Annals of Mathematics and Computer Science
ISSN: 2789-7206
Vol 13 (2023) 53-59

HOLOMORPHS OF GROUPS AND THEIR USE IN THE DIFFIE-HELLMAN KEY-EXCHANGE PROTOCOL

NACER GHADBANE[1*]

Abstract. The holomorph of the group G, usually denoted by $Hol(G)$, is the natural semidirect product $Aut(G)\,G$ of G by its automorphism group $Aut(G)$. Let $\lambda : G \longrightarrow S(G), g \longmapsto f_g : (x \longmapsto gx)$ the left regular representation of G. In this paper we will show that the group $Hol(G)$ is isomorphic to the group $\lambda(G)\,Aut(G)$. Also, we describe the public key exchange in the group $\lambda(G)\,Aut(G)$.

1. INTRODUCTION

The creation of public key cryptography by Diffie and Hellman in 1976 and the subsequent invention of the RSA public key cryptosystem by Rivest, Shamir and Adleman in 1978 are watershed events in the long history of secret communications. Public key cryptography draws on many areas of mathematics, including number theory, abstract algebra, and information theory [13], [15].
A number of public-key cryptosystems based on combinatorial group theory have been proposed since the early 1980s. The first proposal to use nonabelian groups in public key cryptography is due to Wagner and Magyarik in 1985. The cryptosystem is based on the hardness of the word problem for finitely presented monoids. The importance of Wagner and Magyarik's scheme lies in its novelty, which commenced an interplay between cryptography and combinatorial group theory.
In 1993, Sidelnikov et al. Proposed a new idea that infinite non-abelian group and semigroup can be used in public key cryptography [18]. In 2013, Habeeb et al. Proposed a new kind of key exchange protocol which was the first time that a semidirect product of groups was applied to the cryptosystem [14].

A secure public key cryptosystem requires a mathematical operation which is easy to compute (encryption) but computationally difficult to reverse (decreption) in a realistic time without knowing a special secret information, called the trapdoor, which is the private key.

Date: Received: Feb 19, 2023; Accepted: Mar 24, 2023.

* Corresponding author.

2010 *Mathematics Subject Classification.* Primary .

Key words and phrases. Group of automorphisms, semidirect products of groups, public key exchange.

The remainder of this paper is organized as follows: mathematical preliminaries are introduced in Section 2 that are needed in the proposed protocol. The main results of this paper and a key exchange protocol besed on holomorph of a group are proposed in Section 3. We draw our conclusions in Section 4.

2. PRELIMINARIES

A group G is an ordered pair $(G,\cdot)$ consisting of a non-empty set G together with a binary operation " $\cdot$ " defined on G suth that:

(i) If x,y and z in G, then $(xy)\,z = x\,(yz)$;

(ii) There exists an element 1_G in G such that,

for all $x \in G$, $1_G x = x 1_G = x$;

(iii) For each x in G, there exists x^{-1} in G such that $x^{-1}x = xx^{-1} = 1_G$.

A subset H of a group G is a subgroup of G, if and only if $H \neq \emptyset$ and for all x,y in H, xy in H and x^{-1} in H. The subgroup H of a group G is denoted by $H \leq G$. [17] , [19].

Given two subgroups H and F of a group G, $HF = \{hf : h \in H \text{ and } f \in F\}$ may not be a subgroup of G. Hence HF is a subgroup of G if and only if, $HF = FH$. We recall that two subgroups $H, F \leq G$ are called complementary (to eath other) if $H \cap F = \{1_G\}$, and $HF = G$. We also note that if $H, F \leq G$ are complementary then each element g of G can be written uniquely in the form $g = hf$ where $h \in H, f \in F$.

A group homomorphism is a well-defined map $\varphi : G \longrightarrow H$ between two groups G and H which preserves the multiplicative structure. In other words, $\varphi(xy) = \varphi(x)\,\varphi(y)$ for all $x, y \in G$. A bijective homomorphisme is called an isomorphism. When there is an isomorphism between two groups G and H, we say G and H are isomorphic and we write $G \cong H$.

An automorphism of a group G is an isomorphism from G to G. We write the image of g under the automorphism φ as g^{φ} and multiply automorphisms by defining $g^{\alpha\beta} = (g^{\alpha})^{\beta}$. Under this operation the set of all automorphisms of G forms a group $Aut(G)$ [10] , [16].

Let $S(G)$ be the group of permutations on the set G. Consider the right and the left regular representations of G:

$$\begin{cases} \rho : G \longrightarrow S(G) \\ g \longmapsto (x \longmapsto xg) \end{cases} \quad \begin{cases} \lambda : G \longrightarrow S(G) \\ g \longmapsto (x \longmapsto gx)\,. \end{cases}$$

Let H, Q be two, and let $\theta : H \longrightarrow Aut(Q)$ be a homomorphism. Denote $\theta(h)$ by θ_h. Then the semidirect product of H and Q is the set

$\Gamma = H \rtimes_{\theta} Q = \{(h,q)\,, h \in H, q \in Q\}$ where the group operation is given by

$(h,q)\,(h',q') = (hh', q\theta_h(q'))$ [2] , [4] , [14].

The holomorph of G, usually denoted by $Hol(G)$, is the set of all pairs (g,f), where $g \in G, f \in Aut(G)$, with the group operation given by:

$(g,f)\,(g',f') = (f'(g)\,g', ff')$ [1] .

Public key cryptography (or asymmetric cryptography) has been the most significant and striking development in the history of cryptography. This revolutionary concept has been introduced in the famous paper "New Directions in

Cryptography" [18]. Public Key cryptography, was invented by Diffie And Hellman more than forty years ago. In Public Key cryptography, a user U has a pair of related keys (pK, sK): the key pK is public and should be available to everyone, while the key sK must be kept secret by U. The fact that sK is kept secret by a single entity creates an asymmetry, hence the name asymmetric cryptography.

A function f is one-way if it is computationally easy to compute the function $f(x) = y$, but computationally infeasible to invert the function $f^{-1}(y) = x$.

The Diffie-Hellman key exchange (DHKE), proposed by Whitfield Diffie and Martin Hellman in 1976. The DHKE is a very impressive application of the discrete logarithm problem. A more general descriptions of the protocol uses an arbitrary finite cyclic group. We now recall this protocol as following:

1. Alice and Bob agree on a finite cyclic group G and a generating element g in G.
2. Alice picks a random natural number a and sends g^a to Bob.
3. Bob picks a random natural number b and sends g^b to Alice.
4. Alice computes $K_A = \left(g^b\right)^a = g^{ba}$.
5. Bob computes $K_B = (g^a)^b = g^{ab}$.

Since $ab = ba$, both Alice and Bob are now in possession of the same group element $K = K_A = K_B$ which can serve as the shared secret key [7].

3. MAIN RESULTS

3.1. **The holomorph of the group.** In this section, we present some notes on the holomorph of the group.

Proposition 3.1.
Let G be a group and let $\begin{cases} \lambda : G \longrightarrow S(G) \\ g \longmapsto f_g : (x \longmapsto gx). \end{cases}$ *the left regular representation of G. Consider the set $\lambda(G) = \{f_g : g \in G\}$.*
Then the followings hold:
(i) for all $\psi \in Aut(G)$ and $f_g \in \lambda(G)$; $\psi f_g \psi^{-1} = f_{\psi(g)}$.
(ii) $Aut(G) \cap \lambda(G) = \{id_G\}$.
(iii) each element of $\lambda(G)\, Aut(G)$ can be written uniquely in the form $f_g\psi$ where $f_g \in \lambda(G), \psi \in Aut(G)$, i.e, of for all $\psi, \varphi \in Aut(G)$ and $f_g, f_h \in \lambda(G)$; $f_g\psi = f_h\varphi \Longrightarrow f_g = f_h$ and $\psi = \varphi$.

Proof. Let $\psi \in Aut(G)$ and $f_g \in \lambda(G)$. For each $x \in G$,
$\psi f_g \psi^{-1}(x) = \psi f_g(\psi^{-1}(x)) = \psi(f_g(\psi^{-1}(x))) = \psi(g\psi^{-1}(x))$
$= \psi(g)\,\psi(\psi^{-1}(x)) = \psi(g)\,x = f_{\psi(g)}(x)$. Then $\psi f_g \psi^{-1} = f_{\psi(g)}$ which completes the proof of (i). If $\varphi \in Aut(G) \cap \lambda(G)$, then there exists an element g in G such that $\varphi = f_g$. Since $f_g \in \lambda(G)$ then we have for all $x, x' \in G, \varphi(xx') = gxx'$. Also, since $\varphi \in Aut(G)$, then we have for all $x, x' \in G, \varphi(xx') = \varphi(x)\,\varphi(x') = gxgx'$. Therefore $gxx' = gxgx'$, implies $g = 1_G$ and $\varphi = f_g = id_G$. So the proof of (ii) is completed.
For (iii), we only need the uniqueness. But $f_g\psi = f_h\varphi$ implies $f_h^{-1} f_g = \varphi\psi^{-1}$. This is in $Aut(G) \cap \lambda(G)$. Since $Aut(G) \cap \lambda(G) = \{id_G\}$, so
$f_h^{-1} f_g = \varphi\psi^{-1} = id_G$. Then $\varphi = \psi$ and $f_h = f_g$. □

Proposition 3.2.
Let G be a group. Consider the set $\lambda(G)\,Aut(G) = \{f_g\psi : f_g \in \lambda(G), \psi \in Aut(G)\}$. Define an operation " $*$ " on $\lambda(G)\,Aut(G)$ by $f_g\psi * f_h\varphi = f_{g\psi(h)}\psi\varphi$. Then the followings hold:
(i) $(\lambda(G)\,Aut(G), *)$ is a group.
(ii) the mapping $\delta : (\lambda(G)\,Aut(G), *) \longrightarrow (Hol(G), \cdot), f_g\psi \longmapsto (g, \psi)$ is an isomorphism of groups.

Proof. Let $f_g\psi, f_h\varphi \in \lambda(G)\,Aut(G)$, since $f_{g\psi(h)} \in \lambda(G)$ and $\psi\varphi \in Aut(G)$ then $f_{g\psi(h)}\psi\varphi \in \lambda(G)\,Aut(G)$. Moreover the set $\lambda(G)\,Aut(G)$ is closed under the operation " $*$ ". By considering elements $f_g\psi, f_h\varphi$ and $f_k\zeta$ of $\lambda(G)\,Aut(G)$ we have
$(f_g\psi * f_h\varphi) * f_k\zeta = f_{g\psi(h)}(\psi\varphi) * f_k\zeta = f_{g\psi(h)(\psi\varphi)(k)}(\psi\varphi)\zeta$.
Also, we get
$f_g\psi * (f_h\varphi * f_k\zeta) = f_g\psi * f_{h\varphi(k)}(\varphi\zeta) = f_{g\psi(h\varphi(k))}\psi(\varphi\zeta) = f_{g\psi(h)(\psi\varphi)(k)}(\psi\varphi)\zeta$.
This shows that the operation " $*$ " is associative. If $f_g\psi \in \lambda(G)\,Aut(G)$ then
$f_g\psi * f_{1_G}id_G = f_g\psi * id_G id_G = id_G id_G * f_g\psi = f_g\psi$,
so, the identity element for $(\lambda(G)\,Aut(G), *)$ is $id_G id_G$. For the elements $f_g\psi$ and $f_{\psi^{-1}(g^{-1})}\psi^{-1}$ of $\lambda(G)\,Aut(G)$ we have
$f_g\psi * f_{\psi^{-1}(g^{-1})}\psi^{-1} = f_{\psi^{-1}(g^{-1})}\psi^{-1} * f_g\psi = id_G id_G$,
which show that $f_{\psi^{-1}(g^{-1})}\psi^{-1}$ is an inverse of $f_g\psi$ in the group $(\lambda(G)\,Aut(G), *)$. So the proof of (i) is comleted. For (ii), it is easy to see that the mapping δ is onto. Since each element of $\lambda(G)\,Aut(G)$ can be written uniquely in the form $f_g\psi$ where $f_g \in \lambda(G), \psi \in Aut(G)$ (See Proposition 1), then δ is one-to-one. Also for all $f_g\psi, f_h\varphi \in \lambda(G)\,Aut(G)$:
$\delta(f_g\psi * f_h\varphi) = \delta\left(f_{g\psi(h)}\psi\varphi\right) = (g\psi(h), \psi\varphi)$
$= (g, \psi)\cdot(h, \varphi) = \delta(f_g\psi)\cdot\delta(f_h\varphi)$. □

3.2. **On public key exchange using the group $(\lambda(G)\,Aut(G), *)$.** In this section, we present the public key exchange using the group $(\lambda(G)\,Aut(G), *)$. Let G be a groupe, consider the group $(\lambda(G)\,Aut(G), *)$. In our key exchange protocol, $G, Aut(G), f_g\psi \in \lambda(G)\,Aut(G)$ are public information.
Bob chooses a private $n \in \mathbb{N}$, while Alice chooses a private $m \in \mathbb{N}$. Both Alice and Bob are going to work with elements of the form $f_g\psi^r$, where $f_g \in \lambda(G), \psi \in Aut(G), r \in \mathbb{N}$. Note that two elements of this form are multiplied as follows:
$f_g\psi^r * f_h\psi^s = f_{\psi^s(g)h}\psi^{r+s}$

Proposition 3.3.
*1. **Alice:** Alice computes $(f_g\psi)^m$, where $(f_g\psi)^0 = 1_K$, and for all $m \geq 0, (f_g\psi)^{m+1} = f_g\psi * (f_g\psi)^m$.*
Then $(f_g\psi)^m = f_{\psi^{m-1}(g)\ldots\psi^2(g)\psi^1(g)g}\psi^m \in \lambda(G)\,Aut(G)$.
and sends to Bob the element $a = f_{\psi^{m-1}(g)\ldots\psi^2(g)\psi^1(g)g}$ of the group $\lambda(G)$.
*2. **Bob:** Bob computes $(f_g\psi)^n$, where $(f_g\psi)^0 = 1_K$, and for all $n \geq 0, (f_g\psi)^{n+1} = f_g\psi * (f_g\psi)^n$.*
Then $(f_g\psi)^n = f_{\psi^{n-1}(g)\ldots\psi^2(g)\psi^1(g)g}\psi^n \in \lambda(G)\,Aut(G)$.
and sends to Alice the element $b = f_{\psi^{n-1}(g)\ldots\psi^2(g)\psi^1(g)g}$ of the group $\lambda(G)$.

3. ***Alice:*** *let* $x \in Aut(G)$. *Alice computes* $bx * a\psi^m = f_{\psi^{n-1}(g)...\psi^2(g)\psi^1(g)g}x * f_{\psi^{m-1}(g)...\psi^2(g)\psi^1(g)g}\psi^m$
$= f_{\psi^m(\psi^{n-1}(g)...\psi^2(g)\psi^1(g)g)\psi^{m-1}(g)...\psi^2(g)\psi^1(g)g}x\psi^m$.
Her key is now $K_A = f_{\psi^m(\psi^{n-1}(g)...\psi^2(g)\psi^1(g)g)\psi^{m-1}(g)...\psi^2(g)\psi^1(g)g}$
4. ***Bob:*** *let* $y \in Aut(G)$. *Bob computes* $ay * b\psi^n = f_{\psi^{m-1}(g)...\psi^2(g)\psi^1(g)g}y * f_{\psi^{n-1}(g)...\psi^2(g)\psi^1(g)g}\psi^n$
$= f_{\psi^n(\psi^{m-1}(g)...\psi^2(g)\psi^1(g)g)\psi^{n-1}(g)...\psi^2(g)\psi^1(g)g}y\psi^n$.
His key is now $K_B = f_{\psi^n(\psi^{m-1}(g)...\psi^2(g)\psi^1(g)g)\psi^{n-1}(g)...\psi^2(g)\psi^1(g)g}$.
We have $K_A = K_B = K$, *the shared secret key.*

Proof. We have
$K_A = f_{\psi^m(\psi^{n-1}(g)...\psi^2(g)\psi^1(g)g)\psi^{m-1}(g)...\psi^2(g)\psi^1(g)g}$
$= f_{\psi^{m+n-1}(g)...\psi^{m+2}(g)\psi^{m+1}(g)\psi^m(g)\psi^{m-1}(g)...\psi^2(g)\psi^1(g)g}$
$= (f_g\psi)^{m+n}(\psi^{m+n})^{-1}$, where $(\psi^{m+n})^{-1}$ is the inverse of the element ψ^{m+n} in $Aut(G)$.
And $K_B = f_{\psi^n(\psi^{m-1}(g)...\psi^2(g)\psi^1(g)g)\psi^{n-1}(g)...\psi^2(g)\psi^1(g)g}$
$= f_{\psi^{n+m-1}(g)...\psi^{n+2}(g)\psi^{n+1}(g)\psi^n(g)\psi^{n-1}(g)...\psi^2(g)\psi^1(g)g}$
$= (f_g\psi)^{n+m}(\psi^{n+m})^{-1}$, where $(\psi^{n+m})^{-1}$ is the inverse of the element ψ^{n+m} in $Aut(G)$. Then $K_A = K_B = K$

□

Security of this protocol
The security of this protocol relies on the difficulty of recovering the element of the group $\lambda(G)$.

Proposition 3.4.
Let H, Q *be two groupes. In our key exchange protocol,* $H, Q, Aut(Q), (h,q) \in H \times Q$, *and* $n \in \mathbb{N}$ *are public information.*
Bob: *Bobe begins by choosing an embedding* $\theta : H \longrightarrow Aut(Q)$, *which he keeps secret. He then computes*
$X = (h,q)^n$, *where* $(h,q)^0 = 1_{H\rtimes_\theta Q}$, *and for all* $n \geq 0, (h,q)^{n+1} = (h,q)^n(h,q)$.
Then $X = (h,q)^n$
$= (h^n, q\theta_h(q)\,\theta_{h^2}(q)...\theta_{h^{n-1}}(q)) \in H \rtimes_\theta Q$.
Bob then sends X *to Alice.*
Alice: *Alice begins by choosing an embedding* $\mu : H \longrightarrow Aut(Q)$, *which he keeps secret. He then computes*
$Y = (h,q)^n$, *where* $(h,q)^0 = 1_{H\rtimes_\mu Q}$, *and for all* $n \geq 0, (h,q)^{n+1} = (h,q)^n(h,q)$.
Then $Y = (h,q)^n = (h^n, q\mu_h(q)\,\mu_{h^2}(q)...\mu_{h^{n-1}}(q)) \in H \rtimes_\mu Q$.
Alice then sends Y *to Bob.*
Bob: *by multiplying the second coordinate of* Y *by* q^{-1}, *Bob can find the element* $\mu_h(q)\,\mu_{h^2}(q)...\mu_{h^{n-1}}(q) \in Q$.
Alice: *by multiplying the second coordinate of* X *by* q^{-1}, *Alice can find the element*
$\theta_h(q)\,\theta_{h^2}(q)...\theta_{h^{n-1}}(q) \in Q$.
Bob: *Bobe can now compute*
$\prod_{i=1}^{n-1}\theta_{h^i}(\mu_h(q)\,\mu_{h^2}(q)...\mu_{h^{n-1}}(q))$

$$= \prod_{i=1}^{n-1} \theta_h^i \left(\mu_h(q)\, \mu_h^2(q) ... \mu_h^{n-1}(q)\right)$$
$$= \prod_{i=1}^{n-1} \left(\theta_h^i \circ \mu_h\right)(q) \left(\theta_h^i \circ \mu_h^2\right)(q) ... \left(\theta_h^i \circ \mu_h^{n-1}\right)(q).$$

Alice: *similarly, Alice can compute*

$$\prod_{i=1}^{n-1} \mu_{h^i}\left(\theta_h(q)\, \theta_{h^2}(q) ... \theta_{h^{n-1}}(q)\right)$$
$$= \prod_{i=1}^{n-1} \mu_h^i \left(\theta_h(q)\, \theta_h^2(q) ... \theta_h^{n-1}(q)\right)$$
$$= \prod_{i=1}^{n-1} \left(\mu_h^i \circ \theta_h\right)(q) \left(\mu_h^i \circ \theta_h^2\right)(q) ... \left(\mu_h^i \circ \theta_h^{n-1}\right)(q).$$

If in addition to Q being abelian, we require that for all h in H, θ_h and μ_h commute in $Aut(Q)$, then we have the following equality:

$$k = \prod_{i=1}^{n-1} \left(\theta_h^i \circ \mu_h\right)(q) \left(\theta_h^i \circ \mu_h^2\right)(q) ... \left(\theta_h^i \circ \mu_h^{n-1}\right)(q)$$
$$= \prod_{i=1}^{n-1} \left(\mu_h^i \circ \theta_h\right)(q) \left(\mu_h^i \circ \theta_h^2\right)(q) ... \left(\mu_h^i \circ \theta_h^{n-1}\right)(q).$$

The element k is computable by both Bob and Alice as shown above, giving them a shared key.

Proof. We have

$$\prod_{i=1}^{n-1} \theta_{h^i}\left(\mu_h(q)\, \mu_{h^2}(q) ... \mu_{h^{n-1}}(q)\right)$$
$$= \prod_{i=1}^{n-1} \theta_h^i \left(\mu_h(q)\, \mu_h^2(q) ... \mu_h^{n-1}(q)\right)$$
$$= \prod_{i=1}^{n-1} \left(\theta_h^i \mu_h\right)(q) \left(\theta_h^i \mu_h^2\right)(q) ... \left(\theta_h^i \mu_h^{n-1}\right)(q).$$

And

$$\prod_{i=1}^{n-1} \mu_{h^i}\left(\theta_h(q)\, \theta_{h^2}(q) ... \theta_{h^{n-1}}(q)\right)$$
$$= \prod_{i=1}^{n-1} \mu_h^i \left(\theta_h(q)\, \theta_h^2(q) ... \theta_h^{n-1}(q)\right)$$
$$= \prod_{i=1}^{n-1} \left(\mu_h^i \theta_h\right)(q) \left(\mu_h^i \theta_h^2\right)(q) ... \left(\mu_h^i \theta_h^{n-1}\right)(q).$$

As θ_h and μ_h commute in $Aut(Q)$, then

$$\prod_{i=1}^{n-1} \theta_{h^i}\left(\mu_h(q)\, \mu_{h^2}(q) ... \mu_{h^{n-1}}(q)\right)$$
$$= \prod_{i=1}^{n-1} \mu_{h^i}\left(\theta_h(q)\, \theta_{h^2}(q) ... \theta_{h^{n-1}}(q)\right) = k$$

□

Security of this protocol

The security of this protocol relies on the difficulty of recovering the homomorphisms θ and μ from $(h, q) \in H \times Q, X$ and Y.

4. Conclusion

In this work, we present some notes on the group $(\lambda(G)\, Aut(G), *)$. Also we construct the public key exchange in this group.

References

1. A. Caranti and F. Dalla Volta, "Groups that have the same holomorph of a finite perfect group", Journal of Algebra, Vol. 507, N^o 1, pp. 81-102, (2018).
2. A. E. Nagy and C. L. Nehaniv, "*Cascade Product of Permutation Groups*", Centre for computer science and informatics, U. K and Centre for research in mathematics, Australia, 2013.
3. A. H. Clifford and G. B. Preston, "The Algebraic Theory of Semigroups", American Mathematical Society, 1977.
4. A. M. S, "*Wreath Product of Permutation Group*", A Research Oriented Course In Arithmetics of Elliptic Curves, Groups and Loops, Lecture Notes Series, National Mathematical Centre, Abuja, 2001.
5. B. Baumslag and B. Chandler, "*Theory and Problems of Group Theory*", New York University, 1968.
6. C. Meshram andX. Li , "New efficient key authentication protocol for public key cryptosystem using DL over multiplicative group", Journal of Information and Optimization Sciences, Vol, 39, No.2, pp. 391-400, (2018).
7. C. Paar, J. Pelzl, "Understanding Cryptography", Springer, (2010).
8. C. Tsang, "On the multiple holomorph of a finite almost simple group", New York Journal of Mathematics, Vol. 25, N^o 1, pp. 949-963, (2019).
9. D. Guin et T. Hausberger, "*Algèbre Tome 1 Groupes, Corps et Théorie de Galois*", EDP Sciences, 2008.
10. D. L. Kreher. "*Group Theory Notes"*, Univ of Nebraska, Lincoln, 2012.
11. I. A. A and A. M. S, "*On Wreath Product of Permutation Groups*", Proyecciones, Vol. 26, N^o 1, pp. 73-90, (2007).
12. J. D. P. Meldrum, "*Wreath products of groups and semigroups*", Longman, 1995.
13. J. Hoffstein, J. Pipher, J. H. Silverman, "An Introduction to Mathematical Cryptography, Springer, (2014).
14. M. Habeeb, D. Kahrobaei, C. Koupparis and V. Shpilrain, "Public key exchange using semidirect product of semigroups, Applied Cryptography and Network Security, 11th International Conference, ACNS 2013, Canada, PP. 475-486, (2013).
15. M. Mumtaz and L. Ping , "Forty years of attacks on the RSA cryptosystem", Journal of Discrete Mathematical Sciences and Cryptography, Vol. 22, No.1, pp. 9-29, (2019).
16. M. R. A. A. Adhikari. "*Basic modern algebra with applications"*, Springer,Newyork, 2014.
17. O. Bogopolski, Introduction to Group Theory", European Mathematical Society, (2008).
18. V. Sidelnikov, M. Cherepnev, and V. Yaschenko, "Systems of open distribution of keys on the basis of noncommutative semigroup," Russian Acad. Sci.Dokl. Math., vol. 48, No. 2, pp. 566-567, (1993).
19. W. Diffie, M. E. Hellman, "New Direction in Cryptography," IEEE Trans, on Inform Theory, 22(6), P. 644-665, (1976).
20. W. Ledermann, "Introduction to Group Theory, Longman, (1973).

[1] Laboratory of Pure and Applied Mathematics , Department of Mathematics, University of M'sila, BP 166 Ichebilia, 28000, M'sila, Algeria.

Email address: nasser.ghedbane@univ-msila.dz