Variable Key : A new investigation in cryptography and results thereoff

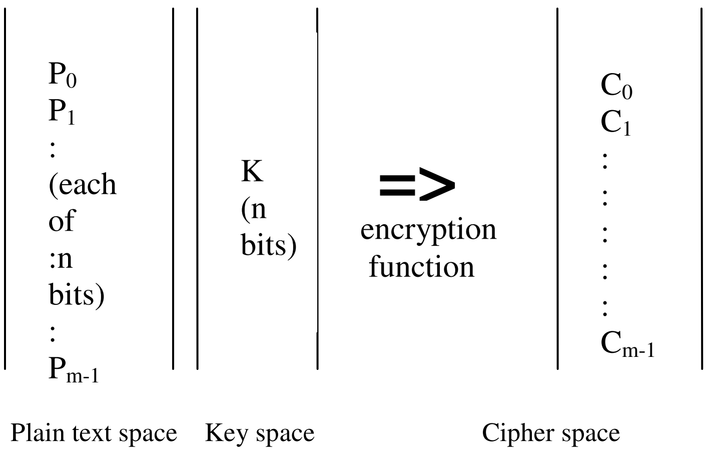
P. Chakrabarti [1], *LMISTE* C.T.Bhunia [2], B. Bhuyan[3]
[1]Bengal Institute of Technology and Management, Santiniketan , West Bengal , Pin-731236,India
[2] Bengal Institute of Technology and Management, Santiniketan and ICTP, 34014 Trieste , Italy
[3]North Eastern Hill University, Shillong , Assam , India
Main/Corresponding author email_id : **prasun9999@rediffmail.com**

Abstract- **This paper deals with the Automatic Variable Key(AVK) that has been studied elsewhere as time variant key for information security. AVK has a very effective approach for achieving highest level of security as per Shannon. We make a study on the essence of automatic variability of key in maintaining perfect secrecy cryptosystem . It is shown that Automatic Variable Key (AVK) is necessary for security enhancement in DES, Trapdoor Knapsack Problem , Vernum Theory , ECB mode of DES.**

1. INTRODUCTION

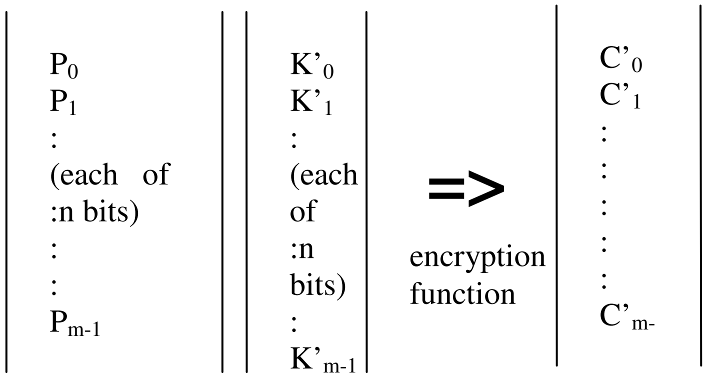
The superiority of time variant key in achieving perfect security is studied further in [1-6]. The famous Vernum Code was the first attempt in the direction of achieving perfect secrecy but no effective variable key has yet been applied neither any concrete theory has been established . For this reason , recently an approach AVK (Automatic Variable Key) has been proposed where key has been made as a function of previously transmitted secret data .The need of automatic variability of key can be explained suitably. If P be a matrix containing plaintext (say n x m data) , K be another matrix containing fixed key k . Then if C be the cipher matrix , then $C_{IJ} = f(K, A_{IJ})$, I and J respectively indicating row number and column number and A_{IJ} is an element of message matrix.Using automatic variable key , the matrix K will also hold (n x m)values and in that case $C_{IJ} = f(K_{IJ}, A_{IJ})$. Here the security level is increased as the attacker has to deal with much more number of keys in order to crack it. The superiority of time variant , AVK over fixed key in terms of brute force attack and differential frequency attack is illustrated below:

(i)Fixed key



Under Brute Force Attack , average number of trials to break a key = 2^{n-1} . The trial is required to be completed in full message encryption time ,T.……………………………..(1)
Under differential frequency attack , if there are R repetitions in plain text then there will be exactly R repetitions in the cipher. This will provide a cipher breaking probability by differential frequency attack = R/m................................(2) , m being the number of messages.

(ii)Under AVK



Under Brute Force Attack , average number of trials to break a key = m * 2 $^{n-1}$,that is required in time T/m …………………………………………………………...(3)

Even if there are R repetitions, there will be no repetition in the cipher. The cipher breakage probability under differential attack is then 0. …………………………………………….(4)

Comparison of (1) with (3) and that of (2) with (4) is conclusive evidence of superiority of AVK over fixed key.

Realization of time variant key is difficult to achieve, as such must be communicated secretly between the sender and the receiver. In conventional security system , the communication is made either by key transport protocol or by key agreement protocol. In AVK , this is done by the combination of both. The AVK is illustrated in the Table 1 for a session between Alice and Bob whereby they respectively exchange data 452 and 791.The key is now variable and after every transmission it changes dynamically such that :
K_0 = initial secret key
$K_i = K_{i-1}$ XOR D_{i-1} for all i >0 where D_{i-1} and K_{i-1} = data and key in (i-1)th session.
The variable key as suggested if implemented, the repetition of patterns will not result unlike in the normal mode .

Table 1: Illustration of AVK for exchange of data 452 and 791

Session slots	Alice sends	Bob receives	Bob sends	Alice receives	Remarks
1	secret key (say 3)	3	secret key (say 8)	8	For first slot, Alice will use 3 as key and Bob 3 as key for transmitting data
2	Alice sends first data as 4XOR8	Bob gets back original data as (4XOR8XOR8) = 4	Bob sends first data as 7XOR3	Alice gets back original data as (7XOR3 XOR3) = 7	Alice will create new key (8XOR7) for next slot. Bob will create new key (3XOR4)
3	Alice sends next data as 5XOR8 XOR7	Bob gets back original data as (5XOR8XOR 7XOR8XOR7) = 5	Bob sends next data as 9XOR3 XOR4	Alice recovers data as (9XOR3 XOR4XOR3 XOR4) = 9	Alice will create new key (8XOR9) for next slot. Bob
4	Alice sends next data as 2XOR8 XOR9	Bob gets back original data as (2XOR8XOR9 XOR8XOR9) = 2	Bob sends next data as 1XOR3X OR5	Alice recovers data as (1XOR3 XOR5XOR3 XOR5) = 1	

II. SUPERIORITY OF AVK WITH DES OVER CONVENTIONAL DES

Let the message to be encrypted be:
"12345678
simple &
12345678
next one
12345678
last one
12345678"

And the key is
"10aefaca83459cd1"
If we use simple DES in ECB mode[7] then we get the ciphers for the plain text if taken as 8 byte stream (output given as hex and binary values):
# - shows redundancy.

```
Hex format
6AF7A74DFD1468A0  #
C50F231298FA1FE1
6AF7A74DFD1468A0  #
41A7421101DAE834
6AF7A74DFD1468A0  #
2A5E7A2463976824
6AF7A74DFD1468A0  #

Binary format
01101010111101111010011101001101111111010001010001
10100010100000  #
11000101000011110010001100010010100110001111101000
01111111100001
01101010111101111010011101001101111111010001010001
10100010100000  #
01000001101001110100001000010001000000011101101011
10100000110100
01101010111101111010011101001101111111010001010001
10100010100000  #
00101010010111100111101000100100011000111001011101
10100000100100
```

```
0110101011110111101001110100110111111010001010001
10100010100000  #
```

Now if we use the AVK method:

```
Different keys:
Key 1 =10aefaca83459cd1
Key 2 =219CC9FEB673ABE9
Key 3 =52F5A48EDA168BCF
Key 4 =63C797BAEF20BCF7
Key 5 =514EFF62BB4CCF76
Key 6 =607CCC568E7AF84E
Key 7 =0C1DBF22AE15962B
```

Now using these keys for different blocks of the previous plaintext we get the ciphers for the 8 byte blocks as follows:

```
Hex format :
6AF7A74DFD1468A0
6B6B8FEBB5BA0F39
AD3232164A77EFE4
3F2B87169B23A113
A22B32624A412B74
73BBD9A43D27AAF5
268E1EA5FFDB0E4F
```

```
Binary format :
0110101011110111101001110100110111111010001010001
10100010100000
0110101101101011100011111101011101101011011101000
00111100111001
10101101001100100011001000010110010010100111011111
10111111100100
00111111001010111000011100010110100110110010001110
10000100010011
10100010001010110011001001100010010010100100000100
10101101110100
01110011101110111101100110100100001111010010011110
10101011110101
001001101000111000011110101001011111111111101101100
00111001001111
```

Here, we see that the duplicate encrypted text for same plain text is absent. This will ensure better protection against frequency attack.

But in case the plain text message has repetition like the one shown below:

“12345678
 12345678
 12345678
 12345678”

then the XORing of keys will alternatively give back the previous keys:

```
key 1=10aefaca83459cd1
key 2=219CC9FEB673ABE9
key 3=10AEFACA83459CD1
key 4=219CC9FEB673ABE9
```

```
Encrypted text will be:
Hex format :
6AF7A74DFD1468A0
F3DA64485C9DE9BC
6AF7A74DFD1468A0
F3DA64485C9DE9BC
Binary format :
0110101011110111101001110100110111111010001010001
10100010100000
111100111101101001100100010010000010111001001110111
10100110111100
0110101011110111101001110100110111111010001010001
10100010100000
111100111101101001100100010010000010111001001110111
10100110111100
```

This type of repetition may however be sorted by proper formatting, but this remains as one limitation of AVK.

III. TRAPDOOR KNAPSACK PROBLEM IN THE LIGHT OF AVK

A. Conventional Scheme

Merkle and Hellman[8-10] proposed that (i) for a given message in binary row vector, x, and (ii) for a known row vector of n integers, a (the vector , a is known as trap door knapsack vector); the cipher vector, c is generated as

$$c = a \ . \ x$$

The construction of the vector, a, provides the secret trap door. The trap door is the secret key, and the trap door knapsack vector is the public key. Any one can send message, x, by making cipher, c when, a is known. The person knowing the trap door information can only decipher the c in order to receive back, the original message, x. A simple example is due to [69]:

1) Public key, a = (171, 197, 459, 1191, 2410)
2) Secret key or Private key or trap door information = each component of a is larger than the sum of the preceding components
3) Plain text, x = (0, 1, 0, 1, 1)
4) Cipher text, c = 3798 [Encryption: it is obtained as: c = a . x = (171, 197, 459, 1191, 2410) . (0, 1, 0, 1, 1) = 3798]
5) Applying the secret key on c, one can find from trap door knapsack vector, a that x = (0, 1, 0, 1, 1) [Decryption: $x_5 = 1$, as because if it were 0, the sum

of the other elements of a, would become less than 3798; After subtracting the effect of x_5 from c, the process be recursively applied to obtain other elements of x.}

B. Proposed scheme

A proposed solution has been given based on variability in the light of simple XOR operation. Secret formation of
intermediate vector by user.
V_1= (v_1, v_2, v_3, v_4, v_5)
Modified a= (a_1 XOR v_1 , a_2 XOR v_2, …)
Plaintext Modified= -$_x$= (1, 0,1, 0, 0)
Cipher text Modified = C mod i = x (Say)
From next session, the v vector will be changed based on
$V_{2=}$($v_{2,1}$, $v_{2,2}$, $v_{2,3}$, $v_{2,4}$, $v_{2,5}$)
where $v_{2,1}$ = v_1 XOR Cmod
$v_{2,2=}$ v_2 XOR Cmod
and so on.

IV. VERNUM CODE USING AVK

A. Essence of AVK in Vernum Code

Vernum[11] showed that if any plain text is made encrypted by a secret key of equal length, it would be difficult to break the encrypted message provided the key is changed with every session. The secret key is nothing but a random number. This is illustrated in fig 1 . The encryption and the decryption algorithm is bit wise XOR. Both transmitter and receiver can have a prearranged understanding of the secret session key, and hence can use the technique for secure data communication. It operates as below:

1) Assume a secret key(k) of, say n bits
2) Break the message or plain text into block each of n bits. Say the blocks are m_1, m_2, …m_n,
3) Generate encrypted blocks as c_i=m_i⊕k, for i=1 to n. Then transmit the encrypted blocks,
4) Receiver will decrypt the blocks as y_i=c_i⊕k for i=1 to n. Note that y_i=m_i for i=1to n. All the blocks received under deciphering will constitute the plaintext.

The technique illustrated above is known as the one time (as it would require change of key from session to session) secret key(key must be secret and made known to only transmitter and intended receiver) technique. This technique, however, has one major problem. The secret key would be made known only to the two communicating parties and no one else. If a third party somehow gets a copy of the secret key, the very purpose of coding will be defeated. Herein lies the necessity of AVK.

The Vernum Theory is known as the one time (as it would require change of key from session to session) secret key(key must be secret and made known to only transmitter and intended receiver) technique. This technique, however, has one major problem. The secret key would be made known only to the two communicating parties and no one else. If a third party somehow gets a copy of the secret key, the very purpose of coding will be defeated.Shannon proved in his original work of 1949 in connecting cryptography with information theory that if Vernum theory is applied, data will be absolutely secured. It is said that in 1967, Fridel Castro of Cuba used the Vernum technique for defense communication. It is believed that the hot line communication between Moscow-Washington was done via Vernum code. For successful communication under this method, the receiver must be informed of the secret key used by the transmitter, every time a block of message is transmitted. The secret key is usually transmitted over conventional channels like the telephone line.In other words, unconditionally secure algorithm is the one time key algorithm. Vernum code falls in this class. But that has also flaws: an eavesdropper can see the two plain texts by overlying the two cipher texts. Proof is as below when the algorithm is XOR operation:

Basic principle for one time key with C, P and K as cipher text, Plain text and key respectively: C = P ⊕ K; P = C ⊕ K = P ⊕ K ⊕ K

Attacker may reveal:C1 ⊕ C2 = P1 ⊕ K ⊕ P2 ⊕ K = P1 ⊕ P2. Making guess or sense out of two overlying plaintexts may make cryptanalysis possible. Only when key changes from cipher to cipher, the security is unconditional; and exactly that is what is Vernum code.

Plain text of original message	00101101	00011111
Random number or secret key	01010101	01010101
Encrypted message after XOR	01111000	01011010

Fig 1: Illustration of Vernum Code

B. Superiority of Vernum variable key over conventional one-time key pad

Consider P number sessions. Each session takes a time of T seconds for completion on average. Assume key size of N bits. We now apply brute force attacks for getting the session keys.

Under one-time key
The eavesdropper may try on average 2^{N-1} trials over a period of PT seconds. The required time for analysis of a pattern will be (PT / 2^{N-1}) trials.

Under Vernum variable key
The eavesdropper has to try on average 2^{N-1} trials over a period of single session i.e. T seconds. This is because the key will change from session to session. Thus the required time of analysis will be (T / 2^{N-1}) trials.

Hence in case of one-time key the attack is more effective by an order of P. In other words , the Vernum code is more secured over one-time key by an order of P. But if p=1, both are same.

V. APPLICATION OF AVK IN ECB MODE OF DES

A. Scheme

The mathematical model of AVK implemented on ECB mode of DES [7]has been explained below. Assume a message made of M continuous bit stream. It is then divided into different blocks each of size 64 bits. Let the blocks so formed be $P_1, P_2,\ldots, P_n$. The key used will not be the same for all the plain text blocks. Different keys will be generated for the different blocks $P_1, P_2,\ldots, P_n$. For the generation of keys, we assume that for the first plain text block $P_{1,}$ the key will be K_1. The other keys are generated as follows:
$K_2 = K_1$ XOR P_1,$K_3 = K_2$ XOR P_2……………$K_n = K_{n-1}$ XOR P_{n-1}
Thus a key at ith position will be:$K_i = K_{i-1}$ XOR P_{i-1}And therefore $K_i = K_1$ XOR P_1 XOR P_2 XOR … XOR P_{i-2} XOR P_{i-1}
The keys generated are now implemented for DES encryption .Let the cipher texts generated be $C_1, C_2,\ldots, C_n$. The scheme is to XOR every previous key with the previous plaintext message to generate the next key. Firstly only K_1 is available so P_1 will be generated by decrypting the first block and then it is XORed with K_1 to get $K_{2.}$ This K_2 is used to decrypt C_2.In a similar way the keys are generated one by one and the corresponding plain text blocks are obtained one by one .

B. Numerical analysis

Table 2: Illustration of Conventional Vs AVK EBC with XOR encryption/decryption

	Conventional ECB		AVK with ECB		Remark
Blocks of plaintext with same pattern	P_1 = 1011	P_2 =1011	P_1 =1011	P_2 =1011	
Key	1010	1010	1010	0001	First key is XORed with previous plaintext data block to generate key for present block
Cipher text Blocks	0001	0001	0001	1010	As all plain text blocks are available, parallel encryption in both the techniques is possible
	Repetition in cipher block due to same pattern in the plaintext blocks		No repetition of cipher pattern		
Decryption	Parallel encryption for two cipher blocks is possible.		Parallel deciphering not possible, as for deciphering second cipher block, the first plaintext block is to recovered for decryption key generation		

VI. CONCLUSION

This paper confirms the viability of AVK in DES in providing better security that is due to making differential frequency attack inapplicable .This paper also reveals that traditional use of Diffie-Hellman protocol has some limitation. In order to solve the limitation, automatic variability concept has been used such that both key and data are made to vary from session to session thereby increasing security level. Trapdoor Knapsack Problem using AVK and Kerberos using AVK have also been pointed out in the present work . In this paper we have shown several methods of enhancing security level using AVK in case of Vernum Theory, ECB mode of DES and AES . The use of AVK is also advantageous in maintaining security level if any relation occurs during encryption thereby decreasing security level thereby eliminating any scope of occurrence of diffusion or confusion.

REFERENCES

[1] R. Anderson , Security Engineering , John Wiley and Sons, New York 2001

[2] C. T. Bhunia, Data Security, IT, Sept'97, pp.69-70

[3] C T Bhunia, Data Security Techniques, CSI Communication, July'2000, pp11-14

[4] C T Bhunia, Integrated Solution to Security and Accuracy Problems of Data Communication , Indian Journal of Engineers, Calcutta,

[5] H Beker & F Piper, Cipher System: The Protection of Communication, Northwood Booker, London, 1982

[6]C.T. Bhunia , Information Technology Network and Internet , New Age International publication , 2005

[7] C.T.Bhunia et al , Application of Automatic Variable Key in ECB with DES and RSA , Proc.Annual CSI Conference , Tata McGraw Hill , 2004, pp-135-145 , June'1977, PP. 74-84.

[8]W. Diffie and M.E. Hellman ,'Exhaustive Cryptanalysis of the NBS Data encryption standard, Computer, June'1977, pp74-84

[9] W. Diffie and M.E.Hellman , "New Directions in Cryptography", Trans Info Theory, Vol IT 22 , Nov 1976 pp 644-654

[10] R C Merkle & M E Hellman, Hiding Information and Signatures in Trap door Knapsacks, IEEE Trans Info Theory, Vol . IT 24, Sept'1978, PP 525-530

[11] Bruce Schneir , "Applied Cryptography", John Willey & Sons Inc. , New York, 1996