Random Mapping Transform Algorithm Applied Private key Cryptography (SWAT Algorithm)

Saifuldeen Abdulameer Mohammed [#1], Walid Ameen[#2], Abdullah Abd Ali Jassim [#3]

[1, 2] *Electrical Department, College of Engineering, Baghdad University*

[3]*Computer Centre, Baghdad University*

Baghdad Iraq

[1]saifuldeen@ieee.org

[3]abdullah@uob.edu.iq

[2]profwaleed54@yahoo.com

Abstract— **using the private and public keys in customized cryptographs is limited by mathematics formulas or in other words mathematically mapping technique. If the message "x" and the cryptograph message "y" are both known , then these keys can be predicted and broken by using high performance computers HPC or parallel computing with advanced cryptanalysis technique or using Quantum Computer (cryptograph massage "y" can be known from the files headers as in many computer files) [1]. In this paper we introduce a simple mathematical technique that can generate randomly the cryptograph data straight (or block form) without needing to the synchronization between the transmitter and the receiver. To explain this , we should enable the transmitter (*Ali*) to send his encrypted data which can be detected by the receiver (*Bob*) and in the same time we should prevent the unlikely person (*Oscar*) from getting any idea about transmitted data between Ali and Bob by using our mathematical technique in this paper, we give an example to show the difficulties which will face Oscar when he try to attack by using a brute force or any cryptanalysis Technique (if the x=the massage and y=crypto-massage are both known in any way) the programming in MATLAB r2012b and for plot helping http://www.fooplot.com.**

***Keywords*—Random Generation, Quantum Computing, Anti Crypto analysis.**

I. INTRODUCTION

This in Fig.1 show the simple for stream or the crypto-graphing system in general form.

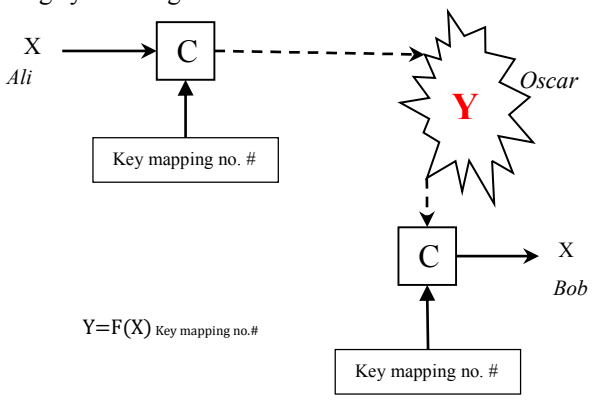

Fig. 1 A crypto graphing system in general form with insecure channel [1]

As shown above the cryptography system (symmetric cryptograph) has formal mapping algebra by using keys, in other words, the tools here work as a function with two variables (keys and x=the massages) and the inverse function also with two variables (usually the variables which are the key and the y=encrypted message data are kept the same most of the time).

Day after day the data security weakness is increased more and more because of insecure data communication channel with advanced attack analytic in both the private and public keys stream and block crypto graphing can be broken by many new ways for crypto analyses like differential cryptanalysis and liner cryptanalysis because all methods use the production mapping when "X" the massage and "Y" the crypto massage both are known (or some of it) from the Header and Footer Identification Codes in all known files on computers operating systems [1][2][3] and the other reason it using Groups theorem and sets of numbers theory (that ever still limited or finite). The first and famous Algorithms in 1970's are DES, AES and 3DES …. and so on from this time many algorithm are related to work and created some of them by practice, the public keys is shown in the second half of 1970's by [4] like RSA and ECC and then this algorithm has simple Arithmetic operations but still work on finite Group with sets Numbers and it can be extended but finally it leads to a slow data transmission rate, so in this paper we introduce our technique by using basic mathematic operations which can work in cryptograph and work randomly without any synchronization. Synchronous is the problem of generating random between the transmitter *(Ali)* and the receiver *(Bob)*, the importance of generating random make no connection between the original message and the encrypted message every time; Therefore, there are many ways to generate random, Random Number Generator (RNG) is a computational to generate a sequence of numbers or symbols that appear random and there are a lot methods to RNG see [5]. But it remains power of random and weakness of synchronous, therefore in this paper we will introduce a novel idea to make both power of random and non-synchronous between *Ali* and *Bob* to transmitter the encryption messages in unsecure

DOI : 04.IJIS.2015.1.1

channels like internet and it can be used in both privet and public key .

II. Basic Math Operations

This section will deal with basic arithmetic operations in 2D vector we will work in the world of xy-plan then [6]:

A.

If we have any two points (x_0, y_0) and (x_1, y_1) in xy-plan then there is one (and must) line runs through them and the equation of it can be:

$y = y_0+m(x-x_0)$ or $y = y_1+m(x-x_1)$..... (1)

Where $m = (y_1-y_0)/(x_1-x_0)$.....(2)

this is liner equations and it is very easy example (1,2) and (3,6) then m=(6-2)/(3-1)=2 and y=2+2(x-1)=2x or y=6+2(x-3)=2x example (2,2) and (4,6) it is the same but shifted by two on y axis m=(6-2)/(4-2)=2 then y=2+2(x-2)=6+2(x-4)=2x-2 if we take $2\leqslant x\leqslant 4$ and the y will be $2\leqslant y\leqslant 6$ and the value of (x, y)are points on the line y=2x-1 but if we take $-\infty<x<+\infty$ it is true that y will be so $-\infty<y<+\infty$ too and (x, y) will be satisfy the equation 0=2x-2-y this properties will help us to applied random operation to our algorithm [6].

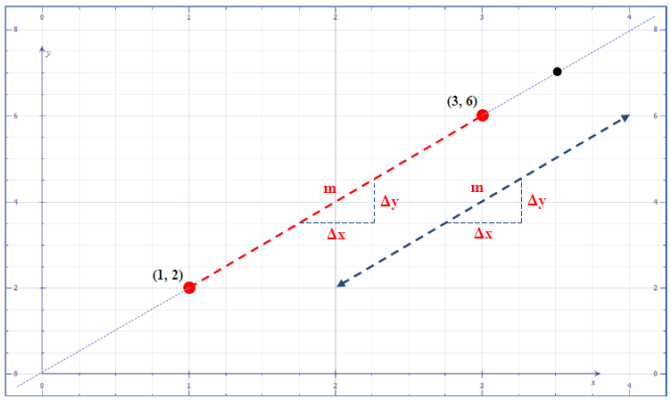

Fig. 2 A Lines equations Basic

B.

if we have two functions $f_1(x), f_2(x)$ then if they are intersection at least on one point then $f_1(x_o) = f_2(x_o)$ to solve this equation we must find x then y example if $f(x) = 2x - 1$ and $g(x) = x^2$ and the band that x work in $\{x: \in 0 \leq x \leq 8\}$ then $2x - 1 = x^2 \rightarrow -x^2 + 2x - 1 = 0 \rightarrow x^2 - 2x + 1 = 0 \rightarrow (x - 1)(x - 1) = 0 \therefore x = 1$ and $y = 1$ the intersection point is (1,1) another example $f(x) = \sqrt[3]{2} - x$ and $g(x) = x^2$ at the same bounder to x then $x = -2$ and $x = 1 \because \{x: \in 0 \leq x \leq 8\}$ then $x = 1$ and $y = 1$ the intersection point is (1,1) too and $\in x^2 \& 2 - x$.

These two basic arithmetic properties are very important to our algorithm in the next section [6].

III. The Algorithm

All paragraphs in this section we will try to transmitter Xm "values of massage" but it must has some deals between *Ali* and *Bob* the attacker (*Oscar* has some *eavesdropping* methods) must do not know some of them. First both *Ali* and *Bob* have keys in form as function and equation, the first key must be one to one function especially in the domain $x_o \leqslant x \leqslant x_{(n-1)}$, the second function not necessary to be one to one maybe equation or very complex one as polynomial have large degree, the algorithm will be:

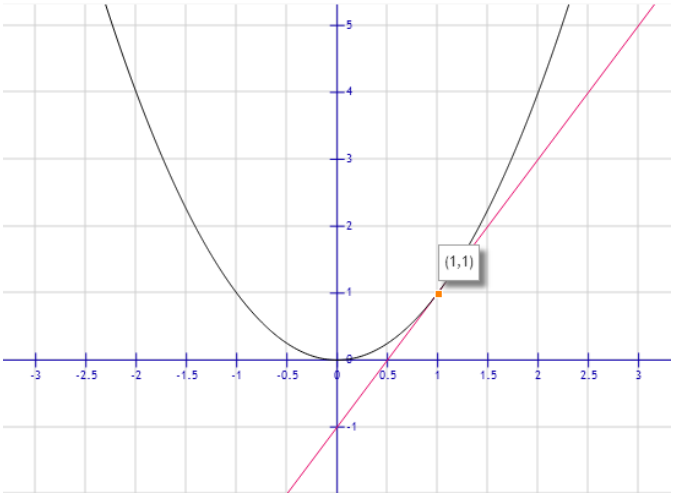

Fig. 3 An intersection point between two functions or equations

A. Ali

(1) X_m {*Ali* must sent (X_m) to *Bob* in the way prevent *Oscar* curiosity}.

(2) Y=f(x) {*Ali* and *Bob* must have both: one-to-one function work at domain $[x_o, x_1 \ldots\ldots x_{n-1}]$}.

(3) $Y_m = f(X_m)$ {*Ali*}.

(4) $P_{r0} = (X_{r0}, Y_{r0})$ {Initial Reference points *Ali* and *Bob* deal and must have it, it can be random}.

(5) $M_c = \frac{Y_m - Yr_0}{X_m - Xr_0}$ {*Ali*: the Slope between Pr_0 and (X_m, Y_m)}.

(6) $y_{ci} = y_m + M_c(x - X_m) = Yr_0 + M_c(x - Xr_0) = f(x_{ci})$ {*Ali*: this is very important step, line equation intersection with y=f(x)}.

(7) $Y_c = y_{ci}$ {Where y_{ci} is random because $\{x_c: x_c \in [x_\alpha \ldots\ldots\ldots x_\beta] \wedge X_m \notin [x_\alpha \ldots\ldots\ldots x_\beta]\}$, *Ali*: very important step is random and it is the core of the algorithm α and β can be any number (-∞,+∞) expect X_m}.

(8) Transmitter (x_c, y_c) {*Ali*}.

(9) $Pr_1 = [P(x)]_{y_c \text{or } x_c}$ or $[P(x)]_{y_c \text{or } x_c}$ {*Ali* and *Bob* will do it P(x) is reference points generating function or equation, may be very complex not one-to-one, Both *Ali* and *Bob* must have it.

This steps for *Ali* only (number 9 for both) now *Bob* will receive (x_c,y_c) we will start from here:

B. Bob

(10) (x_c,y_c) {*Bob* receive the Coded Massage}.

DOI : 04.IJIS.2015.1.1

(11) Y=f(x) {*Ali* and *Bob* must have both: one-to-one function work at domain $[x_o, x_1 \ldots . x_{n-1}]$}.

(12) $P_{r0} = (X_{r0}, Y_{r0})$ { Initial Reference points *Ali* and *Bob* deal and must have it, it can be random}.

(13) $M_c = \frac{y_c - Yr_0}{x_c - Xr_0}$ {*Bob*: Calculate the Slope between Pr0 and (x_c, y_c)}.

(14) $y_d = y_c + M_c(x - x_c) = Yr_0 + M_c(x - Xr_0) = f(x_{ci})$ {*Bob*: Calculate the line equation that intersection with y=f(x)}.

(15) $y_d - f(x) = 0$ {*Bob*: solveing this equation and find xm on sub domain [xo……..xn-1]}.

(16) $Pr_1 = \lceil P(x) \rceil_{y_c \text{or} x_c} \text{or} \lfloor P(x) \rfloor_{y_c \text{or} x_c}$ {*Bob*}.

(17) Go to step (1).

Steps discussion

These Steps can be programming in any language like C++, and MATLAB as a test. We will explain the steps above with detailed one by one as below:

1) Step-1: Xm can be binary Form but converted to decimal form like ASCII code =128=27 code it can be start from 1-128 at x-axis (not from 0-127), then the domain for x will be $\{x: x \in [1,2,3 \ldots \ldots 128]\}$ as a normal so we must Create a table to exchange the Number to Binary or ASCII Code, the Xm must be integer numbers (Note: in this Algorithm can be float number but not in this example!).

2) Step-2: y=f(x) is new Technique for keys between *Ali* and *Bob* (*Oscar* the Attacker must or Should not be know any or one of the Pr(x), f(x) or Pr0) we will explain that, this is the main deferent between our algorithm and the other old algorithms that using keys as a numbers, the probability to find the functions is infinite but f(x) must here only and only one-to-one.

3) Step-3: Ym=f(Xm) this step to find the image for Xm in x-axis on the y-axis (Ym) by the roll y=f(x) to obtains (Xm ,Ym) this is not coded massage but will use to find another equation that will using random technique (it is here in cryptograph issues) see *Step-7*.

4) Step-4: is not step here but it been putting to explain that it initial point or reference point using with (Xm, Ym) to find liner equation.

5) Step-5: Calculate Mc the slop between (Xm, Ym)∈ f(x) and Pr0=(Xr_0, Yr_0) initial point or reference point. The slop here is very important to determine the liner equation that will be as f(x) than determine the final (X_C, Y_C). Note that both Xc and Yc is random for Xm that we have [Xα……..Xβ] ⊄ Xm its self than [Yα……..Yβ] ⊄Ym too. If α and β are very large numbers □±∞ than we will have unusual cryptograph technique, there are many cryptosystems (in work too) have the same idea but not like that the old systems depending on the last or present input to crating random behaviour but this system (our system SWAT) is pure random behaviour.

6) Step-6: This step will compute or building up a liner equation from (Xm, Ym)∈ f(x) and $Pr_0 = (X_{r0}, Yr_0)$ using the equation no. 1 nd 2 than y_{ci} is initial function for coding.

7) Step-7: It is very importance step that calculate (Yc from random Xc) then (Xc, Yc).

8) Step-8: Transmitter the (X_c, Y_c) not M_c or Y_m or (X_{ri}, Y_{ri}). Note that from *Step-1* to *Step-8* doing by *Ali*.

9) Step-9: Then after transmitter (X_c, Y_c) *Ali* compute (X_{ri+1}, Y_{ri+1}) that will be random because Xc or Yc were both random and after *Bob* receive (X_c, Y_c) he will compute (X_{ri+1}, Y_{ri+1}) which is the same point that *Ali* have been computed. The changing in P_{ri} every transmitting will showing to *Oscar* there is no relationship between X_c and Y_c (Note that if it not changing and we know the relationship between X_c and Y_c still we don't have f(x) it will showing in the example more details) may be the Pr0=(X_{r0}, Y_{r0})=(0,0) at first then will be changing using $P_r(x)$ as integer number to easy way at calculating the error be minimized in the *Bob* it easy if he have (x_0, y_0) and f(x), X_m will be found by P(x).

10) Step-10: The result (xc, yc) as a number then will be continuing.

11) Step-11: He "*Bob*" has P_{ro} point.

12) Step-12: Can *Bob* compute M_c.

*13) Step-13:*Calculate or solving the two equations $y_{ci}=y_d$ they are liner equations intersection with f(x) at point X "Sometimes two points" and find the solution on the domain $[x_0 \ldots\ldots\ldots x_{n-1}]$.

14) Step-14: If f(x) is one-to-one function with respect to P_{ri} the solution is one point if not, there is many solutions that is not problem.

15) Step-15: Compute a new P_{ri+1}.

IV. TUTORIAL EXAMPLE

If we used ASCII code for representation the phrase: "ATTACK-Caesar" using 7-bit not extended then:

"Start of text ATTACK-Caesar End of text"

The massage in decimal number will be:

2 65 84 84 65 67 75 45 67 97 101 115 97 114 3 = X_m

- f(x)=x+2
- P_0=(0, 0)
- $P(x) = \pm\lceil\sqrt{x^2 + a^2}\rceil$ Let a=128

Let start (see Figure 4.):

- X_m=2 P_0 = (0, 0) then Y_m=2+2=4.
- M_c=(4-0)/(2-0)=2
- Y_{ci}=4+2(x-2)=0+2(x-0)=2x

Let α=-128 and β=128 then $X_c \in$ [-128……128] ∄2 let X_c=-4 (random) then Y_c=-8 (X_c, Y_c) transmitted the next massages will be as in the Table 1 below.

DOI : 04.IJIS.2015.1.1

TABLE I
TUTORIAL EXAMPLE

i	PN	Massage		Coded (this is will be transmitted)	P_{ri}
0	+	Start of text	2	(-4,-8)	(0,0)
1	-	A	65	(120, 18.37681)	(-4,128)
2	+	T	84	(20, 318,88889)	(120,-45)
3	-	T	84	(-16, 148.5)	(20,126)
4	+	A	65	(-6, -103.04938)	(-16,-127)
5	-	C	67	(-16, 136.08219)	(-6,128)
6	+	K	75	(100, 97.17582)	(-16,-128)
7	-	-	45	(-9, 14.6)	(100.80)
8	+	C	67	(-60, 260.19737)	(-9,-128)
9	-	a	97	(-60, 113)	(-60,113)
10	+	e	101	(-25, -66.04348)	(-60,-113)
11	-	s	115	(10, 123.75)	(-25,126)
12	+	a	97	(-10, -180.18391)	(10,-128)
13	-	r	114	(100, 117.35484)	(-10,128)
14		End of text	3	(1, 168.50515)	(100,-80)

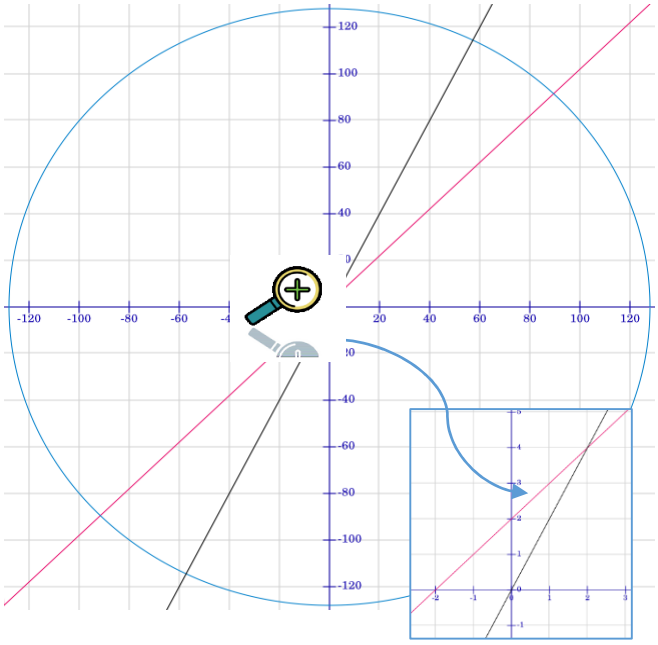

Fig. 4 line graph for the Tutorial Example

V. CONCLUSIONS

Depending on the previous experience in security and cryptograph ,technique like AES DES 3DES RSA Elliptic curve….etc. algorithms possible breakthrough algorithms through a sophisticated and advanced decryption methods alongside high speed of giant computer, or use Quantum Computer Machines "It's now 512-bit works on a commercial scale" [1][2] and so, this algorithm "and affixes before, knowing that zero dimensions, one-dimensional and three-dimensional"[7] is precisely it two-dimensional and the best is the three-dimension that has no intersection points between f(x) and the line equation.

Using brute-force method to find the keys (f(x) Pr(x) and P0(x,y)) in this way is impossible because the key (even is short) are not in usual ways even one or more is knowing for example if all keys are in hand but the initial reference point is missing then the massage cannot be broken even if the attacker knows the algorithm (kerckhoffs' principle)[1] therefore it is very strong point for this algorithm. We mentioned that our way is customized not standardized and in Table II we give more information about the meanings of customization by showing the programmable parts of our customized way (and if you need more information about its programming, please, contact us).

TABLE II
PROGRAMMING AND CUSTOMIZATION VARIABLES

	Keys function	In the example	How!
1	PN	+-+-+-+……..	any sequence we want
2	Reference point	(0,0)	Any point
3	Y=f(x)	x+2	Any linear equation
4	P(x)	$^{+}_{-}\lceil\sqrt{x^2+a^2}\rceil$	Any circle or ellipse equation
5	a	a=128	Any number floating or integer

ACKNOWLEDGMENT

This research is a part of a series and we have more advanced researches under development, this research is finished and now we are using it with other algorithms (Sumerian Algorithm) in Iraq for text cyphering and also we are preparing to use it in e-Health, e-Government and Banking solutions based on IBM WebSphere Message Brokers, Message queue, Websphere Sensor Events and Websphere Telemetry with MQTT in the Internet of Things (IoT) applications and solutions like Smart Cities, smart transportation, smart e-Health , smart water and waste water, Mobile Enterprise Computing, ePayment, Smart Cards and many other applications and solutions.

We have other more advanced researches about new techniques by using the IBM Power 8 (we are using the instruction set 2.07 with transactional memory but till now we are waiting the hardware) with the NVidia GPU and FPGA using transactional memory according to the PCIe 3 for smart multi levels and multi nodes machine learning cryptograph system.

REFERENCES

[1] C. Paar and J. Pelzl, *Understanding Cryptography* Copyright Springer-Verlag Berlin Heidelberg 2010.

[2] L. Grover. *A fast quantum-mechanical algorithm for database search*. In Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing, pages 212–219. ACM, 1996.S.

[3] Frederik Armknecht. Algebraic attacks on certain stream ciphers. PhD thesis, Department of Mathematics, University of Mannheim, Germany, December 2006.

[4] W. Diffie and M. E. Hellman, *New directions in cryptography*. IEEE Transactions on Information Theory, IT-22:644–654, 1976.

[5] Christophe Dutang and Diethelm Wuertz *A note on random number generation* September 2009

[6] James Stewart, *Calculus Early Transcendental* 7th Edition, U.S.A Publisher Brooks/Cole, 2011.

[7] Saifuldeen Abdulameer Mohammed, *Dedicated communication device and encryption of Arabic and English texts together by unifying repeated characters algorithm and synchronous random selection,* Series Lecturers Notes in Electrical Engineering Department College of Engineering, Baghdad University, in Baghdad Iraq, 2012-2013.

DOI : 04.IJIS.2015.1.1