ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, Vol 9(48), DOI: 10.17485/ijst/2016/v9i48/106505, December 2016 ISSN (Online) : 0974-5645

Data Analysis between Various Symmetric Encryption Algorithms on Wireless Security

S. Revathi[1]* and A. Malathi[2]

[1]Department of Computer Science, Dr. N. G. P Arts and Science College, Coimbatore – 641048, Tamil Nadu, India;
revathisujendran86@gmail.com
[2]Department of Computer science, Government Arts College, Coimbatore – 641018, Tamil Nadu, India;
malathi.arunachalam@yahoo.com

Abstract

Security on the wireless networks is the problem analyzed in this paper based on various symmetric encryption algorithms. This research work is mainly designed to achieve safety measures in wireless network. Symmetrical encrypting algorithms use identical keys for processing. This research works analysis data security based on Advanced Encryption Standard (AES) and Rivest Cipher (RC4) encryption algorithms on various platforms and calculates the performance based on time and memory consumption. The given text was encrypted and decrypted using various key sizes and concluded that compared with RC4, AES is more secure for both encryption and decryption while data transmission. The research analysis have been carried for 16 byte data and proved that AES is approximately 3 times faster than RC4 algorithm for encryption, similarly the decryption is double that of encryption. The memory space require for AES is more than RC4 because AES consist of more routines to calculate values for each rounds. This helps the users to choose the encryption techniques depending on their environment and the need for data protection while transmission.

Keywords: Authentication, Advanced Encryption Algorithm, Rivest Cipher4, Wireless Security, WEP, WPA

1. Introduction

Wireless networks are broadly used by corporate and laptop users. The business and personal data must be secured by a proper security mechanism that is supplied with the network because radio waves are used for data transmission[1]. Thus it becomes important to analyze the various standard security protocols. In this paper, we have analyzed the two important algorithms namely RC4 which is used in WEP (Wired Equivalent Protocol) and AES which is used in WPA2. We have also discussed the flaws of WEP and how they are eradicated in WPA2. AES encryption method is studied in detail with a sample data analysis. Finally, AES is compared with RC4 with certain parameters such as time, power and memory consumption on the light weight devices namely pocket PC and Laptop.

2. Security in Wireless Communication

The security in wireless networks can be ensured by Authentication, Confidentiality, and Integrity of the data which is transmitted via the air media[2]. The type of security mainly based on wireless standards that support the access point or wireless card. Basically, there are three security standards to be considered. They are Wired Equivalent Privacy, Wi-Fi Protected Access and Wi-Fi Protected Access 2[3].

2.1 WEP - Wired Equivalent Privacy Protocol

In order to secure the transmitted data, the protocol allows 64 bit key for encryption technique, which consist of 40 bit key with a 24 bit Initialization Vector (IV).

*Author for correspondence

Later 128 bit (140 bit key size) WEP key has been used to encrypt the data[4]. The RC4 algorithm works in key setup and ciphering phase. In first phase, the key length various from 1 to 256 bytes which is used to initialize 256 arrays bytes denoted as S. The S array contains 8 bits permutation for all numbers from 0 to 255. In second phase, key K is generated from S array based on 255 unique key streams for Encryption and decryption[5].

The vulnerability of WEP

1. Wired Equivalent Privacy uses same key with different IV value to encrypt the data.
2. Unauthorized data integrity.
3. No access point authentication.

2.2 WI-FI Protected Access (WPA)

WPA is used to increase the security level of wireless LANs. The two major modes of WPA are enterprise mode and personal mode. WPA uses Temporal Key Integrity Protocol (TKIP) for key generation. It also uses RC4 algorithm along with Cyclic Redundancy Check mechanism that reduces the security flaws in WEP.

2.3 WPA2 and 802.11i

WPA2 also known as Wi-Fi Alliance, It is a final version of IEEE 802.11i standards. The major difference between WPA and WPA2 is the encryption algorithm used to secure the data on transmission.WPA2 uses Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP) to protect the data. WPA2 also called RSN (Robust Security Network)[7].

3. Algorithm Specification for Advanced Encryption Standard

In this research work the block length of 128 bits be denoted as $Nl= 4$, the number of rounds to be performed is dependent on the Nk size.

For example the number of rounds be Nr, where $Nr =10$ when $Nk= 4$, $Nr = 12$ when $Nk= 6$, and $Nr = 14$ when $Nk= 8$. The Key-Block-Round combinations are given in Table 1.

Table 1. Key-block-round combination

	Key Length	Block Size (Nb words)	Number of Rounds (Nr)
AES 128	4	4	10
AES 192	6	4	12
AES 256	8	4	14

3.1 The Add Round Key Operation

It is applied to each state by using XOR operation based on key length function. The key length (Block) is 16 bytes. The XOR operation is applied based on preceding result of 128 bit keys. For each state byte the round key is derived from cipher key and be never reused.

3.2 The Sub Bytes Operation

It uses S-box (Substitution box) and inverse S-box table values for transformation shown in Table 2 and Table 3. Each bytes are replaced with 8 bit lookup table values $S(b_{ij}) = S(a_{ij})$.

3.3 The Shift Row Operation

In this operation the rows are left shifted cyclically based on previous byte values. The values of first rows remain unchanged.

3.4 The Mix Column Operation

In this round, the four bytes of each column are combined using an invertible linear transformation which affects output bytes during cipher text.

4. Key Expansion

The following cipher key expansion of 128 bit size is:

Cipher Key = 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c

For $Nk= 4$, denoted as

$d0$ = 2b7e1516 $d1$ = 28aed2a6 $d2$ = abf71588 $d3$ = 09cf4f3c.

4.1 AES Key Algorithm

The key schedule algorithm for one dimensional array is explained below that parameterized round key function.

Cipher (byte in[4*Nl], byte out[4*Nl], word d[Nl*(Nr+1)]) [5].

```
Start
    byte[4,Nl]
    S = in
    addroundkey (S, d [0, Nl-1])
```

Table 2. AES s-box lookup table

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

Table 3. Inverse of the s-box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
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

```
    for round = 1 step 1 to Nr–1
    Sub bytes (S)
    Shift rows (S)
    Mix columns (S)
    addroundkey (S, w [round*Nl, (round+1)*Nl-1])
    End for
    Sub bytes (S)
    Shift rows (S)
    addroundkey (S, d[Nr*Nl, (Nr+1)*Nl-1])
    out = S
End
```

4.2 Cipher Example

With the help of the above algorithm, the below example is carried out to encrypt the given text[9]. The block length and Key length of 16 bytes be denoted as *Nl*= 4 and *Nk*= 4. For example on transmitting text as "**Computer world now**" the hex value will be

PLAINTEXT: 63 6f 6d 70 75 74 65 72 77 6f 72 6c 64 6e 6f 77

Nk: 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c

CIPHER (ENCRYPT):

R[0]. Input: 63 6f 6d70 75 74 65 72 77 6f 72 6c 64 6e 6f 77

R[0]. K_sch: 2b 7e 15 16 28 ae d2 a6ab f7 15 88 09 cf 4f 3c

R[1].start: 48 11 78 665d da b7 d4 dc 98 67 e4 6d a1 20 4b

R[1].s_box: 52 82 bc 33 4c 57 a9 48 86 46 85 69 3c 32 b7 b3

R[1].s_row: 52 57 85 b3 4c 4b b7 33 86 32 bc a9 b3 33 48 69

R[1]. m_col: 6b dbda 59 d6 31 2a 43 b5 75 0f 8f 25 AA 2c bd

…

R[10]. Start: 3c 91 6b 1a 0c 9b 5f 60 85 93 b3 49 54 fd 74 e7

R[10].s_box : eb 81 7f a2 fe 14 cf d0 97 dc 6d 3b 20 54 92 94

R[10].s_row: eb 14 6d 94 fe dc 92 a2 97 54 7f d0 20 81 cf 3b

R[10].k_sch: d0 14 f9 a8 c9 ee 25 89 e1 3f 0c c8 b6 63 0c a6

Ciphertext: 3b 00 94 3c 37 32 b7 2b 76 6b 73 18 96 e2 c3 9d

4.3 Decryption

For the same plain text "Computer world now", cipher to plain text conversion is given below:

Ciphertext: 3b 00 94 3c 37 32 b7 2b 76 6b 73 18 96 e2 c3 9d

R[1]: eb 14 6d 94 fe dc 92 a2 97 54 7f d0 20 81 cf 3b

R[2]: 50 79 f2 49 e2 4f 03 18 0c 62 c1 d2 0a 21 c3 b7

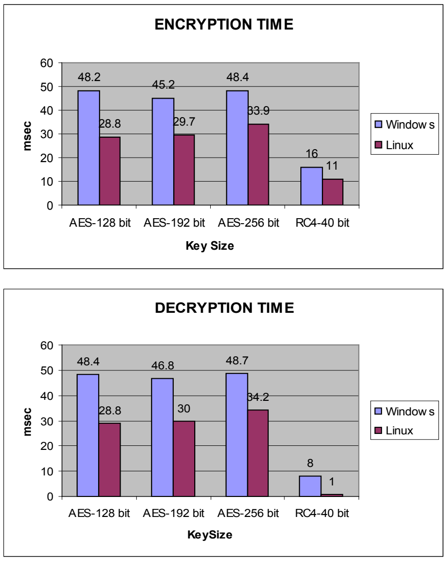

Figure 1. Encryption/decryption time analysis.

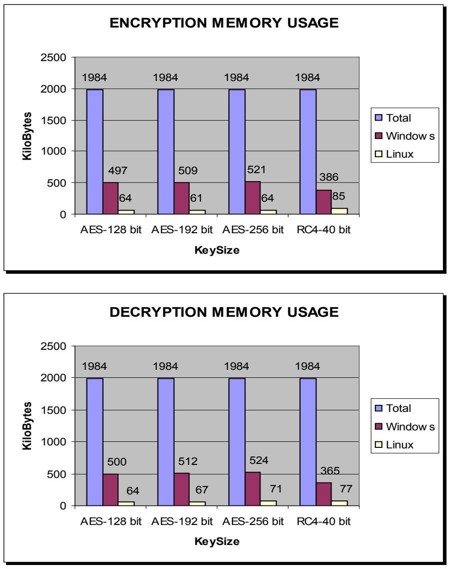

Figure 2. Encryption/decryption memory analysis.

….

R[10]: 52 57 85 b3 4c 46 b7 33 86 32 bc 48 3c 82 a9 69

Plaintext: 63 6f 6d 70 75 74 65 72 77 6f 72 6c 64 6e 6f 77

We obtain the equivalent plain text after decryption. The key expansion and decryption method requires more time for the intruders in the case of AES compared to RC4.

5. Results and Discussions

The performance analysis between RC4 and AES encryption method based on time and memory usage on windows and Linux based operating system[10]. Both the systems were installed with JDK1.5.

Based on various key sizes like 128, 192 and 256, the given text was encrypted and decrypted on both the platforms. The key size is taken on the x-axis and time in y-axis. From Figure 1 and Figure 2, we conclude that AES requires more time and memory for encryption and decryption on both the platforms. The above figures show the time and memory comparison for a single block which contains 16 byte of data only. This can be extended for various block sizes of data.

6. Conclusion

In this paper, we have presented different encryption methods namely WEP, WPA and WPA2 available for ensuring security of data in wireless environment. WEP is the first protocol used for for data protection in wireless LANs. It gains three safety measures as verifying someone's identity, keeping private information secure and maintain quality of the message. In general WEP not having enough methods to secure and verify someone's identity, because of IV value and poor key management that fails to maintain the originality of the data. WPA gives more wireless protection by WI-Fi Standards that increases data protection, access control and integrity. AES counter turn messages into secret code and increase of data protection during transmission; in addition CBC-MAC is used to maintain integrity of the data by mixing encrypted and non-encrypted data blocks. In this paper, we have also compared the two main protocols AES and RC4 on different platforms. This study helps the users to choose the encryption techniques depending on their environment and the need for data protection while transmission. 802.11i standard provides a high level of security to protect data for attacks but still it suffers from DOS attacks (Jamming). So the future work is focused on these sorts of attacks to save the wireless environment.

7. References

1. Wi-Fi Alliance. "Wi-Fi Protected Access – Overview". URL: http://www.wi-fi.com/OpenSection/pdf/Wi- Fi_Protected_Access_Overview.pdf

2. Stallings W. Cryptography and network security: Principles and practice. Prentice Hall, Upper Saddle River, New Jersey; 2003.
3. Knudsen LR. Truncated and higher order differentials. Fast Software Encryption, LNCS 1008, Preneel B editors. Springer-Verlag; 1995. p. 196–211.
4. Borisov N, Goldberg I, Wagner D. Intercepting mobile communications: The insecurity of 802.11. 7th Annual International Conference on Mobile Computing and Networking, Rome, Italy; 2001 July 16–21.
5. Mousa A, Hamad A. Evaluation of the RC4 algorithm for data encryption. International Journal of Computer Science and Application. 2006 Jun; 3(2):44–56.
6. Wong S. The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards. GIAC Security Essentials Certification (GSEC) Practical; 2003.
7. Daemen J, Rijmen V. AES Proposal: Rijndael. The Rijndael Block Cipher. 1999 Sep 3; 2:4–45.
8. Daemen J, Knudsen LR, Rijmen V. The block cipher square. In: Biham E editors. International Workshop on Fast Software Encryption, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg. 1997; 1267:149–65.
9. Lee A. Guideline for implementing cryptography in the federal government. National Institute of Standards and Technology (NIST) Special Publication 800-21, Gaithersburg, MD, United States; 1999 Nov.
10. Barka ES, Mohamed EE, Hayawi K. End-to- end security solutions for WLAN: A performance analysis for the underlying encryption algorithms in the lightweight devices. In the Proceedings of the International Wireless Communications and Mobile Computing Conference (IWCMC), Vancouver, British Columbia, Canada; 2006 July 3–6. p. 1295–300.