Adamawa State University Journal of Scientific Research
Volume 7 Number 1, April, 2019; Article no. ADSUJSR 0701023
ISSN:2705-1900(Online); ISSN: 2251-0702 (Print)
http://www.adsujsr.com

Subgroup Presentations of Symmetric Group in Crypto-Analysis

S. G. Ngulde[1], B. A. Madu[1] and D. Samaila[2]
[1]Department of Mathematical Sciences, University of Maiduguri, Nigeria.
[2]Department of Mathematics, Adamawa State University, Mubi, Nigeria.

Abstract

This paper is aimed at improving the shift cipher by providing more keys which guarantee the security of information being sent across a communication channel. The more radical solution to the problem of key sharing developed by Diffie-Hellman is adopted, merged with group theoretic approach. The result is demonstrated using Romeo and Juliet scenario, where the key exchange was done thrice; single key followed by two different keys, a total of three. Finally, the result was modeled mathematically using group presentations, as set of bijections on finite sets.

Keywords: Finite groups; Symmetry; conjugacy; shift cipher; group presentation; 2010 Mathematics Subject Classification**:** 20B30

Introduction

In ordinary life, the first perception of symmetry is what is called mirror symmetry. Every normal human being have, to a good approximation, mirror symmetry in which the right sight is matched by the left as if a mirror passed along the central axis of the body (Robert, 1990). The roles that govern symmetry are found in the mathematics of group theory, and in the case of symmetry group, an element is the operation needed to produce one object from another. For example, a mirror operation takes an object in one location and produces another of the opposite hand located such that the mirror doing the operation is equidistant between them. These manipulations are called symmetry operations, and are combined by applying them to an object sequentially. An object (regular or irregular) can also be rotated or transposed in different ways to produced different objects, but preserving the structure.

A cipher is a method of making a message unreadable either by rotating or transposing it to look meaningless to the general public. The simplest possible substitution cipher is the *Caesar cipher*, reportedly used by Julius Caesar during the Gallic Wars. Each letter is shifted to a fixed number of places to the right. (Caesar normally used a shift of three places) (Robert, 2002). We regard the alphabet as a cycle, so that the letter following Z is A. There are two procedures for any cipher: these are the encryption procedure and the decryption procedure. In this article, we only focused on the shift cipher because it is symmetrical in nature.

1.1 Preliminaries

Definition 1.1.1: A group G is called cyclic with generator x if every element of G is of the form x^m for some integer m (Rotman, 1999).

Definition 1.1.2: Let G be a group. Two elements x and y of G are said to be conjugate if $x = gyg^{-1}$ for some $g \in G$ (Samaila, Mshelia and Adamu 2010). In other words, if $x,g \in G$, we define the conjugate of x by g or x by g^{-1} to be the element gxg^{-1} or $g^{-1}xg$ respectively.

Definition 1.1.3: A homomorphism $\varphi: G \to K$ from a group G to a group K is a function with the property that $\varphi(g_1 * g_2) = \varphi(g_1) * \varphi(g_2)$ for all $g_1, g_2 \in G$, where $*$ denotes the group operation on G and on K (Hawthorn, 2015).

Definition 1.1.4: An isomorphism $\varphi: G \to K$ between two groups G and K is a homomorphism that is also a bijection mapping G onto K. Two groups G and K are isomorphic if there exists an isomorphism mapping G onto K, written as $G \cong K$. While an automorphism is an isomorphism mapping a group onto itself (Rotman, 1999).

1.2 Symmetric Group

If S is a non-empty set and G = {σ:S→S|σ is a bijection}, then G is called the group of transformations on S (or Symmetric group on S), denoted by S_s. If S is a finite set of order *n*, then G is called a permutation group of degree *n* denoted by S_n (Dixon, 1996). Let S = {a_1, a_2, …, a_n}. For any α∈S_n, let α(a_i) = a_j, $1 \le i, j \le n$. Thus, each α∈S_n may be regarded as a permutation of {a_1, a_2, …, a_n}. This leads to a notion of symmetric cipher.

One of the symmetric ciphers is the shift cipher in which the encryption procedure consists of shifting the letters in a message by a fixed number of spots in the alphabetical order. This fixed number which is a positive integer is called the key, k, which is also the permutation applied to the positions of the letters (Michal, 2006). This paper aimed at making message more secure by splitting the 26 English alphabets into two subsequences (see Table 1) of prime order in the ratio $G_1:G_2$ = 13:13. In this case, we have to assign two different keys k_1 and k_2 for the corresponding subsequences.

With a little twist of the alphabets (through $\frac{2\pi}{13}$ radian), the following table is obtained.

Table 1: The two Subsequences of the 26 Alphabets

G_1	A	C	E	G	I	K	M	O	Q	S	U	W	Y	A
G_2	B	D	F	H	J	L	N	P	R	T	V	X	Z	B

Note that the encryption and decryption procedures are essentially the same. Hence, the named *Symmetric Cipher* (Douglas, 2002).

Materials and Methods

Let G be a cyclic group with a generator *g* and let *q* be an arbitrary element of G. Then there exists an integer *n* such that $g^n = q$. As discussed by Simon, 2018, if the Discrete Logarithmic Problem (DLP) is easy then so is the Diffie– Hellman Problem (DHP). This in turn means that the Diffie– Hellman key agreement protocol is insecure. This paper aimed at finding difficult instances of the DLP in order to make it more secure. It is observed that difficulty of the DLP depends heavily on the representations of the group rather than its isomorphism class.

We discussed in this paper some ways in which group theory is used to construct variants of the Diffie–Hellman key agreement protocol. Since the protocol uses cyclic subgroups of finite groups, the approach in this paper is to use groups (not necessarily Abelian) that can be efficiently represented and manipulated, and possesses cyclic subgroups.

Results

Group Theoretic Approach

Let G be a non-abelian group and *g*, *h* ∈ G. Then the conjugation of *g* by *h* is given by

$$g^h = h^{-1}gh.$$

This means that conjugation can be used in cryptography instead of exponentiation (Samaila, 2013). Now, with *g*, *h* ∈ G, let $g = h^x$ for some element *x* of G. Again with *g*, *h* ∈ G, find an element *y* ∈ G such that $g = h^y$. This leads to a problem called Conjugacy Search Problem (CSP), which provides the basic foundation of the encryption-decryption analysis used in this paper.

The other way of using conjugation in place of exponentiation in the Diffie–Hellman Protocol is as follows. Define a homomorphism $\varphi : G \to G$ by $g^{\varphi(x)} = \varphi^{-1}(x)gx$ for all $g \in G$ and Let H and M be cyclic subgroups of G. Then for all $h \in H$ and $m \in M$, $[h, m] = 1$, since $H \neq M$.

Now, if Romeo and Juliet wish to create a common secrete key, they can proceed as follows:

- Romeo randomly selects an element $h \in H$, computes $g^{\varphi(h)} = \varphi^{-1}(h)gh,$ and sends it to Juliet.
- Juliet randomly selects an element $m \in M$, computes $g^{\varphi(m)} = \varphi^{-1}(m)gm,$ and sends it to Romeo.
- Romeo then computes $K_h = (g^{\varphi(m)})^{\varphi(h)}$, while Juliet computes $K_m = (g^{\varphi(h)})^{\varphi(m)}$.

But H and M are cyclic subgroups of G, hence, Abelian so that $\varphi(m)\varphi(h) = \varphi(h)\varphi(m).$ This in

turn, means that $K_h = K_m$ as group elements whose representations might be different. This idea can be used for many groups to compute a secret key especially if G has an efficient algorithm to compute a normal form for its elements. The secret key K is then the normal form of K_h and K_m.

Symmetric Cipher

One of the symmetric ciphers is known to be the shift cipher where the encryption procedure consists of shifting the letters in a message by a fixed number of spots (also known as permutation) in some alphabetical order. This fixed number is called the key, K, called the permutation applied on the letters (Michal, 2006 and Samaila, 2013). To achieved the aim of making a message more secured, the English alphabets is split into two subsequences (see table 1) in the ratio G_1:G_2 = 13:13. This is claimed to be more secured since there are 13!×13! possible arrangements and the concept requires two different keys K_1 and K_2 for the corresponding subsequences. For example, let K_1 = 3 and K_2 = 7 for the subsequences G_1 and G_2 respectively (Table 1).

Then with these values, the message
CUT YOUR COAT ACCORDING TO YOUR SIZE
is encrypted as:
IAH EUAF IUGH GIIUFROBM HU EUAF YONK
On the other hand, if an encrypted message is received such as:
HVK PUE OY FABBOBM VUSK
then using the keys provided for each subsequence in a reverse form (as an inverse function), the message is decrypted as follows:
THE BOY IS RUNNING HOME.

This shows that the encryption and decryption procedures have the same pattern as inverse of each other (regarded as elements of a cyclic group).

Public Key Exchange

One of the major problems of the symmetric cipher is the privacy of the key. Changing the key often is an efficient idea and how to accomplish an exchange of a new key if the present key has been broken is another task. This is precisely what the idea of a public key exchange of Diffie-Hellman is all about (Rivest, 1978). Let p be a prime number and g be a primitive root modulo p. In practice, p has to be large but in this paper, let p = 13 and g = 2.

Then Romeo and Juliet would perform a secure key exchange over an unsecure channel as follows:

- Romeo selects a *secret* number m, say m = 23 and calculate

$X = 2^m \pmod{13}$; $2^{23} \equiv 7 \pmod{13}$.

He sends X = 7 to Juliet over an unsecure channel.

- Juliet selects a *secret* number n, say n = 31 and calculate

$Y = 2^n \pmod{13}$; $2^{31} \equiv 11 \pmod{13}$.

She sends Y = 11 to Romeo over an unsecure channel.

- Romeo receives the number Y from Juliet and calculates the key modulo 13

$K = Y^m \equiv 6 \pmod{13}$

- Juliet receives the number X from Romeo and calculates the key modulo 13

$K = X^n \equiv 6 \pmod{13}$.

The key K is the same for Romeo and Juliet since $(2^m)^n = (2^n)^m \pmod{13}$. With the key at hand, the two friends can now exchange message safely. A simple example is given below as follows:
Romeo's message reads
YOU ARE THE LOVE OF MY LIFE, …
encrypted as
KAG MDQ FTQ XAHQ AR YK XURQ, …
with the key K = 6. Juliet then receives the encrypted message together with the number X = 7, which she used to calculate the key K = 6.

Again, for the message to be more secured, Romeo decided to use two different keys K_1 and K_2 for G_1 and G_2 respectively to encrypt the rest of the message. The procedures being the same as above. The rest of the message reads
I WANT TO MARRY YOU,
which is now encrypted as
S GKBH HY WKFFI IYE.

Hence, Juliet receives the complete message from Romeo as:
KAG MDQ FTQ XAHQ AR YK XURQ, S GKBH HY WKFFI IYE.
With the calculated keys K, K_1 and K_2, Juliet then decrypt the message as
YOU ARE THE LOVE OF MY LIFE, I WANT TO MARRY YOU.

Mathematical Model

Let G be a group acting on a non-empty set X and let δ be a representation of G. Then the set of all symmetry operations considered on the elements of X can be modeled as an action δ:G×X → X such that $\delta(g, x) = g \cdot x$ for all g∈G and x∈X. The operations g for which $g \cdot x = x$ formed the symmetric group of x, a subgroup of G. And if for some g, $g \cdot x = y$ then x and y are said to be symmetrical (Derek *et al*, 2005). If G is a group such that each g∈G is a bijection, then g:X→X acts on the set of functions h:X→V by $(gh)(x)=h(g^{-1}(x))$. This implies that a group of bijections of space induces the group action of "objects" in it.

Now, from the two subsequences in table 1 above, the following bijections describe the encryption and decryption procedures of a symmetric cipher with respect to the assigned keys $i = K_1$ and $j = K_2$.

$$\varphi : G_1 \to G_1 \text{ by } \varphi(g_n^1) = g_{(n\pm i) \bmod 13}^1;\ g_0^1 = g_{13}^1,\ 1 \le n \le 13, \quad 1$$

$$\rho : G_2 \to G_2 \text{ by } \rho(g_n^2) = g_{(n\pm j) \bmod 13}^2;\ g_0^1 = g_{13}^1,\ 1 \le n \le 13, \quad 2$$

for all g^1∈G_1 and g^2∈G_2.

Note that in this case, the representations φ and ρ are both isomorphism and the collection of all such bijections formed a group with respect to the operation of function composition.

Conclusion

The role of symmetry in cryptography cannot be under estimated, specifically in shift cipher. The shift cipher behaves like cyclic group with the property that if g and q are elements of a cyclic group G, then there exists an integer n such that $g^n = q$. This paper analyzed some difficult instances of finding such integer n = K, called the key in order to make the cipher text more secure. It also presents a method in which group theory is used to construct variants of the Diffie–Hellman key agreement protocol and finally, conclude on some mathematical model for symmetric cipher using group presentations.

It is therefore recommended that such techniques should be tested on any group G of prime order, whose only subgroups are the whole of G and the trivial subgroup {e}, where e is the identity element of G.

References

Robert B. V. (1990), Crystal Symmetry Groups; *Los Alamos Science Summer*, Los Alamos, 152-157.

Robert C. (2002), Codes and Ciphers; Julius Caesar, the Enigma and the Internet, Cambridge University Press, Cambridge.

Samaila D., I.B. Mshelia and M.S. Adamu (2010), A derived model for the construction of double dihedral groups Q_{2N} and their properties, *JOLORN*, 11(2), 115-123

Hawthorn I., Yue G. (2015), Arbitrary Functions in Group Theory, New Zealand Journal of Mathematics, v.45, 1 – 9.

Rotman J. J. (1999), An Introduction to the Theory of Groups, (4th ed.), New York: Springer.

Dixon J. D. and Mortimer B. (1996), Permutation groups, Graduate Texts in Mathematics, Springer-Verlag, Berlin, New York.

Michal S. (2006), New Results in Group Theoretic Cryptology. Ph.D. Thesis, Florida Atlantic University, Boca Raton.

Douglas R. S. (2002), Cryptography; Theory and Practice, 2nd ed, CRC Press, New York, NY.

Simon R. Blackburn, Carlos Cid and Ciaran Mullan (2018); Group theory in Cryptography, Egham, Surrey TW20 0EX, United Kingdom

Samaila D., Ibrahim B. A. and Pius M. P. (2013), On the Conjugacy Classes, Centers and Representation of the Groups S_n and D_n, Int. J. Pure Appl. Sci. Technol., 15(1), pp. 87-95.

Samaila D. and Pius P. M. (2013), Secrete Sharing Scheme Using Transpositions in Symmetric Group, *International Journal of Pure and Applied Sciences and Technology*, 14(1), pp. 27-32, ISSN 2229-6107

Rivest R., Shamir A. and Adleman L. (1978), A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Comm. ACM*, 21, 120-126.

Derekt H., Bettina E. and Eamonn A. O. (2005), Handbook of computational group theory, Chapman & Hall/CRC Press, Boca Raton.