International Journal of Security and Its Applications
Vol. 10, No. 2 (2016), pp.279-286
http://dx.doi.org/10.14257/ijsia.2016.10.2.25

A Study to Examine the Superiority of CSAVK, AVK over Conventional Encryption with a Single Key

Rajat S Goswami[1], Swarnendu K Chakraborty[2], Chandan T Bhunia[3]

[1,2,3]*Department of Computer Science & Engineering, National Institute of Technology, Arunachal Pradesh, India*
[1]*rajat.nitap@gmail.com*, [2]*swarnendu.chakraborty@gmail.com*,
[3]*ctbhunia@vsnl.com*

Abstract

Time variant key is one of the great research challenges in the field of cryptography for achieving the perfect security. Automatic variable Key (AVK) has been well researched and established as an important technique to realize time variant key in achieving towards perfect security. In AVK, proposed by Bhunia, the key is made to vary from data to data or session to session that is essentially required for achieving perfect secrecy. The variable key is generated in each time a data is sent and or a session is made. The time variant key (in AVK) is found to reduce the frequency attack as seen in earlier research, while such key was in applied in AES algorithm. In the present experimental research the authors study the application of AVK & Computing & Shifting AVK (CSAVK) in RSA to examine the reducing effect of frequency attack.

Keywords*: AVK, CSAVK, Randomness, Perfect Security, Frequency attack.*

1. Introduction

The fundamental research of Shannon in achieving perfect security is well documented [1-2]. The pioneer work of Bhunia [3-5] in implementing the Shannon's theorem for realization of variable key for variable data / session is well researched [6-16]. The documented research findings used the simple technique of realizing Automatic Variable Key (AVK) as originally proposed by Bhunia. This paper reports and analyses the superiority of Computing & Shifting AVK (CSAVK) and AVK used in RSA over conventional single key encryption in RSA.

In AVK the key is made variable by an agreement that creates new key for each data:

K_0= initial key that may be exchanged by any conventional secret mode between a sender and a receiver like RSA.

Subsequent keys for different data (D_0) exchanged are generated as for from

$K_0=K_{i-1}$ XOR D_{i-1} $i>0$ …….. (1)

The key is made variable with exchanged data between a sender and a receiver. A new key is generated every time a data is exchanged. The new key so generated is used subsequently for further exchange of data.

So far applied AVK is based on the generating function XOR as in equation (1).

In CSAVK [14-15] technique illustrated in below the key is made variable by one agreement that also creates new key for each data.

Say, K_0 = initial key that may be exchanged by any conventional secret mode between a sender and a receiver.

Subsequent keys for different data (D_{i-1}) to be exchanged are generated are:

ISSN: 1738-9976 IJSIA

$K_i = K'_{i-1}$ XOR D'_{i-1} i>0 …….. (2)

Where K'_{i-1} = Bit wise right shifted (circular) K_{i-1} / the number of shift will be the number of 1's present in K_{i-1}.

D'_{i-1} = Bit wise left Shifted (Circular) D_{i-1} / the number of shift will be number of 1's present in D_{i-1}.

Table 1. Elucidation of Application of Simple AVK in Cryptology

Session slots	Sender sends his /her private key to receiver	Receiver recovers private key from sender	Receiver sends his / her private key to sender	Sender receives private key from receiver	Remarks
1	Secret key Say 5(101)	101	A secret key Say 7(111)	111	For next slot sender will use 111 as key and receiver 101 as key for
2	Sender sends first (random 3) data 011⊕111 =100	Receiver gets original data 011⊕111 ⊕111=011	Receiver sends first (random data 9) as 1001 ⊕0101=1100	Sender gets back original data as 1001⊕ 0101 ⊕0101 =1001	Sender will create new key 0111⊕1001 for next slot receiver will create new key 101⊕011
3	Sender sends new data 4(100) as 0100 ⊕0111 ⊕1001	Receiver recovers original data as 0100⊕0111 ⊕1001⊕0111 ⊕1001= 0100	Receiver sends next data 8 (1000)1000⊕ 0101⊕0011	Sender receives original data 1000 ⊕0101 ⊕0011 ⊕0101 ⊕0011 =1000	Sender computes new key 011⊕100 receiver computes key 1001⊕1000 for transmitting next data

2. Comparison of Frequencies of Appearance of Characters after Applying Various Techniques of Key Generations (AVK & CSAVK) in RSA

Original Message (Plaintext)

Bold letters are representing the letter 'f', underlined letters are representing the letter 'i' and italics letters representing numeric '0'.

Plaintext 1: **f**inanci̲al bi̲d= Rs 37*00* **f**or modem.

Plaintext 2: **f**inanci̲al bi̲d = Rs 37*000* **f**or machine.

Encrypted message under conventional RSA

8859/3503/9944/4269/9944/2518/3503/4269/5505/4990/4269/3503/2518/3249/4990/973/355/4990/9110/2528/*2837/2837*/4990/**8859**/4224/3342/4990/5505/4224/2518/6030/5505/458

8859/3503/9944/4269/9944/2518/3503/4269/5505/4990/4269/3503/2518/4990/3249/4990/973/355/4990/9110/2528/*2837/2837/2837*/4990/**8859**/4224/3342/4990/5505/4269/2518/618/3503/9944/6030/458

Encrypted message under RSA with AVK

8859/4121/609/4267/9944/5448/3606/9216/4494/5317/4754/7520/3431/1459/5056/4671/6996/158/6692/8221/*7269/4446*/2819/**4121**/318/9292/6297/4709/6718/6681/7221/3702/6835

8859/4121/609/4267/9944/5448/3606/9216/4494/5317/4754/7520/3431/3767/6930/7404/6832/7287/3978/2521/9109/*2641/1671/2641*/7738/**5048**/5531/250/6316/8548/4754/1366/8343/1752/2534/3913/1191

Encrypted message under RSA with CSAVK

8859/4121/5482/9216/615/2215/8550/8729/2312/1458/2329/4018/5071/4330/5056/8656/7080/2419/6163/1017/*4446/2544*/9840/**8857**/3154/167/9219/6620/1205/4387/3359/1459/4928

8859/4121/5482/9216/615/2215/8550/8729/2312/1458/2329/4018/5071/158/6571/4225/2403/9431/7394/4410/9140/*9518/9003/3077*/1936/**1235**/1432/2912/9926/5119/1939/3527/7725/6284/1842/3140/6938

Table 2. Occurrence of Characters of Plaintext-1 and Encrypted Text by using Conventional RSA and RSA with AVK & CSAVK

Letter	Plain text	RSA	AVK	CSAVK
f	2	2 (8859)	1 (8859/ 4121)	1 (8859/8857)
i	3	3 (3503)	1 (4121/3606 / 7520)	1 (4121/ 8550/ 4018)
0	2	2 (2837)	1 (7269/ 4446)	1 (4446/ 2544)

Table 3. Occurrence of Characters of Plaintext-2 and Encrypted Text by using Conventional RSA and RSA with AVK & CSAVK

Letter	Plain text	RSA	AVK	CSAVK
f	2	2 (8859)	1 (8859 / 4121)	1 (8859 / 1235)
i	3	3 (3503)	1 (4121 / 3606 / 7520)	1 (4121/ 8550 / 4018)
0	3	3 (2837)	2 (2641 / 1671)	1 (9518/ 9003/ 3077)

3. Illustration of AVK, CS AVK & DSAVK

3.1. Illustration of AVK

Authors assume that sender sends original data (D_0) 11010011 in encrypted form using an initial key (K_0) = 01011111. Then in order to maintain the linearity, the encrypted form is 11010011 XOR 01011111 = 10001100.
At receiver end receiver will perform 10001100 XOR 01011111 and gets 11010011.

3.2. Illustration of CSAVK

Let sender sends initial data (D_0) 11010011 in encrypted form using key (K_0) = 01011111. As per technique of CSAVK of eqn. (2) next key will be generated in the next data transmission by left shifting the previous data (D_0) up to the total number of 1's present in that data (SD_0) XOR with right shifting the previous key (K_0) up to the total number of 1's present in that key (SK_0).

So the new key will be $K_1 = SD_0 \oplus SK_0$ = 01111010 $\oplus$ 11111010 = 10000000.

4. Analysis and Comparison

Randomness as a measure of amount of variation made between two cypher texts of same character. The randomness for the purpose is defined as the number of bit location in which any two successive cipher text vary. For example if:

$$C_1=11111010, C_2=10001001$$

The randomness between two successive cipher texts is 5. We call C_1 is random to C_2 by 5.

From the above experimental results obtained so far, we tried to do the frequency analysis of characters of encrypted text with RSA AVK, RSA CSAVK over conventional RSA with single key. Following are the observations:

- For similar set of data and initial keys the graph of randomness for RSA, RSA with AVK & CSAVK which is portrayed in fig. (1-2)
- Frequencies of appearance of repeated 'f', 'i' and '0' is in cypher of conventional single key RSA are 2, 3 and 2 respectively whereas the said frequency in cipher in RSA with AVK and CSAVK is 1 only.
- Randomness is measured under the same experiment and it is seen that for some set of keys the randomness are varying for same plaintext in different session of secure data transmission. In some cases it is found that the superiority of AVK technique over CSAVK technique as illustrated in table-2, but in some cases as in table-3 CSAVK is found to be superior to AVK.
- In the experimental result of plaintext-2, it is observed that the frequency of occurrences of plaintext numeric '0' in cipher with RSA with AVK is 2 and 1in RSA CSAVK.

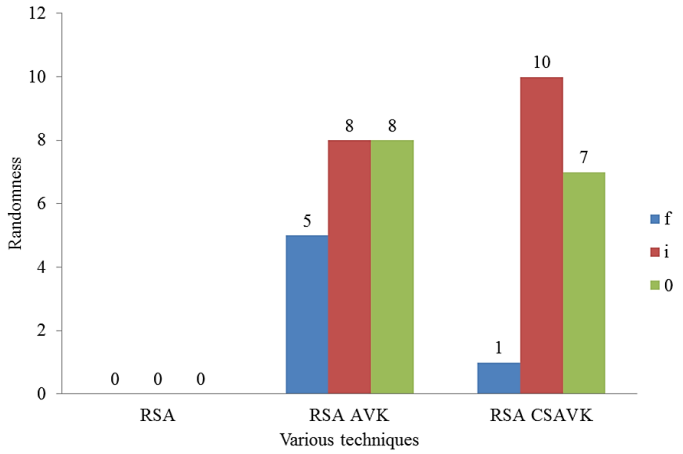

Figure 1. Randomness of Encrypted Text in Conventional RSA and RSA with AVK & CSAVK for Plaintext-1

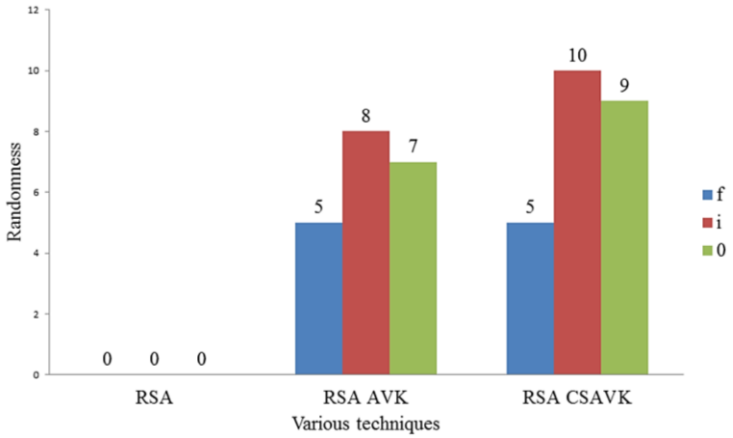

Figure 2. Randomness of Encrypted Text in Conventional RSA and RSA with AVK & CSAVK for Plaintext-2

5. Conclusions

The AVK and the CSAVK are well researched. In this paper the authors have applied CSAVK and AVK techniques over conventional cryptographically algorithm RSA with single key. To establish the superiority of CSAVK over AVK, experimentation has been done with two numbers of plaintext. In plaintext-1, it is seen that for two consecutive numeric '0' both RSA with AVK and RSA with CSAVK produces two different cypher text whereas for plaintext-2 for three consecutive numeric '0' RSA with AVK produces two different encrypted text and RSA with CSAVK produces three different encrypted text. So far frequency attack is concerned, to reduce the frequency of occurrences of one character in cypher text; from the above observation it can be concluded that, CSAVK is much more effective than AVK technique. The new technique (CSAVK) need to be applied in various encryption / decryption techniques like DES, AES to examine the effect on brute force attack and differential frequency attack to realize the superiority over AVK.

References

[1] C E Shannon, "Mathematical theory of communication", The Bell System Tech J, Vol.27, **(1984)**, pp. 379-423, 623-656.
[2] C E Shannon, "Communication Theory of Secrecy System" The Bell System Tech J, **(1949)**.
[3] C.T.Bhunia, G.Mondal, S.Samaddar, "Theory and application of time variant key in RSA and that with selective encryption in AES", Indian Engineering Congress, Kolkata, **(2006)**.
[4] C. T. Bhunia, "New approaches for selective AES towards tackling error propagation effect of AES", Asian Journal of Information Technology, 5990, **(2006)**, pp. 1017-1022.
[5] P. Chakrabarti, B. Bhuyan, A. Chowdhuri and C.T.Bhunia, "A novel approach towards realizing optimum data transfer and automatic variable key (AVK)", International Journal of Computer Science and Network Security, Vol. 8, no.5, **(2008)**.
[6] C Konar, C T Bhunia, "A novel approach towards realizing optimum Data Transfer and AVK in cryptography", International Journal of Computer Science and Network Security, vol. 8, no. 5, pp. 241-250.
[7] C T Bhunia, "New Approaches for Selective AES towards Tackling Error Propagation Effect of AES", Asian Journal of Information Technology, vol. 5, no. 9, **(2006)**, pp. 1017- 1022.
[8] B Bhuyan, P Chakraborti, A Chowdhuri, F Masulli, C T Bhunia, "Implementation of Automatic Variable Key with Choas Theory and Studied Thereof", J IUP Computer Science, vol. 5, no.4, **(2011)**, pp. 22-32.
[9] C T Bhunia, G Mondal, S Samaddar, "Theories and Application of Time Variant Key in RSA and that with selective encryption in AES", Proceedings EAIT, Elsevier Publications, **(2006)**, Calcutta CSI, pp. 219-221.
[10] P.Chakrabarty, C T Bhunia, "A novel approach towards realizing optimum Data Transfer and AVK in cryptography", International Journal of Computer Science and Network Security, vol. 8, no. 5, **(2008)**, pp. 241-250.
[11] C. T. Bhunia, Swarnendu Kumar Chakraborty, Rajat Subhra Goswami, "A New Technique (CSAVK) of Automatic Variable Key in Achieving Perfect Security", 100th Indian Science Congress Association, **(2013)**, Kolkata.
[12] Rajat Subhra Goswami, Swarnendu Kumar Chakraborty, Abhinandan Bhunia, C. T. Bhunia, "New approach towards generation of Automatic Variable Key to achieve Perfect Security", IEEE computer Society, CPS, **(2013)**,USA, pp. 489-491.
[13] R. S. Goswami, S. K. Chakraborty, A. Bhunia, C. T. Bhunia, "Various New Methods of Implementing AVK", 2nd International Conference on Advances in Computer Science and Engineering, Los Angeles, USA, ,CSE2013, Atlantis Press, **(2013),** 149-152.
[14] R. S. Goswami, S. K. Chakraborty, A. Bhunia, C. T. Bhunia, "New Techniques for generating of Automatic Variable Key in Achieving Perfect Security", Journal of Institute of Engineers, India (Springer) Series B, vol. 95, no. 3, **(2014)**, pp.197-201.
[15] R. S. Goswami, S. K. Chakraborty, A. Bhunia, C. T. Bhunia, "Generation of Automatic Variable Key under various approaches in Cryptography System", Journal of Institute of Engineers, India (Springer) Series B, vol. 94, no. 4, **(2014)**, pp. 215-220.

Authors

Rajat Subhra Goswami, He is working as an Assistant Professor in the department of Computer Science and Engineering at National Institute of Technology Arunachal Pradesh, Govt. of India. He is having more than 8 years of teaching experience. His research areas are cryptography and information security. He is the author of 20 peer-reviewed publications. In 2013, he got international travel support grand from Department of Science & Technology to present one of his research papers at Los Angeles, USA. In 2013, he was awarded as best teacher for the academic year 2012-2013. He received his Ph.D from National Institute of Technology Arunachal Pradesh in 2015.

Swarnendu Kumar Chakraborty, He is working as an Assistant Professor & HoD in the department of Computer Science and Engineering at National Institute of Technology Arunachal Pradesh, Govt. of India. He is having more than 6 years of teaching experience. His research areas are advanced error control, cryptography and information security. He is the author of 22 peer-reviewed publications. In 2013, he has visited USA to present his one of article in ITNG 2013, he was awarded as best teacher for the academic year 2010-11. He received his Ph.D from National Institute of Technology Arunachal Pradesh in 2015.

Chandan T Bhunia, He earned his B.Tech in radio physics and electronics in 1983 from the Calcutta University, and then joined DVC of Govt. of India as telecommunication engineer. He got M.Tech in radio physics and electronics in 1985, and then joined North Bengal University as a lecturer of computer science & application in 1988, and became Assistant Professor of electronics & communication engineering at the North Eastern Regional Institute of Science & Technology (NERIST) of Govt. of India in 1990. He got his PhD in computer science &engineering from the Jadavpur University. He became full Professor in 1997 at NERIST where he was HOD of ECE & CSE for about 6yrs and Dean (Academics/Post Graduate Studies) for about 1.5 years. He then switched to private engineering colleges from 1999 to 2003 as HOD, Deputy Director and Director. Lastly, he was a full Professor of computer science & engineering of the Indian School of Mines (Deemed University) of Govt of India. He was a senior Professor and Dy Director (Acad) of Haldia Institute of Technology. He has extensively visited foreign countries, namely China, Italy, Singapore, UK and Bangladesh on several assignments including BOYSCAST Fellowship and ICTP senior associate ship. He has published around 200 research papers and technical articles/reports in national/international journals/magazines/seminars. He is the author of the books a) "Introduction to Knowledge Management" published by Everest Publishing House, Pune in 2003 and b) "Information Technology, Network and Internet", published by the New Age International Publishers, New Delhi. He is Fellow of the IETE and the IE(I), and a senior member of the IEEE & CSI. He is currently as a director of NIT Arunachal Pradesh.