ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 21, August 2017

DATA SECURITY IN TV CHANNELS

N.V. RamanaMurty*,
Dept. of Mathematics,
Andhra Loyola College,
Vijayawada – 520008
raman93in@gmail.com

V. Gopinath, Research Scholar,
Dept. of Mathematics,
Krishna University,
Machilipatnam
gopinath.veeram@gmail.com

B.N. Padmavathi,
Dept. of Mathematics,
Andhra Loyola College,
Vijayawada – 520008
padma9480@gmail.com

ABSTRACT

This paper makes an attempt to study of maintenance of data security in TV channels. Data security plays an important role in relaying their programmes to subscribed customers only. Behind the maintenance of data security, Group theory plays a significant role. Especially, the group $(Z_2,+)$ plays an interesting role. Therefore, in this paper, it has been discussed some important properties of the group Z_2 and their application in data security.

INTRODUCTION

Definition 1: Theset $Z_2 = \{0,1\}$ forms a group under addition modulo 2.

Definition 2: The external direct product of a finite collection of groups $G_1, G_2, \cdots G_n$ is denoted by $G_1 \oplus G_2 \oplus \cdots \oplus G_n$, and is defined as the set of all *n*-tuples for which the *k*-th component is an element of thegroup G_k .

That is, $G_1 \oplus G_2 \oplus \cdots \oplus G_n = \{(g_1, g_2, \cdots, g_n) : g_k \in G_k\}$.

Definition 3: The external direct product $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ of n groups forms a group under the component wise operation. That is, $(g_1, g_2, \cdots, g_n)(g_1', g_2', \cdots, g_n') = (g_1 g_1', g_2 g_2', \cdots, g_n g_n')$, where each product $g_k g_k'$ is performed with operation of the group G_k.

MAIN RESULTS

It is well known that. In computers the information is represented by binary strings formed by 0's and 1's. Therefore, a binary string of length n can be treated as an element of the direct sum $Z_2 \oplus Z_2 \oplus \cdots \oplus Z_2$ (n copies). For example, the binary string 101010 corresponds to the element (1,0,1,0,1,0) in $Z_2 \oplus Z_2 \oplus \cdots \oplus Z_2$ (6 copies). The addition of two binary strings $x_1 x_2 \cdots x_n$ and $y_1 y_2 \cdots y_n$ is defined as component wise modulo 2. For example,100011 + 011010 = 111001 and 100011+100011 = 000000.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 21, August 2017

Lemma 4: The sum of two binary strings is equal to the identity element in $Z_2 \oplus Z_2 \oplus \cdots \oplus Z_2$ (n-copies) if an only if they are identical.

Proof: Easy.

This fact is a basis for data security system used by TV channels. Although many TV channels use binary strings of length more than 64, we will illustrate the method by using the binary strings of length 6.

It is known that owner of a TV channel scrambled its signal. A cable system operator pays a monthly fee for a password to unscramble the signal. Normally, this password is changed every month. Let the password for this month be 'p'. Each Authorized user will be assigned a unique string which is known as 'key'. Let $k_1, k_2, \cdots$ be the keys assigned to distinct authorized users. Now, TV channel transits the password *p*, the scrambled signal, and the encrypted strings $k_1 + p, k_2 + p, \cdots$ to distinct authorized users.

A microprocessor in decoding box adds its key, say k_i to each of the encrypted strings. Thus, it calculates $k_i + (k_1 + p), k_i + (k_2 + p), \cdots$. The *i*-th user decoding box we get a sequence $k_i + (k_i + p)$. This gives $(k_i + k_i) + p = 000000 + p = p,$ by associative property and by Lemma4. Thus, the user gets the unscrambled signal. Since $k_i + (k_j + p) \neq p$ if $k_i \neq k_j$, in case an *i*-th subscriber with key k_i fails to pay the monthly bill, the TV channel owner can terminate the defaulter's service by not transmitting the string $k_i + p$ the next month.

Example 5: Let the password for this month be p = 101011and a subscriber key be k = 001111. Therefore, the TV channel transmits the string $k + p = 001111 + 101011 = 100100.$ Now, decoder box will add its key $k = 001111$ to all the strings received. Therefore, we get 001111+100100 = 101011which is the user's password *p*. Hence, this password permits the decoder to unscramble the signal.

CONCLUSION

Hackers may try to crack the password by simply trying a large number of possible keys. But, it is not easy to do it as TV channels using the strings of length 64 or more. Therefore, there exist 2^{64} possible keys. So, it is not that much easy to crack the password.

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 21, August 2017

REFERENCES

[1] J.A.Gallian, Contemporary Abstract Algebra, Narosa Publishing House, New Delhi, 1999

[2] Rudolf Lidl, Gunter Pilz, Applied Abstract Algebra, Springer, New York, 2004

[3] David S.Dummit, Richard M. Foote, Abstract Algebra, John Wiely& Sons, New York, 2005