www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
Vol. 02, Issue 05, May 2022, pp : 183-188

e-ISSN : 2583-1062
Impact Factor : 2.205

STRATEGY TO CREATE VARIABLE KEYS IN MODERN CRYPTOGRAPHY

Moumita Das[*1], Chowdhury Md. Mizan[*2], Suparna Karmakar[*3], Prince Kumar[*4]

[*1,2,3,4]Department of Information Technology, Guru Nanak Institute of technology, Kolkata, India.

ABSTRACT

Information Security is an area of study and professional activity concerned with the development and implementation of security countermeasures of all available sections (technical, organizational, human-oriented and legal) to keep information securely in all its locations and, consequently, in information systems where information is created, processed, stored, destroyed, transmitted, etc. The major objective of this research is to provide such an environment in a public network where the information can be exchanged securely between the authorized entities.

Keywords: CSAVK, ASAVK, DKAVK, KVRN, Randomness, Standard Deviation.

1. INTRODUCTION

There is a developing enthusiasm for innovative work in the territory of data security with the expansion of stealing of computational resources, disruption of computational directions, unapproved exposure and alteration of PC data. Additionally there also have been various PC break-ins and security ruptures. This research work starts with a declaration of the issue of information security and presents a total situation of past and present related research work with appropriate outcomes. Since the beginning of the 21st century, the utilization of the internet developing exponentially, keeping up the secrecy in the domain of technology and innovation has turned into a significant issue. A key in cryptography is a parameter that governs a cryptographic algorithm's efficient output. The level of security of cipher text may be improved if both the encryption/decryption algorithm and secret key can be hidden. The resilient power of cipher text-only attack solely lies on the secrecy of the key. It implies that if key guessing is made very difficult, there is no need to hide the encryption/decryption algorithm. To prevent cipher text-only attack, brute force attack, frequency attack, etc., the keys are made larger enough so that in linear polynomial time, the attacker cannot attempt all possible combinations. Shannon's [1-2] vital security investigation recommended that if the key is rendered inconsistent in information correspondence from information to information or session to session, better security can be identified. An administrative methodology for mitigating the issue of data security we have proposed some new techniques of Auto. Var. Kay as well as the advancement of Auto. Var. Key with a noise burst (AVK with a NB). Auto. Var. Key's pre dominance suggests that new schemes can be applied to standard algorithms such as AES [7], and DES [29-30] for encipherment and decipherment that can raise the level of security in different genuine applications. The produced keys of Auto. Var. Key with a noise burst and Auto. Var. Key without noise burst are well established in this research work. The practical approach of better security was invented by Bhunia [6-8] in the year 2006 which is known as Automatic Variable Key (AVK) technique. Other researchers namely, Goswami [11-16], Banerjee and Dutta et.al. [9-10] have proposed easier a few more secure techniques based on the working principle of Automatic Variable Key (AVK) in terms of randomness, root mean square and standard deviation. The idea behind AVK technique can be stated as:

Let us assume, K_0 be the initial key which will be exchanged between sender and receiver in a secret mode. Subsequent keys for the data D_i to be sent will be automatically generated by computational technique $K_i=K_{i-1}\oplus D_{i-1}$

The following are the algorithms based on the principle of AVK technique and have been used while proposing our algorithms in this manuscript.

Goswami et. al. has proposed CSAVK [11] technique in which the key is made variable. Successive keys for different data (D_{i-1}) can be generated with the help of following equation:

$K_i=K'_{i-1} \oplus D'_{i-1} \star \quad i > 0. \ldots\ldots\ldots\ldots\ldots\ldots (1)$

where K'_{i-1} = Bit wise right shift of key K_{i-1} by the number of 1's present in K_{i-1} and

D'_{i-1} = Bit wise left shift of data D_{i-1} by the number of 1's present in D_{i-1}.

ASAVK [14] technique, also proposed by Goswami et al., creates new key for each data inthe following way.

Initial key K_0 is exchanged between sender and receiver and subsequent key K_i (i^{th} stage) is generated by both sender and receiver as per the following equations:

$K_i=K'_{i-1} \oplus D_{i-1} \star \quad i > 0. \ldots\ldots\ldots\ldots\ldots\ldots(2)$

$K_{i+1}=K_i \oplus D'_{i-1} \star \quad i > 0 \ldots\ldots\ldots\ldots\ldots\ldots(3)$

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
Vol. 02, Issue 05, May 2022, pp : 183-188

e-ISSN : 2583-1062
Impact Factor : 2.205

where $K^{'}_{i-1}$ = Block wise shift of key K_{i-1} and the number of shift will be total length of K_{i-1} divided by 2 and $D^{'}_{i-1}$ = Block wise shift of data D_{i-1} and the number of shift will be total length of D_{i-1} divided by 2.

DKAVK[16] technique is also proposed to generate new key for each data in which initial key K_0 is exchanged between sender and receiver and subsequent key K_i (i^{th} stage) is generated by both the parties as follows:

$K_i = D_{i-1}$ ..... (4)

$K_{i+1} = D_{i-1} \oplus D_i$ ✯ $i > 0$.....(5)

where D_{i-1} = previous data and D_i= current data.

In case of KVRN [13] technique

1. Initial key K_0 and one numeric value are exchanged between sender and receiver.
2. Subsequent keys K_i is generated by both sender and receiver as
3. $K_i = K_{i-1} + X$…… (6) for $i > 0$ and X = 1 to mwhere K_{i-1} is the previous key
4. When X = m, another key (K_m) and one numeric value (n) are exchanged between sender and receiver
5. Subsequent keys will be generated as per equation number (6).

2. PROPOSED SCHEME

We propose new techniques to generate new keys in AVK technique with noise burst. The main purpose of our research is to enhance the security features by increasing the randomness between two successive keys.

Working principle of the proposed techniques can be stated as:

- Initial key (K_0) and noise burst will be exchanged between the communicating parties.
- Following key (K_i) is generated by both the parties.
- The bits of noise burst will be read from left to right and reading of noise burst will be continued until the end of all bits of noise burst.

Case 1: At first, bits of noise burst will be read. If noise burst bit is 1, then, new key will be generated according to the principle of CSAVK technique (as per equation number 1). If noise burst bit is 0, then, new key will not be generated and the current key will be as same as the most recent key. This new technique can be termed as CSAVK technique with noise burst (CSAVK with NB).

Case 2: If bit of noise burst is 1, then, new key will be generated as per ASAVK technique (equation number 2-3). If noise burst is 0, then, no new key will be generated and the key will be as same as the most recent one. The outcome of case 2 can be referred to as ASAVK technique with noise burst (ASAVK with NB).

Case 3: If noise burst bit is 1, then key will be generated based on DKAVK technique as per equation number (4-5). If noise burst bit is 0, most recent key will be the next key. We have named the proposed technique as DKAVK technique with noise burst (DKAVK with NB).

Case 4: The new key will be generated as per KVRN technique when noise burst bit is 1 as per equation number (6) and if bits of noise burst is 0 , no new key will be generated, the key will be as same as the most recent one.

In the research, we have compared our proposed techniques with CSAVK technique without noise burst, ASAVK technique without noise burst, DKAVK technique without noise burst and KVRN technique without noise burst.

Example 1: CSAVK technique with noise burst (CSAVK with NB)

In this example, initial key K_0 = 0111100000111101111000101001000011110001001000 0010100110100011001101111000101001100011110001000110001100111001101000001

010011101 and noise burst = 0011110100111101011000101111010011110101001010101

0100110101011011110010100101010111101100110101011010111011100110100010001

0100101 with data D_0 = 0101010001110111011011110010000001101011011001010111

1001011100110010110000100000011010010110111001110011011101000110010101100

001 are assumed. Then the subsequent keys will be generated as per equation number (1)as follows:

1st bit of noise burst is 0, so the next key will be same as the previous key hence,

K_1 = 0111100000111101111000101001000011110001001000001010011010001100110 1

1110001010011000111100010001100011001110011010000010100111100

2nd bit of noise burst is 0 so the new key will be same as the previously generated keys:

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
Vol. 02, Issue 05, May 2022, pp : 183-188
e-ISSN : 2583-1062
Impact Factor : 2.205

K_2 = 01111000001111011110001010010000111100010010000010100110100011001101
111000101001100011110001000110001100111001101000001010011100

3rd bit of noise burst is 1 so the new key will be:

K_3 = 1111000100010000111011010110000000101010100010110000010010100101001
0011011101101001000011110110111011101101110010001001110110110

4th bit of noise burst is 0 so the key will be as same as previous key

K_4 = 11110001000100001110110101100000001010101000101100000100101001010010
011011101101001000011110110111011101101110010001001110110110

And the procedure is continued until noise burstG Ø.

Example 2: ASAVK technique with noise burst (ASAVK with NB)

Here, we have considered initial key K_0 = 01111000001111011110001010010 000111100
0100100000101001101000110011011110001010011000111100010001100011001110011
01000001010011101 and data D_0 = 0101010001110111011011110010000001101011011
0010101111001011100110010110000100000011010010110111001110011011101000110
010101100001 with noise burst = 001111010011110101100010111101001111010100101
0101010011010101101111001010010101011110110011010101101011101110011010001
0010100101.

Then the subsequent keys will be generated as per ASAVK technique (equation number(2-3)):
1st bit of noise burst is 0, so the next key will be as same as previous key

K_1 = 01111000001111011110001010010000111100010010000010100110100011001101
111000101001100011110001000110001100111001101000001010011101K_2 =
01111000001111011110001010010000111100010010000010100110100011001101
111000101001100011110001000110001100111001101000001010011101

And the procedure is continued until noise burst Ø.

Example 3: DKAVK technique with noise burst (DKAVK with NB)

Let us consider, initial key K_0= 01111000001111011110001010010000111100010010000
0101001101000110011011110001010011000111100010001100011001110011010000010
10011101 and data D_0 = 0101010001110111011011110010000001101011011001010111
1001011100110010110000100000011010010110111001110011011101000110010101100
001with noise burst = 001111010011110101100010111101001111010100101010101001
1010101101111001010010101011110110011010101101011101110011010001001010010
1 for this experiment.

The successive keys can be generated as per DKAVK technique (equation number (4-5)): 1st bit of noise burst is 0, so the next will be generated as follows:

K_1 = 011110000011110111100010100100001111000100100000101001101000110 01101
111000101001100011110001000110001100111001101000001010011101

K_2 = 01111000001111011110001010010000111100010010000010100110100011001101
111000101001100011110001000110001100111001101000001010011101

and the key generation is continued until noise burst Ø.

Example 4: KVRN technique with noise burst (KVRN with NB)

Let us assume, initial key K_0 = 0111100000111101111000101001000011110001001000
0010100110100011001101111000101001100011110001000110001100111001101000001
010011101 with data D_0 = 0101010001110111011011110010000001101011011001010 1
1110010111001100101100001000000110100101101110011100110111010001100101011
00001 with noise burst = 0011110100111101011000101111010011110101001010101010
0110101011011110010100101010111101100110101011010111011100110100010010100
101

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
Vol. 02, Issue 05, May 2022, pp : 183-188
e-ISSN : 2583-1062
Impact Factor : 2.205

Then the subsequent keys will be generated as per KVRN technique (equation number(6)):

1st bit of noise burst is 0, so the next will be same as previous key

K_1 = 01111000001111011110001010010000111100010010000010100110100011001101
111000101001100011110001000110001100111001101000001010011100

2nd bit of noise burst is 0 so the next key will be same as previous key

K_2 = 01111000001111011110001010010000111100010010000010100110100011001101
111000101001100011110001000110001100111001101000001010011100

3rd bit noise burst is 1 so the next new key will be generated as follows:

K_3 = 110000101100101101111111100010011010100000101011101011101001011100000
01011011000011000111000010010001010110111011100111111010001010

and the keys will be generated until noise burst G Ø and the keys generated are as follows:

2.5. Explanation of existing CSAVK technique without noise burst, ASAVK technique without noise burst, DKAVK technique without noise burst and KVRN technique without noise burst:

Let us assume that sender sends initial key K_0 = 011110000011110111100010100100001
1110001001000001010011010001100110111100010100110001111000100011000110011
10011010000010100111O1 with data D_0 = 0101010001110111011011110010000001101O
110110010101111001011100110010110000100000011010010110111001110011011101O
0011001010110000. The new key will be as per CSAVK technique:

K_1 = 0011100011100111111000011010100000000000000110101001010110111111110010
0101010000110001001110101100011111011001101100011111110001110

In case of ASAVK technique, the key will be generated by equation number (2-3) when initial key K_0 = 0111100000111101111000101001000011110001001000001010011010O
011001101111000101001100011110001000110001100111001101000001010011101

with data D_0 = 01010100011101110110111100100 0000110101101100101011110010111
0011001011000010000001101001011011100111001101110100011001010110000

And new key will be as follows:

K_1 = 01001010011010010111000100111110011101010111101101100111011011010010
001101011000110011010101001000111011010111011100011001010110

K_2 = 11010011001000100111100100100110001010011110001000101111011101011111
111111010100010010010101111111010111100110011100101110111011

Again, we have considered that sender sends initial key K_0 = 01111000001111011110001
0100100001111000100100000101001101000110011011110001010011000111100010001
10001100111001101000001010011101 with data D_0 = 010101000111011101101111001
0000001101011011001010111100101110011001011000010000001101001011011100111
001101110100011001010110000.

According to DKAVK technique (equation number 4-5), the new key will be generated asfollows:

K_1 = 01010100011010000110010100100000011011010110010101110011011100110110
000101100111011001010010000001100101011110000111000001100001

K_2 = 00111010000110110000110001001111000000110100010100010110000111010001
001000010010000101110100010100010110010101000101000000010101

In case of KVRN technique, initial key K_0 = 011110000011110111100010100100001111
0001001000001010011010001100110111100010100110001111000100011000110011100
1101000001010011101 with data D_0 = 01010100011101110110111100100000011010110
1100101011110010111001100101100001000000110100101101110011100110111010001
1001010110000. The key will be generated as per equation number (6) as follows:

K_1 = 00101100010010101000110110110000100110100100010111011111111111111111
0010000001001111001100111111111111111100100101110011111111101

K_2 = 01001000011010101110001011010110101110100010101010110001100110101101

1110001010011000011100001101100110101011001010000100100011111

3. PERFORMANCE ANALYSIS

For performance analysis of the proposed techniques, we have assumed initial key K_0 = 01 1110000011110111100010100100001111000100100000101001101000110011011110001 0100110001111000100011000110011100110100000101001101 and noise burst = 00 11 110100111101011000101111010011110101001010101010011010101101111001010010 1010111101100110101011010111011100110100010010100101with following dataset

"Two keys, instead of one, are created, one between Alice and Eve and one between Eve and Bob, When Alice sends data to Bob encrypted with key K1 and it can be deciphered and read by Eve, Eve can send the message to Bob encrypted by key K2 or she can even change the message or send a totally new message, Bob is fooled into believing that message has come from Alice, and the same thing will happen in the other direction".

We have calculated the randomness, average randomness and standard deviation by using same initial key and data set pairs with noise burst which have been depicted from Figure 1 to 3. For analysis, we have assumed randomness as a parameter. Randomness is a measure of amount of variation occurred between two successive keys. For example if K_i = 01010101111101100111 and K_{i+1}= 00011101010110011000 then the randomness between K_i and K_{i+1} is 12. When we apply noise burst to the existing algorithms, more productive and superior results are obtained.

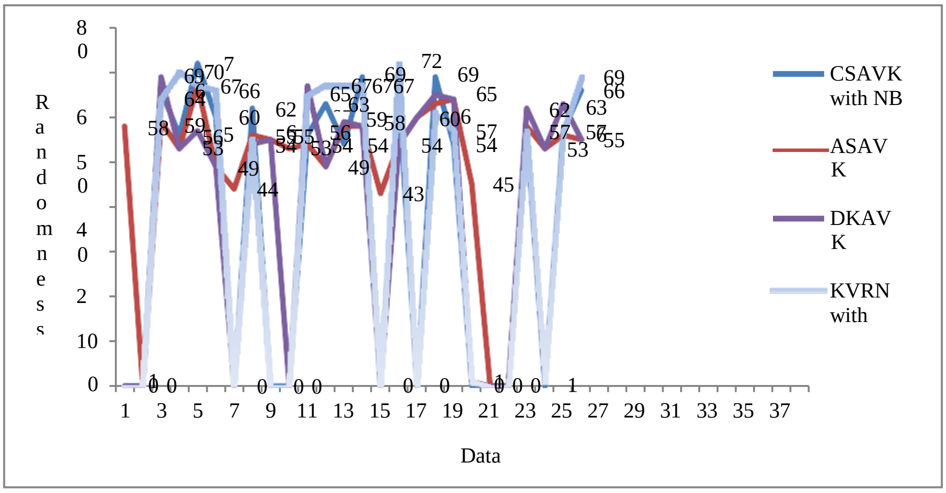

Figure 1: Randomness of keys of CSAVK with NB, ASAVK with NB, DKAVKwith NB and KVRN with NB

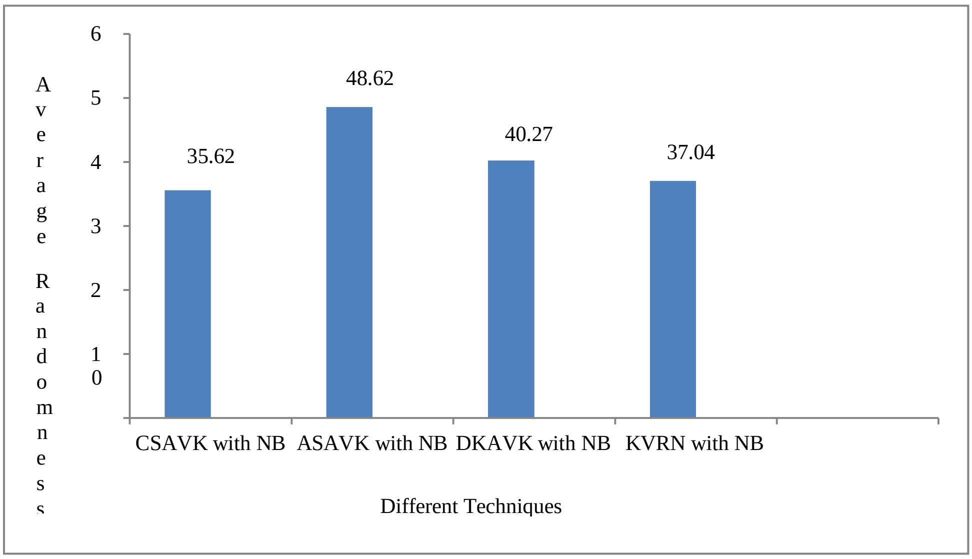

Figure 2: Average Randomness of CSAVK with NB, ASAVK with NB, DKAVKwith NB and KVRN with NB

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
Vol. 02, Issue 05, May 2022, pp : 183-188

e-ISSN : 2583-1062
Impact Factor : 2.205

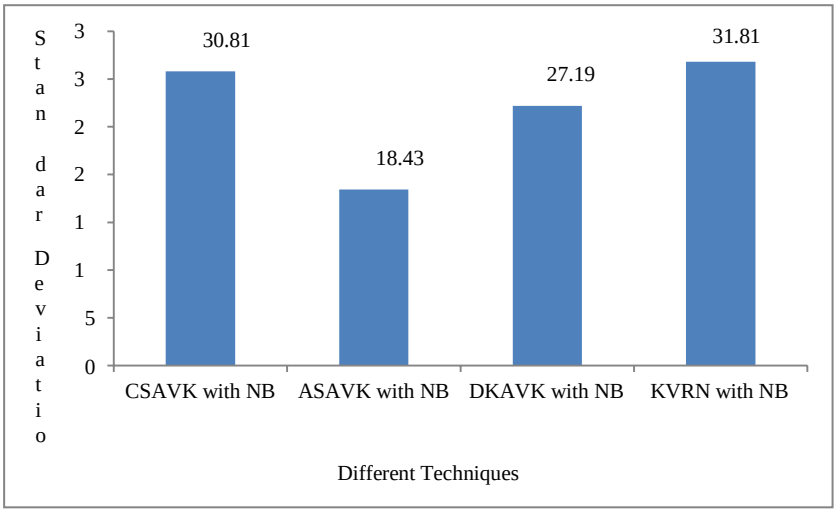

Figure 3: Standard Deviation of CSAVK with NB, ASAVK with NB, DKAVK with NB and KVRN with NB

4. CONCLUSION

We calculated average randomness and standard deviation of auto-generated successive keys in our proposed schemes that can be used for security purposes in various cryptographic applications. The generated Automatic Variable Computing and Shifting Key with a noise burst (CSAVK with a NB), Alternating and Shifting Auto. Var. Key with a noise burst (ASAVK with a NB), Data as a Key in Auto. Var. Key with a noise burst (DKAVK with a NB), Key Variation with Random Noise Burst (KVRN with a NB) techniques are well established.

5. REFERENCES

[1] Shannon, C E. (1949). Communication Theory of Secrecy System, the Bell SystemTech J.

[2] Shannon,C E. (1948). A Mathematical Theory of Communication, Bell System Tech J,27, 379-423,623-656.

[3] Diffie,M.,Hellman,E. (1977). Exhaustive Cryptanalysis of the no of bits Data Encryption Standard. Computer, pp.74-84.

[4] FIPS 140-1 (1994). Security Requirements for Cryptographic Modules. Federal Information Processing standards Publication140-1.U.S, department of Commerce
/NIST, National Technical Information science, Springfield, VA.

[5] Bhunia, C. T. (2006).New Approach for Selective AES towards Tackling Error Propagation Effect of AE. ASIAN Journal of Information Technology, volume 5990, pp.1017-1022.

[6] Bhunia,C.T.(2005). Information Technology, Network and Internet. New age publication.

[7] Bhunia,C.T.(2011).Implementation of AVK with Chaos Theory and Studied Thereof.J IUP Computer Science volume V, No 4, pp.22-32.

[8] Singh,B. K.,Banerjee, S., Dutta, M. P., Bhunia,C. T.(2014).Generation of Automatic Variable key to Make Secure Communication. International Conference on Recent Cognizance in Wireless Communication& Image Processing-ICRCWIP.

[9] Dutta, M.P., Banerjee, S., Bhunia,C. T.(2015).Two New Schemes to Generate Automatic Variable Key to Achieve the Perfect Security in Insecure Communication Channel. In preceding of the International Conference on Advanced Research in Computer Science Engineering &Technology (ICARCSET, Eluru, India),