Taylor & Francis
Taylor & Francis Group

Journal of Discrete Mathematical Sciences and Cryptography

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tdmc20

On public key cryptosystem based on the word problem in a group

Nacer Ghadbane

To cite this article: Nacer Ghadbane (2022) On public key cryptosystem based on the word problem in a group, Journal of Discrete Mathematical Sciences and Cryptography, 25:6, 1563-1568, DOI: 10.1080/09720529.2020.1776937

To link to this article: https://doi.org/10.1080/09720529.2020.1776937

Published online: 12 Oct 2020.

Submit your article to this journal

Article views: 10

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=tdmc20

Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 25 (2022), No. 6, pp. 1563–1568
DOI : 10.1080/09720529.2020.1776937

Taylor & Francis
Taylor & Francis Group

On public key cryptosystem based on the word problem in a group

Nacer Ghadbane
Department of Mathematics
Laboratory of Pure and Applied Mathematics
University of M'sila
BP 166 Ichebilia
M'sila 28000
Algeria

Abstract

The asymmetric encryption methods are based on difficult problems in mathematics. Let G be a group, A group word in G on a set Γ of generators is a string $\gamma_{i_1}^{\mu_1}\gamma_{i_2}^{\mu_2}..\gamma_{i_n}^{\mu_n}$ where $n\in\mathbb{N},\gamma_{i_k}\in\Gamma,\mu_i\in\{-1,1\},1\le k\le n$.

The word problem in a group G with respect to a subset Γ is the question of telling whether two words in Γ are equal. It is known that in general the word problem is undecidable, meaning that there is no algorithm to solve it.

In this paper, we introduce a cryptosystem based on the word problem in a group G.

Subject Classification: (*2010*) *68Q42, 20M05.*

Keywords: *Group, Word in a group, Word problem in a group, Public key cryptography.*

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[13], abstract algebra, and information theory.

A secure public key cryptosystem requires a mathematical operation which is easy to compute (encryption) but computationally difficult to

E-mail: nasser.ghedbane@univ-msila.dz

© Taru Publications

reverse (decreption) in a realistic time without knowing a special secret information, called the trapdoor, which is the private key[7].

Recall that if G is a group and $X \neq \varnothing$ a subset of G,

$$gp(X) = \{x_1^{\varepsilon_1} ... x_n^{\varepsilon_n} : x_i \in X, \varepsilon_i \in \{1, -1\}\}$$

If $x_1^{\varepsilon_1} ... x_n^{\varepsilon_n}$ and $y_1^{\mu_1} ... y_m^{\mu_m}$ are two words with $x_i, y_i \in X$ and $\varepsilon_i, \mu_i \in \{1, -1\}$, then they are said to be identytical if $n = m, x_i = y_i$ and $\varepsilon_i = \mu_i$ for $i = 1, ..., m$.

The word problem in a group G with respect to a subset $S = \{s_1, ..., s_n\}$ is the question of telling whether two words in S are equal. It is known that in general the word problem is undecidable, meaning that there is no algorithm to solve it.

The remainder of this paper is organized as follows. In Section 2, we begin with some elementary material concerning of group and word problem in a group. In Section 3, we investigate the public-key cryptosystem based on The word problem in a group. Finally, 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 $H \neq \varnothing$ and for all x, y in H, xy in H H and x^{-1} in H. The subgroup H of a group G is denoted by $H \leq G$.

If a and b are any two elements of G, we have that

$(ab)(b^{-1}a^{-1}) = abb^{-1}a^{-1} = 1$, whence, by the uniqueness of the inverse, $(ab)^{-1} = b^{-1}a^{-1}$.

In a finite group of order m there are m^2 such products, which may be conveniently listed in a $m \times m$ multiplication table, as was first suggested by A. Cayley [6].

For a fixed set of elements $S = \{s_1, ..., s_n\}$ in group G, a word in S is any expression of the sort $s_{i_1}^{k_1} s_{i_2}^{k_2} ... s_{i_n}^{k_n}$ where the exponents k_j are positive

or negative integers, and $s_{i_1},...,s_{i_n} \in S$. For example, $s_1 s_2^3 s_1^{-5} s_2$ is a word in s_1, s_2 and their inverses.

The set S generates G if every element of G is expressible as a word in the elements of S and their inverses.

Fix a group G and a set S of generators $s_1,...,s_n$ for G. For an element $w \in G$, choose an expression of w in terms of the s_i's that is as possible $w = s_{i_1}^{k_1} s_{i_2}^{k_2} ... s_{i_n}^{k_n}$, that is, we choose such an expression with minimal $|k_1| + |k_2| + ... + |k_n|$. Then the length of w (with respect to S) is $l(w) = |k_1| + |k_2| + ... + |k_n|$.

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" [3]. 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.

3. Results

In the following proposition we present the public-key cryptosystem based on the word problem in a group.

Proposition 1

Public-Key (pK) : a group G and two lists $S_A = \{a_1,...,a_m\}$, $S_B = \{b_1,...,b_n\}$ of elements of G.

Alice : choose a secret word $a = k_{pr,A}$ in S_A where

$$a = k_{pr,A} = a_1^{\varepsilon_1} ... a_m^{\varepsilon_m}, \text{ for all } 1 \le i \le m, a_i \in S_A, \varepsilon_i = 1 \text{ or } \varepsilon_i = -1.$$

Alice transmits to **Bob** the list $\{ab_1a^{-1},...,ab_na^{-1}\}$.

Bob: choose a secret word $b = k_{pr,B}$ in S_B where

$$b = k_{pr,B} = b_1^{\mu_1} ... b_n^{\mu_n}, \text{ for all } 1 \le i \le n, b_i \in S_B, \mu_i = 1 \text{ or } \mu_i = -1.$$

Bob transmits to **Alice** the list $\{ba_1b^{-1},...,ba_mb^{-1}\}$.

Encryption: to encrypt $m \in G$, **Alice** compute

$$c = a(ba_m b^{-1})^{-\varepsilon_m}(ba_{m-1}b^{-1})^{-\varepsilon_{m-1}}...(ba_1 b^{-1})^{-\varepsilon_1} m.$$

Decryption: upon receipt c, **Bob** compute

$$b(ab_n a^{-1})^{-\mu_n}(ab_{n-1}a^{-1})^{-\mu_{n-1}}...(ab_1 a^{-1})^{-\mu_1} c = m.$$

Proof : Let $2 \le i \le m-1$, we compute $(ba_{i+1}b^{-1})^{-\varepsilon_{i+1}}(ba_i b^{-1})^{-\varepsilon_i}$, there is only four cases to be considered.

- If $\varepsilon_{i+1} = 1, \varepsilon_i = 1$, then $(ba_{i+1}b^{-1})^{-\varepsilon_{i+1}}(ba_i b^{-1})^{-\varepsilon_i}$
  $= (ba_{i+1}b^{-1})^{-1}(ba_i b^{-1})^{-1} = ba_{i+1}^{-1}a_i^{-1}b^{-1}.$
- If $\varepsilon_{i+1} = 1, \varepsilon_i = -1$, then $(ba_{i+1}b^{-1})^{-\varepsilon_{i+1}}(ba_i b^{-1})^{-\varepsilon_i}$
  $= (ba_{i+1}b^{-1})^{-1}(ba_i b^{-1})^{1} = ba_{i+1}^{-1}a_i b^{-1}.$
- If $\varepsilon_{i+1} = -1, \varepsilon_i = 1$, then $(ba_{i+1}b^{-1})^{-\varepsilon_{i+1}}(ba_i b^{-1})^{-\varepsilon_i}$
  $= (ba_{i+1}b^{-1})^{1}(ba_i b^{-1})^{-1} = ba_{i+1}a_i^{-1}b^{-1}.$
- If $\varepsilon_{i+1} = -1, \varepsilon_i = -1$, then $(ba_{i+1}b^{-1})^{-\varepsilon_{i+1}}(ba_i b^{-1})^{-\varepsilon_i}$
  $= (ba_{i+1}b^{-1})^{1}(ba_i b^{-1})^{1} = ba_{i+1}a_i b^{-1}.$

We have

$$c = a(ba_m b^{-1})^{-\varepsilon_m}(ba_{m-1}b^{-1})^{-\varepsilon_{m-1}}...(ba_1 b^{-1})^{-\varepsilon_1} m = (aba^{-1}b^{-1})m.$$

A similar argument shows that

Let $2 \le i \le n-1$, we compute $(ab_{i+1}a^{-1})^{-\mu_{i+1}}(ab_i a^{-1})^{-\mu_i}$, there is only four cases to be considered.

- If $\mu_{i+1} = 1, \mu_i = 1$, then $(ab_{i+1}a^{-1})^{-\mu_{i+1}}(ab_i a^{-1})^{-\mu_i}$
  $= (ab_{i+1}a^{-1})^{-1}(ab_i a^{-1})^{-1} = ab_{i+1}^{-1}b_i^{-1}a^{-1}.$
- If $\mu_{i+1} = 1, \mu_i = -1$, then $(ab_{i+1}a^{-1})^{-\mu_{i+1}}(ab_i a^{-1})^{-\mu_i}$
  $= (ab_{i+1}a^{-1})^{-1}(ab_i a^{-1})^{1} = ab_{i+1}^{-1}b_i a^{-1}.$
- If $\mu_{i+1} = -1, \mu_i = 1$, then $(ab_{i+1}a^{-1})^{-\mu_{i+1}}(ab_i a^{-1})^{-\mu_i}$
  $= (ab_{i+1}a^{-1})^{1}(ab_i a^{-1})^{-1} = ab_{i+1}b_i^{-1}a^{-1}.$
- If $\mu_{i+1} = -1, \mu_i = -1$, then $(ab_{i+1}a^{-1})^{-\mu_{i+1}}(ab_i a^{-1})^{-\mu_i}$
  $= (ab_{i+1}a^{-1})^{1}(ab_i a^{-1})^{1} = ab_{i+1}b_i a^{-1}.$

We have $b(ab_n a^{-1})^{-\mu_n}(ab_{n-1}a^{-1})^{-\mu_{n-1}}...(ab_1a^{-1})^{-\mu_1}c = bab^{-1}a^{-1}c = bab^{-1}a^{-1}(aba^{-1}b^{-1})m = m.$ □

Example 2 : Let $G = (\{1, x, x^2, y, xy, x^2y\}, \cdot)$ The Cayley table of $G = (\{1, x, x^2, y, xy, x^2y\}, \cdot)$ is defined as follows

(see Table 1):

.	1	x	x^2	y	xy	x^2y
1	1	x	x^2	y	xy	x^2y
x	x	x^2	1	xy	x^2y	y
x^2	x^2	1	x	x^2y	y	xy
y	y	x^2y	xy	1	x^2	x
xy	xy	y	x^2y	x	1	x^2
x^2y	x^2y	xy	y	x^2	x	1

Public-Key (*pK*) : a group $G = (\{1, x, x^2, y, xy, x^2y\}, \cdot)$ and two lists $S_A = \{x, x^2, y\}$, $S_B = \{xy, x^2y\}$ of elements of *G*.

Alice : choose a secret word $a = k_{pr,A}$ in S_A where $a = k_{pr,A} = x^{-1}$: $x^2y^{-1} = x^2x^2y = xy$.

Alice transmits to **Bob** the list $\{(xy)(xy)(xy)^{-1}, (xy)(x^2y)(xy)^{-1}\} = \{xy, y\}$.

Bob : choose a secret word $b = k_{pr,B}$ in S_B where $b = k_{pr,B} = (xy)(x^2y)^{-1} = (xy)(x^2y) = x^2$.

Bob transmits to **Alice** the list

$$\{(x^2)(x)(x^2)^{-1}, (x^2)(x^2)(x^2)^{-1}, (x^2)(y)(x^2)^{-1}\} = \{x, x^2, xy\}.$$

Encryption: to encrypt $y \in G$, **Alice** compute

$$c = xy(xy)(x^2)^{-1}(x)y = x^2y.$$

Decryption: upon receipt *c* **Bob** compute

$$x^2(y)(xy)^{-1}c = x^2(y)(xy)^{-1}x^2y = x^3y = y.$$

4. Conclusion

In this work, based on the hardness of the word problem in a group, we investigate the public key cryptosystem.

References

[1] B. Baumslag, B. Chandler, "Theory and Problems of Group Theory, Schaum's outline series, (1968).

[2] O. Bogopolski, Introduction to Group Theory", *European Mathematical Society*, (2008).

[3] W. Diffie, M. E. Hellman, "New Direction in Cryptography," *IEEE Trans, on Inform Theory*, 22(6), P. 644-665, (1976).

[4] D. Guin et T. Hausberger, "Algèbre Tome 1 Groupes, Corps et Théorie de Galois", EDP Sciences, (2008).

[5] J. Hoffstein, J. Pipher, J. H. Silverman, "An Introduction to Mathematical Cryptography, Springer, (2014).

[6] W. Ledermann, "Introduction to Group Theory, Longman, (1973).

[7] 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).

[8] 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).

[9] C. Paar, J. Pelzl, "Understanding Cryptography", Springer, (2010).

[10] L. Perret, "Etude d'Outils Algébriques et Combinatoires pour la Cryptographie à Clef Publique," thèse de doctorat, Universite de Marne-la-Vallée, (2005).

[11] H. Phan, P. Guillot," Preuves de Sécurité des Schémas Cryptographiques," université Paris 8, (2013).

[12] E. Post, "Recursive Unthenlvability of a Problem of Thue,", *Journal of Symbolic Logic*, 12(1):1-11, (1947).

[13] P. Sundarayya, G. Vara Prasad, "A public key cryptosystem using Affine Hill Cipher under modulation of prime number", *Journal of Information and Optimization Sciences*, Vol. 40, No.4, pp. 919-930, (2019).

[14] S. Qiao, W. Han, Y. Li and L. Jiao, "Construction of Extended Multivariante Public Key Cryptosystems," *International Journal of Network Security*, Vol. 18, No.1, pp. 60-67, (2016).

[15] N. R. Wagner, M. R. Magyarik. A Public Key Cryptosystem Based on the Word Problem. Proceedings of CRYPTO'84, LNCS 196, Springer-Verlag, pp. 19-36, (1985).

Received May, 2019
Revised January, 2020