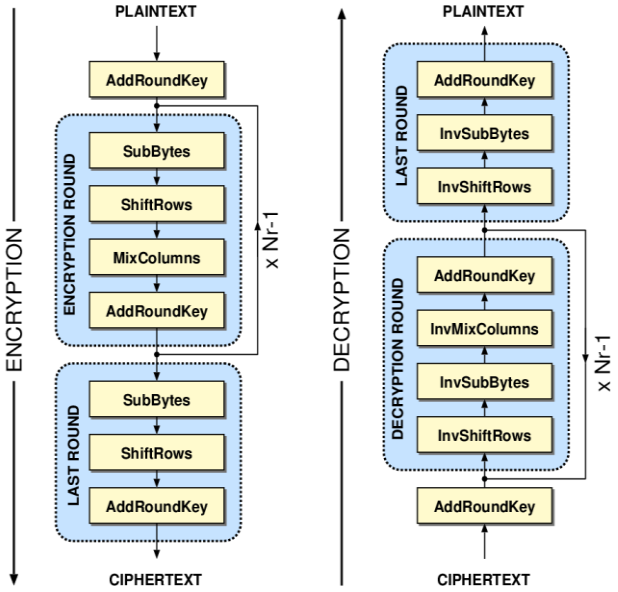

Fig7: The flowchart diagram for AES algorithm[12].

The method of decryption is in the same series as in the encryption phase. The transformations; the InvSubBytes, the InvShiftRow, the Mixcolumns, and the Add-round-key consent to the form of the key schedules to be equal for encryption and decryption.

B. Stream Cipher

A stream cipher is a cryptographic algorithm that encryptes a plain-text by one bit or byte at a moment. It utilizes an unlimited pseudorandom flux of bits as the key. This mode splits Plain text P into sequent bits P1, P2,…, and XORing each P with K of a key stream K= K1,K2,K3……etc. A large bits sequence is produced in stream ciphers from a brief sequence of key bits, and the ciphertext is bitwise added with the modulo 2 to the plain-text [14],[1]. Stream ciphers usually have lower complicated and faster hardware circuits than those from block ciphers [14]. It is also better, and in some instances obligatory (e.g. in certain apps for telecommunications), if the buffering is restricted, or if characters have to be separately processed on receipt. Because they have restricted or no propagation of mistakes, stream ciphers may also be beneficial in circumstances where there have been highly likely transmission errors[15].

The one-time Pad which should have a pure random key could ultimately accomplish "perfect secrecy." This type is engineered to increase an ideally-designed cipher, called the one-time path. In other words, it must be completely resistance to cyber-attacks [16].

One of the known stream cipher algorithm is the Rivest Cipher 4 (RC4) especially Vigenere cipher and Vernem cipher. RC4 algorithm uses the classical operation (XOR) [12].

- **RC4 Stream Cipher Algorithm**

RC4 is the most satisfactory stream cipher, Ron Rivest outlined the RC4 algorithm in 1987 but the algorithm was kept as a mystery until the point that it was as often as possible to the cypherpunks mailing list in 1994[15],[16].

The abbreviation of the "Rivest Cipher 4" or “Ron’s Code 4” is RC4 which uses random permutation. It is utilized as a part of numerous web conventions, for example, Wireless Protected Access (WPA), Wired Equivalent Privacy (WEP), and Secure Socket Layer/ Transport Layer Security (SSL/ TLS) [16].

The RC4 proves its efficiency in both hardware and software and speed. It is extremely straightforward and quick equivalent to other encryption algorithms. This algorithm is a simple, fast, easy to explain and efficient, that is why it became so popular [17].

The RC4 is a key-size variable stream cipher relying on the inner secret state of 256-byte and two one-byte metrics. The information is encoded with the key stream that RC4 creates from the main using XORing information [9].

The RC4 algorithm predominantly comprises of two phases: the KSA (Key Scheduling Algorithm) to produce, from the key, an initial permutation of the S array and the PRGA (Pseudo Random Generation Algorithm) to create the key stream[17].

- **Description of the RC4**

RC4 picks a cluster (S_{box}) and a secret key (K). The cluster known as S-box which includes N (N=2^n) (N=256, where n=8). The KSA and the PRGA are two algorithms contained in the RC4 algorithm [18].

A variable key length is used in the RC4, which runs between (0-255) bytes for instating 256-byte array in the underlying state by components from S_{box} [0] to S_{box} [255] [19]. The KSA uses the symmetric key to permute an array S containing 256 entries. The S array is initialized with identity permutation ranging from 0 to 255, as suggested in [17],[12], RC4 must utilize a key longer than 128 bytes. Then, a 256-iteration loop is utilized to produce a random permutation of the exhibit S, where the entries of the S array are continually swapped using the key value[17]. The KSA steps are shown in Figure 8.

Algorithm of the KSA:

set N ← 256
set ki to 0
while (true)
begin
S_{box} [ki] ← ki
ki←ki+1
end while
set kj←0
set ki←0
while (true)
begin
kj←(kj+S_{box} [ki]+k[ki]) Mod N;
swap(S_{box}[ki],S_{box}[kj])
ki←ki+1
end while

Fig8: The KSA of the RC4

The objective of the PRGA is to create a sequence of key stream. In the PRGA, two indices; ki and kj, are initialized to zero. In each iteration, ki is recomputed as (ki+1) and kj is recomputed as (kj+S_{box} [ki])mod 256 , and then a swap operation is conducted between S[ki],S[kj]. The key stream is (XOR) with clear-text. The key stream is generated as (S_{box} [(S_{box} [ki]+ S_{box} [kj]) mod 256) [12],[17],[20]. The PRGA steps are shown in Figure 9.

Algorithm of PRGA:

set N←256
set ki←0
set kj← 0
while (generate key-stream)
begin
ki←ki+ mod N;
kj←kj+S_{box} [ki]mod N
swap(S_{box} [ki], S_{box} [kj])
Output←S_{box} [(S_{box} [ki]+ S_{box} [kj]) mod N]
end while

Fig9: The PRGA of RC4

IV. An asymmetric Cryptosystem (Public Key):

The public or two-key Cryptosystem was launched by Diffie and Hellman in 1976. **Cryptosystem** of the traditional secret key bases employs shared-type of a single key by both communicational sides. Disclosing this key leads to compromising of information [1]. The connected sender and receiver don't publicly uncover their secret keys; however, the public one could be identified by different users [21],[7]. The most commonly used cryptography algorithms are Diffie-Hellman, RSA, ECC, ElGamal, and DSA.

The main drawbacks that are accompanied with asymmetric key cryptosystem are the needed for the sophisticated key management techniques and the high computational cost of the most algorithms, which makes them less suitable to lightweight applications [22].

A. The RSA Cryptosystem

The RSA cryptosystem was invented in August-1977. It is known and widely regarded as the most practical public-key scheme. The RSA invented by Rivest, Shamir and Adleman. This system is considered as a public-key scheme that can be utilized for message encryption, key exchanging, and digital signature production [23].

The RSA security depends on the difficulty of factoring huge numbers. In the RSA, a private key is kept secret; however, the public key is known to everybody in the system.. The steps of the RSA are shown below:

- **The RSA Key Generation**
  - Select prime numbers p_n and q_n.
  - Find $N = p_n$ x q_n.
  - Find φ(N) = (p_n -1) × (q_n-1).
  - Select e_x, like that gcd (e_x, φ (*N*)) = 1; 1 < e_x< φ (*N*).
  - Find *d*, $e_x \times d \equiv 1 \bmod \varphi(N)$.
  - The public key =(e_x, *N*) and private key=(*d*, *N*).
- **The RSA Encryption**
  - Select a message "M" to encrypt.
  - Compute the cipher-text C = M^{e_x} Mod *N*.
  - Send "C" to the receiver.
- **The RSA Decryption**
  - The reception should do the following to find original message "M":
  - M= C^d mod N.

V.Comparison between the Symmetric and Asymmetric Algorithms

This section discusses the comparison between the AES, RC4 which are symmetric algorithms and RSA that is an example of asymmetric algorithms, as shown in table(3)

Table3: Comparison between the AES, RC4, and RSA

Parameters	Symmetric		Asymmetric
	AES	RC4	RSA
Published	2001	1987	1977
Author	Vincent Rijmen, Joan Daeman[13]	Ron Rivest [16]	Rivest Shamir Adleman[23]
Block Size	128 bits [12]	40-2048 [19]	1+floor((x-1)/8) x= key size [22]
Key Size	128/192/256 [10]	Variable [20]	1024 to 4096 [23]
Rounds	10/12/14 [1]	256 [18]	1 [23]
Structure	Substitution Permutation [11]	Festiel Stream[9]	Public Key Algorithm [23]
Security	Excellent[13]	Adequate[16]	Good[23]
Speed	Fast[13]	Fast[22]	Slow[22]

VI.Conclusion

This paper introduces a review of some cryptographic algorithms according to the type of each of them. The survey gives good understanding for studying these algorithms. The paper also shows that the symmetric cipher is faster than asymmetric as the comparison between them. We can see that the AES is the most reliable according to security, speed of encryption, key size, and structure. The RC4 is useful for real-time encryption according to the comparison parameters.

Reference:

[1] Ali, Y., "Improve E-Services Security Level by Modifying AES Algorithm", Master's Thesis, Department of Computer Science, University of Technology, (2016).

[2] Piper, F. & Murphy, C. , "Cryptography: A Very Short Introduction", © Oxford University Press, Oxford, UK, (2006).

[3] Dent, A. & Mitchell, C., "User's Guide to Cryptography and Standards", Artech House, INC. USA, (2005).

[4] Kessler, G., "An Overview of Cryptography", [online]: http://www.garykessler.net/library/crypto.html, (2013).

[5] Stamp, M. & Low, R. , "Applied Cryptanalysis Breaking Ciphers in the Real World", © John Wiley & Sons, Inc., New Jersey, USA, (2007).

[6] Pavithra, S., & Ramadevi, E., "Study and Performance Analysis of Cryptography Algorithms", International Journal of Advanced Research in Computer Engineering & Technology, 1(5), 82-86. (2012).

[7] Delfs, H. & Knebl, H. , "Introduction to Cryptography Principles and Applications Second Edition", © Springer-Verlag Berlin Heidelberg, (2007).

[8] Barker, E., & Roginsky, A., "Transitions: Recommendation for Transitioning the Use of 595 Cryptographic Algorithms and Key Lengths", National Institute of Standards and Technology, Gaithersburg, Maryland, (2015).

[9] Hussein, Z., "Design and Implementation of Enhancement RC4 Stream Cipher System", Master's Thesis, Department of Computer Science, University of Technology, (2015).

[10] Kawle, P., Hiwase, A., Bagde, G., Tekam, E. & Kalbande, R., "Modified Advanced Encryption Standard", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-4, Issue-1, (2014).

[11] Omran, A. ,"Performance Analysis of AES and LWAES Algorithms", Master, thesis, Iraqi Commission for Computers and Informatics, (2018).

[12] Sadiq, A.T. & Faisal, F.H., "Modification AES algorithm based on Extended Key and Plain Text" , Journal of Advanced Computer Science and Technology Research, ISSN: 2231-8852, Vol.5 No.4, (2015).

[13] Daernen, J. & Rijrnen V., "The Design of Rijndael AES - The Advanced Encryption Standard", © Springer-Verlag Berlin Heidelberg, (2002).

[14] Knudsen, L., "Contemporary Block Ciphers", © Springer-Verlag Berlin Heidelberg, University of Bergen, Department of Informatics, (2008).

[15] Menezes, A., Oorschot, P., & Vanstone, S., "Handbook of Applied Cryptography", CRC Press, (1996).

[16] Maity, S., Sinha, K. & Sinha, B.P., "An Efficient Lightweight Stream Cipher Algorithm for Wireless Networks", IEEE: Wireless Communications and Networking Conference (WCNC) , (2017).

[17] Hameed, S. & Mahmood, I., "A Modified Key Scheduling Algorithm for RC4", Iraqi Journal of Science, Vol. 57, No.1, (2016).

[18] Weerasinghe, T.D.B., "An Effective RC4 Stream Cipher", IEEE 8th International Conference on Industrial and Information Systems, (2013).

[19] Xie, J. & Pan, X., "An Improved RC4 Stream Cipher", IEEE: International Conference on Computer Application and System Modeling, (2010).

[20] Hammood, M.M., Yoshigoe, K. & Sagheer, A.M., "Enhancing Security and Speed of RC4", International Journal of Computing and Network Technology, ISSN 2210-1519, (2015). [21]: O. Goldreich , "Foundations of Cryptography: A Primer", O. Goldreich, Now Publishers Inc., USA, 2005.

[22] Lata, M. & Kumar, A., "Survey on Lightweight Primitives and Protocols for RFID in Wireless Sensor Networks", International Journal of Communication Networks and Information Security (IJCNIS), (2014).

[23] Rivest, R.L., Shamir, A. & Adleman, L. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Commun ACM, (1978).