International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:2, No:11, 2008

Modified Diffie-Hellman Protocol By Extend The Theory of The Congruence

Rand Alfaris, Mohamed Rushdan MD Said, Mohamed Othman, and Fudziah Ismail

Abstract—This paper is introduced a modification to Diffie-Hellman protocol to be applicable on the decimal numbers, which they are the numbers between zero and one. For this purpose we extend the theory of the congruence. The new congruence is over the set of the real numbers and it is called the "real congruence" or the "real modulus". We will refer to the existing congruence by the "integer congruence" or the "integer modulus". This extension will define new terms and redefine the existing terms. As the properties and the theorems of the integer modulus are extended as well. Modified Diffie-Hellman key exchange protocol is produced a sharing, secure and decimal secret key for the the cryptosystems that depend on decimal numbers.

Keywords—Extended theory of the congruence, modified Diffie-Hellman protocol.

I. Introduction

WE use Diffie-Hellman protocol, [4], mainly as a key exchange in cryptography field. This protocol gives the sharing secret key as an integer number. The questions are, when the cryptosystem does not depend on integer numbers, [11], how can we produce a sharing secret key as real number while keeping it secure and how can we use the theory of the integer congruence when the numbers in use are only the real numbers, specifically, decimal numbers?

Of course, it is easy to go directly to Diffie-Hellman protocol, and we can introduce the modification on it. However, the problems that we will encounter are, what is this modification based on? How can we use the modulo function $(\mathrm{mod}\ m)$ on real number m when it is never defined on such numbers, and how can we just define the modulo on the real numbers when we do not have definition for the greatest common divisor on the real numbers? Finally, the most important problem that we will face is, how can we built a computer program to implement the decimal cryptosystem and modified Diffie-Hellman protocol without having algorithms for defining and applying topics like mod, gcd and discrete logarithmic equation on the real numbers in the library of the computer programming?

In this research we give the answers to these questions by introducing an extension to the theory of the congruence to cover the set of the real numbers. The most important part of this extension depends on two definitions. The first is the definition of the greatest common divisor on the real numbers and the second is the definition of the modulus on the real numbers.

We extend theorems like "Least Positive real number", "Well-Ordering principle" and "Greatest common divisor theorem" which are the bases for proving that the greatest common divisor is applicable on the real numbers. In addition, we give most of the proofs of the extended theorems of the congruence.

For the greatest common divisor and the congruence concept we refer to [8], [9], [5], [3], [1], [2], [6] and [7]. We refer to [4] and [12] for the modification of Diffie-Hellman key exchange protocol. Finally, in this paper, we do not include all the proofs of the theorems and the propositions. The full proofs can be found in [10]

This research is organized as follows. Beside the section on the introduction, we introduce the theories of the greatest common divisor on the real numbers and the congruence on the real numbers in the second and the third sections respectively. In the fourth section we modify the Diffie-Hellman scheme.

II. The Extension of the Theory of the Congruence

A. Real Greatest Common Divisor

To put the greatest common divisor on the real numbers in its right form, we introduce new terms such as "the length of the real number" and "zero real length divisors", and redefine the related terms to the congruence and the greatest common divisor. The theorems that related to the greatest common divisor are extended in this section.

Definition 1: **The length of the real number**
The ***length of the real number r*** is the number of the digits to the right of the decimal point, and we denote by $\mathrm{rl}(r)$.

For example, $\mathrm{rl}(34.9273543) = 7$ and $\mathrm{rl}(618) = 0$.

We are introducing an extension to the theory of the congruence in order to implement it in cryptography, we need to apply the pure mathematics theories in computer programs. Therefore, definition (1) is important to define the number of digits after the decimal point of the real numbers.

R. Alfaris (the corresponding author) and M. Said are with the Institute for Mathematical Research, University Putra Malaysia, Serdang, 43400, Selangor, Malaysia, e-mail: randalfaris@yahoo.co.uk
M. Othman is with Department of Communication Technology and Networks, Faculty of Computer Science and Information Technology, University Putra Malaysia.
F. Ismail is with Mathematical Department, Faculty of Science, University Putra Malaysia.

Definition 2: **The real factor, real divisor**
Let x and m be real numbers. We say m is a ***real factor*** or ***real divisor*** of x if there exist a real number r such that $x = m \cdot r$ and $\mathrm{rl}(r) = s$, where $s \in \mathbb{Z}^+$. We say m is ***not divisor*** or ***nondivisor*** of x if $\mathrm{rl}(x/m) = \infty$.

For example, $0.4,\ 0.6,\ 0.002$ and 160 all considered as some of the real factors of the real number 0.32, but, 3.5 is not a factor or not a divisor of 1.29 because $1.29/3.5 = 0.368571422857142\cdots$, here $\mathrm{rl}(1.29/3.5) = \infty$.

Definition (2) produces two main results, the first one is, there are infinitely many real factors for each real number and hence there are infinitely many real divisors. The second result is, the real divisor could be greater than the number itself.

Proposition 1: If the real number m is a common real divisor of real numbers a and b, then m is a common real divisor of the linear combination $ac + bd$ for any integer numbers c and d.

Proof: We have m divides a and b, which means, $a = m \cdot r_1$ and $b = m \cdot r_2$ with $rl(r_1)$ and $rl(r_2)$ finite integers. Therefore, $ac + bd$ can be written as $m(r_1 \cdot c + r_2 \cdot d)$, it is obvious that the real length of $r_1 \cdot c + r_2 \cdot d$ is still finite integer. That means m is a real divisor of $ac + bd$.

■

Definition 3: **ZRL-divisor**
We say the real number m is ***zero real length divisor*** of the real number x if $x/m \in \mathbb{Z}$. That means, if m divides x without remainder then $\mathrm{rl}(x/m) = 0$. We denoted the zero real length divisor by ZRL-divisor.

For example, 2.005 is the ZRL-divisor of 52.13 since $\mathrm{rl}(52.13/2.005) = 0$.

Definition 4: **The greatest common divisor of the real number**
The greatest common divisor of the two real numbers a and b, denoted by $\mathrm{rgcd}(a, b)$ and called ***real greatest common divisor***, is the largest positive ZRL-divisor of a and b and $\mathrm{rl}(\mathrm{rgcd}(a, b)) = \max\{\mathrm{rl}(a), \mathrm{rl}(b)\}$.

The algorithm for finding the rgcd is the same as the Euclidian algorithm for finding the gcd but the difference is that it should be done without removing the decimal points of the real numbers. For instance, $\mathrm{rgcd}(2.11, 3.8) = 0.01$.

Definition 5: **Real multiple**
Let r and s be real numbers. If r is a real divisor of s, then we say that s is a ***real multiple*** of r. Moreover, the real numbers $r_1, r_2, \cdots, r_n$ are not all equal to zero, have a common real multiple s if r_i is a real divisor of s for $i = 1, 2, \cdots, n$. The least positive common real multiple is called the ***least common real multiple***, and it is denoted by $[r_1, r_2, \cdots, r_n]_{\mathbb{R}}$.

Definition 6: **Real prime numbers**
We say a is a ***real prime number*** if $\mathrm{rl}(a) = \infty$.

Following definition (2), the number a, such that $\mathrm{rl}(a) = \infty$, has no real divisors except itself and the integer number 1. This fact is consistent with the definition of the integer prime numbers.

Definition 7: **Relatively real prime numbers**
Any two real numbers a and b are called ***relatively real prime***, if the $\mathrm{rgcd}(a, b) = 10^{-s}$ where $s = \max\{\mathrm{rl}(a), \mathrm{rl}(b)\}$.

Proposition 2: **(Extension of Least Positive real number)**
For every set S of all positive real numbers of the definite maximum real length, say t , the real number 10^{-t} is the least positive real number. That is $10^{-t} \leq x$ for all $x \in S$.

Proof: Let S be the set of all positive real numbers x of the definite maximum real length t such that $10^{-t} \leq x$. Then $10^{-t} \in S$. Suppose $k \in S$. Now $0 < 10^{-t}$ implies $k = k + 0 < k + 10^{-t}$, so we have $10^{-t} \leq k < k + 10^{-t}$. Thus $k \in S$ implies $k + 10^{-t} \in S$.

■

According to this theorem, the least positive real number is not unique. There is a family of the least element in the set of real number. each member in this family is a unique when we define its real length.

Proposition 3: **(Extension of Well-Ordering Principle)**
Every nonempty set S of positive real numbers of the definite maximum real length contains a least element. That is, there is an element $m \in S$ such that $m < x$ for all $x \in S$.

Proof: Let S be the nonempty set of positive real numbers and let these real numbers have the definite maximum real length, say t, that is $t = \max\{\mathrm{rl}(x) : \forall x \in S\}$.
If $10^{-t} \in S$, then $10^{-t} \leq x$ for all $x \in S$, by the extension of the least element theorem. In this case, $m = 10^{-t}$ is the least element in S. Consider now the case $10^{-t} \notin S$, and let L be the set of all positive real numbers p of the definite maximum real length t, such that for all $p < x$. That is,

$$L = \left\{p \in R^+ : \mathrm{rl}(p) = t \quad \text{and} \quad p < x, \forall x \in S\right\}.$$

Since $10^{-t} \notin S$, then the extension of the least element theorem assure us that $10^{-t} \in L$. We shall show that there is a positive real number $p_\circ$ such that $p_\circ \in L$. And $p_\circ + 10^{-t} \notin L$. Suppose that this is not the case. Then we have that $p \in L$ implies $p + 10^{-t} \in L$. This contradicts the fact that S is nonempty (note that $L \cap S = \phi$). Therefore, there is $p_\circ$ such that $p_\circ \in L$ and $p_\circ + 10^{-t} \notin L$. We must show that $p_\circ + 10^{-t} \in S$. We have $p_\circ < x$ for all $x \in S$, so $p_\circ + 10^{-t} \leq x$ for all $x \in S$ (because 10^{-t} is the least element, then there is no element n such that $m < n < m + 10^{-t}$ in S. If $p_\circ + 10^{-t} < x$ were always true for this set, then $p_\circ + 10^{-t}$ would be in L. Hence $p_\circ + 10^{-t} = x$ for some $x \in S$, and $m = p_\circ + 10^{-t}$ is the required least element in S.

■

Proposition 4: **(Extension of the Division Algorithm)**
For any two real numbers a and b with $a > b$, there exist unique positive integer number q and unique positive real number c and $\mathrm{rl}(c) = \max\{\mathrm{rl}(a), \mathrm{rl}(b)\}$ such that $a = bq + c$, with $c \in [0, b)$.

Proof: **Existence:** Let S be the set of all real numbers $j = a - bn$ for $n \in \mathbb{Z}$ and $\mathrm{rl}(j) = \max\{\mathrm{rl}(a), \mathrm{rl}(b)\}$, and let S' be the set of all nonnegative real numbers in S. The set S' is nonempty. (for specific example: $0.18 = 1.2 - 0.51(2)$). If $0 \in S'$, we have $a - bq = 0$ for some q, and $a = bq + 0$. If $0 \notin S'$, since all the numbers in S' have real length not greater than the maximum real length of a and b, then S' has definite maximum real length then by the extension of well-ordering theorem, S' contain a least element $c = a - bq$ which gives

$$a = bq + c,$$

where c is positive. Now

$$c - b = a - bq - b = a - b(q + 1),$$

So $c - b \in S$. Since c is least element in S' and $c - b < c$, it must be true that $c - b$ is negative. That is, $c < b$. Combining the two cases, we get $a = bq + c$, with $c \in [0, b)$.

Uniqueness: To show q and c are unique, suppose $a = bq_1 + c_1$ and $a = bq_2 + c_2$ where $0 \leq c_1, c_2 < b$, we may assume $c_1 \leq c_2$ without loss of generality. This means that

$$0 \leq c_2 - c_1 \leq c_2 < b.$$

However, we also have

$$0 \leq c_2 - c_1 = (a - bq_2) - (a - bq_1) = b(q_2 - q_1).$$

That is, $c_2 - c_1$ is nonnegative multiple of b that is less than b. This gives $c_2 - c_1 = 0$ and $c_2 = c_1$. It follows that $bq_2 = bq_1$ and $q_2 = q_1$ where $b \neq 0$.

■

Proposition 5: **(Extension of Greatest common divisor theorem)**
Let a and b be real numbers, at least one of them not equal to zero. Then there exist a unique real greatest common divisor d of a and b. Moreover, d can be written as $d = a \cdot p + b \cdot q$ with $\mathrm{rl}(d) = \max\{\mathrm{rl}(a), \mathrm{rl}(b)\}$, for integer numbers p and q.

Proof: Consider the linear combination $ap_\circ + bq_\circ$, where $p_\circ$ and $q_\circ$ are integer numbers. According to proposition (2), We can choose p and q such that $l = ap + bq$ is the least positive real number for the family of all the linear combinations $\{ap_\circ + bq_\circ\}$, of course this family includes all the numbers.
The strategy of the proof is, first, we need to prove that l is a ZRL-divisor of both a and b. Second, we prove that $d = l$.
Let us prove that l is a ZRL-divisor of a, the other one will follow the same scheme. We assume that l is a real divisor of a, (i.e. $a/l = t$, $rl(t) = s$ and $s \in \mathbb{Z}$), but not ZRL-divisor of a, (i.e. t is integer number). Then, by the extension of division algorithm, proposition (4), there exist unique positive integer number k and unique positive real number r and $\mathrm{rl}(r) = \max\{\mathrm{rl}(a), \mathrm{rl}(l)\}$ such that $a = lk + r$, with $r \in [0, |l|)$. This will lead to, $r = a - k(ap + bq) = a(1 - kp) + b(-kq)$, this means that r is in the set of $\{ap_\circ + bq_\circ\}$, which is cannot be. So that l is must be ZRL-divisor of a. Similarly we can prove that l is ZRL-divisor of b.
Finally, d is the real greatest common divisor of a and b. That means it is the ZRL-divisor of them. In this case we may write: $a = dz_1$ and $b = dz_2$ and $l = d(z_1 p + z_2 q)$, there for d is ZRL-divisor of l, that means $d \leq l$. But $d < l$ is impossible because here we have to follow the definition of divisor on integer numbers for we have ZRL-divisor. So we conclude that $d = l$. Then $d = a \cdot p + b \cdot q$.

■

Proposition 6: **(Extension of Least common real multiple theorem)**
If s is any common real multiple of $r_1, r_2, \cdots, r_n$, then $[r_1, r_2, \cdots, r_n]_{\mathbb{R}}$ is a real divisor of s.

Proof: Let $[r_1, r_2, \cdots, r_n]_{\mathbb{R}} = u$. Then, $0, \mp u, \mp 2u, \mp 3u, \cdots$ are all common real multiples of $[r_1, r_2, \cdots, r_n]_{\mathbb{R}}$.
Now, let t be any common real multiple, and divide t by u. By extension the division algorithm, proposition (4), there exist unique positive integer number q and unique positive real number c and $\mathrm{rl}(c) = \max\{\mathrm{rl}(t), \mathrm{rl}(u)\}$ such that $t = uq + c$, with $c \in [0, u)$. Now, we need only to prove that $c = 0$. Let us assume that $c \neq 0$, then for each $i = 1, 2, \cdots n$ we know that r_i is a real divisor of u and r_i is a real divisor of t, so that r_i is a real divisor of c. Therefore, c is a positive common real multiple of $r_1, r_2, \cdots, r_n$, but this contradict the fact that u is the least of all the positive common real multiples.

■

The next theorem gives some of the properties of the real greatest common divisor. We will not include the proofs.

Theorem 1: The greatest common divisor on the real numbers has the following properties.

1) The extension of Bezout's identity is applicable for real greatest common divisor. $\mathrm{rgcd}(a, b)$, where a and b are not both zero, may be defined alternatively and equivalently as the smallest positive integer d which can be written in the form $d = a \cdot p + b \cdot q$ where p and q are integer numbers. Numbers p and q like this can be computed with the extended Euclidean algorithm as well.
2) Every common real divisor of a and b is a real divisor of $\mathrm{rgcd}(a, b)$.
3) If $d = \mathrm{rgcd}(a, b)$ then d is ZRL-divisor of $a - b$.
4) If a and b are relatively prime then $(\mathrm{rgcd}(a, b))^n$ is a real divisor of $a - b$ for all n and it is a ZRL-divisor of $a - b$, for all $n \geq 1$.
5) If m is any real number then $\mathrm{rgcd}(m \cdot a, m \cdot b) = m \cdot \mathrm{rgcd}(a, b)$ and if m is nonzero then $\mathrm{rgcd}\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{\mathrm{rgcd}\ (a,b)}{m}$.
6) If $\mathrm{rgcd}(a, b) = d$ then $\frac{a}{d}$ and $\frac{b}{d}$ are integer relatively prime, i.e. $(\mathrm{rgcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1)$.
7) $\mathrm{rgcd}(a \pm b, b) = \mathrm{rgcd}(a, b)$.
8) The rgcd is commutative and associative.
9) The rgcd of three numbers can be computed as $\mathrm{rgcd}(a, b, c) = \mathrm{rgcd}(\mathrm{rgcd}(a, b), c)$, or in some different way by applying commutatively and associatively. This can be extended to any number of numbers.

Proposition 7: Let a be a real number and let c and b are integer numbers. If c is a real divisor of the product ab and $\mathrm{grc}(b, c) = 1$ then c is a real divisor of the product a.

Proof: We have $\mathrm{rgcd}(m \cdot a, m \cdot b) = m \cdot \mathrm{rgcd}(a, b)$ by theorem (1)–(5). By the hypothesis c is a real divisor of ab and it is clear that c is a real divisor of the product ac, so c is a real divisor of a by theorem (1)–(2).

■

B. Real Congruence

The important part in this research is the real congruence on the set of real numbers, since the modification of Diffie-Hellman protocol depends on applying the theory of modulo on the real numbers. Here, we will introduce the extension of the definitions and the theorems of this theory.

Definition 8: **Real congruence**
Let a and b belong to the set of real numbers $\mathbb{R}$. We say that ***a congruence to b modulo real number r*** if $a - b = k \cdot r$, for some $k \in \mathbb{Z}$, that is r is ZRL-divisor of $(a - b)$. We denote the modulus of real numbers by rmod and we write $a \equiv b \pmod{r}$. In the cases that r is real divisor or nondivisor of $a - b$, we say that a is not congruent to b real modulo r, and in this case we write $a \not\equiv b \pmod{r}$.

For a further explanation, a, b and r are all real numbers. If a congruence to b real modulo r, then r divides the value $a - b$ without remainder. According to the definition (3), r is ZRL-divisor of $(a - b)$.
We say that a is not congruent to b real modulo r in two cases, both of them followed the definition (2). The first case is when r a real divisor of $(a - b)$, in this case $\mathrm{rl}\left(\frac{a-b}{r}\right) = k$ where $k \in$ Z. The second case is when r not a divisor of $(a - b)$, and in this case $\mathrm{rl}\left(\frac{a-b}{r}\right) = \infty$.
This definition is an extension to the classic definition of the modulus; the difference is that we expand the set of numbers that is implemented under this operation.

Definition 9: **The real residue**
If $a \equiv b \,\mathrm{rmod}\, r$ then b is called a ***real residue*** of $a \; modulo \; r$, for all a, b and r in the set of real numbers.

Definition 10: **The least real residue**
The real number s is called the ***least real residue*** of a if $a \equiv s \,\mathrm{rmod}\, r$ and $s \in [0, r)$.

In the integer congruence, the least residue y of $x \equiv y \mod m$ is could be one on the integers in $0 \leq y < x$. The important note here is the least real residue s in $a \equiv s \,\mathrm{rmod}\, r$ is belong to uncountable set.

Definition 11: **The complete canonical real residue system**.
An infinite set of real numbers $s_i \in [0, r)$ is called a ***complete canonical real residue system modulo r*** if for every real number b there is one and only one s_i such that $b \equiv s_i \,\mathrm{rmod}\, r$.

It is very important to note that the complete canonical real residue system is an uncountable set, because, $s_i \in [0, r)$ means s_i belong to uncountable interval. This is considered as the significant difference from the integer complete canonical residue system. The consequences of the difference will affect the solution of the real congruence equation as we will see in the subsection (II-C).

Definition 12: **The real congruence class**
For fixed real number a and $d > 0$, the set of all real numbers x satisfying $x \equiv a \,\mathrm{rmod}\, d$ is the arithmetic progression

$$..., a - 2d, a - d, a, a + d, a + 2d, ...$$

called a ***real residue class*** or real congruence class of real modulo d.

Proposition 8: $a \equiv b \pmod{r}$ if and only if a and b leave the same remainder when dividing by r.
Proof: We have

$$a \equiv b \pmod{r} \tag{1}$$

then there exist a unique $c \in [0, r)$ such that

$$a \equiv c \pmod{r}. \tag{2}$$

From Eq. (1) there exist t such that

$$rt = a - b. \tag{3}$$

The same for Eq. (2), there exist s such that

$$rs = a - c. \tag{4}$$

From Eq's. (3) and (4) we will get

$$r(t - s) = c - b \Rightarrow \quad r \quad \text{divides} \quad c - b. \tag{5}$$

That means there exist a unique $q \in [0, r)$ such that

$$b = qr + c \tag{6}$$

also from Eq. (2) we have

$$a = sr + c \tag{7}$$

In other word, a and b leave the same remainder when dividing by r.
On the other hand, if we have $a = sr + c$ and $b = qr + c$ then $a - b = r(s - t) \Rightarrow a \equiv b \,\mathrm{rmod}\, r$.

■

The proposition above leads to the next corollary, which is another way to describe this relation.

Corollary 1: $a \equiv b \pmod{r}$ if and only if there exist an integer k such that $a = b + k \cdot r$.

Proposition 9: Every real number is congruent modulo r to exactly one of the values in the interval $[0, r)$, and no two values in this interval are congruent modulo r.
Proof: Using the division algorithm on real numbers gives $a = rq + c$ where q is unique positive integer and $c \in [0, r)$ is unique real number. That is, $a - c = rq$ which it means, that $a \equiv c \pmod{r}$ where $c \in [0, r)$.
It is simple to prove that if $a \equiv c_1 \pmod{r}$ and $a \equiv c_2 \pmod{r}$ then $c_1 = c_2$ for $0 \leq c_1, c_2 < r$.

■

Proposition 10: If $a \equiv b(\mathrm{rmod} r)$ then $\mathrm{rgcd}(a,r) = \mathrm{rgcd}(b,r)$.

Proof: We have $a \equiv b(\mathrm{rmod}\ r)$ which means $a-b = r\cdot k$, for some $k \in \mathbb{Z}$. Since $\mathrm{rgcd}(a,r)$ divides a and r without reminder, that means $\mathrm{rgcd}(a,r)$ is a ZRL-divisor of a and r. Then we have $\mathrm{rgcd}(a,r)$ is a ZRL-divisor of b and hence $\mathrm{rgcd(a,r)}$ is a ZRL-divisor of $\mathrm{rgcd(b,r)}$. In the same way we can prove $\mathrm{rgcd\ (b,r)}$ is a ZRL-divisor of $\mathrm{rgcd(a,r)}$ and that leads to $\mathrm{rgcd(a,r)} = \mathrm{rgcd(b,r)}$ because both of them are positive.

■

We will highlight the properties of the real congruence in the next theorem. We will see that some of the properties are similar to the integer congruence.

Theorem 2: The congruence on the real numbers has the following properties,

1) There are infinitely many complete real residue systems and each system is uncountable set.
2) For any real numbers a and b, $a \equiv b\ (\mathrm{rmod}\ \mathrm{rgcd}(a,b))$.
3) If a and b are relatively prime then $a \equiv b\ \mathrm{rmod}\ (\mathrm{rgcd}(a,b))^n$, $n \geq 1$.
4) If $a \equiv b\ \mathrm{rmod}\ r$ and $a' \equiv b'\ \mathrm{rmod}\ r$ then $a \pm a' \equiv b \pm b'\ \mathrm{rmod}\ r$ for any real numbers a, b, a' and b'.
5) i. if $a \equiv b\ \mathrm{rmod}\ r$ and $c \equiv d\ \mathrm{rmod}\ r$ then $ax + cy \equiv bx + dy\ \mathrm{rmod}\ r$, where x and y are integers.
   ii. if $a \equiv b\ \mathrm{rmod}\ r$ and $c \equiv d\ \mathrm{rmod}\ s$ then $ac \equiv bd\ \mathrm{rmod}\ rs$
6) i. $a \equiv b\ \mathrm{rmod}\ r$, $b \equiv a\ \mathrm{rmod}\ r$ and $a - b \equiv 0\ \mathrm{rmod}\ r$ are equivalent statement.
   ii. $a \equiv b\ \mathrm{rmod}\ r$ and $b \equiv c\ \mathrm{rmod}\ r$ then $a \equiv c\ \mathrm{rmod}\ r$.
   iii. If $a \equiv b\ \mathrm{rmod}\ r$ then $k\cdot a \equiv k\cdot b\ \mathrm{rmod}\ k\cdot r$, $\forall\ k \in \mathbb{R}$.
   iv. If $a \equiv b\ \mathrm{rmod}\ r$ then $l \cdot a \equiv l \cdot b\ \mathrm{rmod}\ r$ where l is integer.
   v. If $a \equiv b\ \mathrm{rmod}\ r$ and d is ZRL-divisor of m then $a \equiv b\ \mathrm{rmod}\ d$.
   vi. The real modulus is reflexive, symmetric and transitive.

Proposition 11: Let a, x, y and r be real numbers,

1) $ax \equiv ay\ \mathrm{rmod}\ r$ if and only if $x \equiv y\ (\mathrm{rmod}\ \frac{r}{\mathrm{rgcd(a,r)}})$.
2) $x \equiv y\ (\mathrm{rmod}\ r_i) for i = 1, 2, \cdots, s$ if and only if $x \equiv y\ (\mathrm{rmod}\ [r_1, r_2, \cdots, r_s])$.

Proof:

1) We have $ax \equiv ay\ \mathrm{rmod}\ r$, by the definition of the real modulo we get, $\frac{ax-ay}{r} \in \mathbb{Z}$. Hence,

$$\frac{a}{\mathrm{rgcd(a,r)}}(y-x) = \frac{r}{\mathrm{rgcd(a,r)}}k, \text{for some integer } k$$

and thus, $\frac{r}{\mathrm{rgcd}(a,r)}$ is ZRL-divisor of $\frac{a}{\mathrm{rgcd(a,r)}}(y-x)$. But, by theorem (1)–(5) second assertion, we have

$$\mathrm{rgcd}\left(\frac{a}{\mathrm{rgcd}(a,r)}, \frac{r}{\mathrm{rgcd}(a,r)}\right) = 1.$$

And by using proposition (7), we get that $\frac{r}{\mathrm{rgcd}(a,r)}$ is ZRL-divisor of $(x-y)$. This implies

$$x \equiv y\ \left(\mathrm{rmod}\ \frac{r}{\mathrm{rgcd}(a,r)}\right).$$

To prove the other direction, we have $x \equiv y\ \left(\mathrm{rmod}\ \frac{r}{\mathrm{rgcd}(a,r)}\right)$, we can multiply by a to get $ax \equiv ay\ \left(\mathrm{rmod}\ \frac{ar}{\mathrm{rgcd}(a,r)}\right)$ by using theorem (2)–(6iii). But $\mathrm{rgcd}(a,r)$ is a ZRL-divisor of a, so that we can write $ax \equiv ay\ \mathrm{rmod}\ r$ by using (2)–(6iv).

2) If $x \equiv y\ (\mathrm{rmod}\ r_i)$ for $i = 1, 2, \cdots, s$ then r_i is a ZRL-divisor of $x - y$ for $i = 1, 2, \cdots, s$. That is $x - y$ is a common real multiple of $r_1, r_2, \cdots, r_s$, by using proposition (6) we get that $[r_1, r_2, \cdots, r_s]_{\mathbb{R}}$ is a real divisor, and more specific is a ZRL-divisor of $x-y$. And this implies $x \equiv y\ (\mathrm{rmod}\ [r_1, r_2, \cdots, r_s]_{\mathbb{R}})$.
From the other side, if $x \equiv y\ (\mathrm{rmod}\ [r_1, r_2, \cdots, r_s]_{\mathbb{R}})$ then by theorem (2)–(6v) $x \equiv y\ (\mathrm{rmod}\ r_i)$ since r_i is ZRL-divisor of $[r_1, r_2, \cdots, r_s]_{\mathbb{R}}$).

■

The modification to Diffie-Hellman that we want to introduce in the next section does not depend on the prime numbers and their relatives. For this reason we do not need to go deep analyzing into the topic of the prime numbers and the relatively prime numbers. We see that it is enough for the time being to propose only their extended definitions in this research. But from our observations, we can conclude the next statement. It is still not proved yet, so we introduce it as a conjecture.

Conjecture 1: Let a and b be real numbers. Let $a < b$, If $\mathrm{rl}(a) = \infty$ and/or $\mathrm{rl}(b) = \infty$ then either $\mathrm{rgcd}(a,b) = a$ or a and b are real relatively prime.

C. The Solution of the Real Congruence Equation

As we extend the definitions and the theorems that related to the congruence so that it can be applied on the set of the real numbers with some specific conditions, we must now introduce the extended method of solving the real congruence equation. The solution of the real congruence equation does not differ much from the solution of the integer congruence.

Let $f(x)$ denote a polynomial with real coefficients, and we will write,

$$f(x) = r_1x^n + r_2x^{n-1} + \cdots + r_n. \tag{8}$$

If u is a real number such that,

$$f(u) \equiv 0\ \mathrm{rmod}\ d \tag{9}$$

then we say that u is a solution of the congruence

$$f(x) \equiv 0\ \mathrm{rmod}\ d \tag{10}$$

Definition 13: Let $s_i \in [0, d)$ denote the complete canonical residue system real modulo d. The number of the solutions of $f(x) \equiv 0\ \mathrm{rmod}\ d$ is the number of the s_i such that $f(s_i) \equiv 0\ \mathrm{rmod}\ d$.

Proposition 12: The number of the solutions of $f(x) \equiv 0\ \mathrm{rmod}\ d$ is uncountable.

Proof: The argument of the proof is as follows. Consider definitions (13) and (11), we have $s_i \in [0, d)$ is a complete canonical real residue system for the $b \equiv s_i \pmod{d}$. Thus the number of the number of the solutions is uncountable because it is depending on the interval $[0, d)$ which is uncountable.

■

Example 1: The real congruence $x^2 - 3.6784161x + 0.00558882072 \equiv 0 \bmod 0.164$ *has the solution* $x = 0.00152$ *and also the solution* $x = 3.6768961$ *and all the numbers that can be obtained by adding or subtracting* 0.164.

The important note here, if the real length of the solution of the polynomial is infinity, then there is no solution to the real congruence equation.

Example 2: The real congruence $x^2 + x - 8.325 \equiv 0 \pmod{0.164}$ *has no solution because,* $\text{rl}\left(\frac{-1+\sqrt{1+4(8.325)}}{2}\right) = \infty$.

III. Modified Diffie-Hellman Protocol

We all know that Diffie-Hellman key exchange protocol depend on agreement between the partners on two values s and p, where p is a large prime number, and s integer number less than p. As a first step in real modulus is that we will introduce another number, a secret agreement between Alice and Bob but this number will be decimal number. Let it be d, $d \in (0, 1)$, and then each of the two partners (A, B) pick a random number (R_A, R_B) and then each of them computes the required equations of Diffie-Hellman scheme:

$$Y_A = s^{R_A} \bmod p \quad \text{and} \quad Y_B = s^{R_B} \bmod p$$

Now, each of them submits his value to his partner and each of them should do the last computation related to the classic Diffie-Hellman scheme to get what we call *the initial value for the secret key*. So for the partners A and B will get

$$g_A = Y_B^{R_A} \bmod p \quad \text{and} \quad g_B = Y_A^{R_B} \bmod p; \tag{11}$$

respectively, where $g_A = g_B$, is an integer number.

Now the two partners A and B should do the last computation by using the real modulus to get the shared secret key as a secure real numbers:

$$g_{AB} = (g_A)^d (\text{rmod } d), \tag{12}$$

and

$$g_{AB} = (g_B)^d (\text{rmod } d) \tag{13}$$

respectively.

Example 3: Let A *and* B *be the partners.*

A	B
Agree for $s = 16, p = 41, d = 0.375816173$	
pick $R_A = 6$	pick $R_B = 3$
$Y_A = 16^6 \bmod 41 = 37$	$Y_B = 16^3 \bmod 41 = 23$
Submit Y_A to B	Submit Y_B to A
$g_A = 23^6 \bmod 41 = 18$	$g_B = 37^3 \bmod 41 = 18$
$g_{AB} = (18)^{0.37581673} \pmod{0.37581673}$ =0.332424507	$g_{AB} = (18)^{0.37581673} \pmod{0.37581673}$ =0.332424507

The Solution of the Real congruence in Modified Diffie-Hellman protocol is exist but it is not unique. Lets consider equation (12) or (13). The number g_A or g_B is unknown integer number, received from Diffie-Hellman protocol which g_{AB} and d are unknown decimal numbers.

As we saw in the previous section, solving real modulus equation is no different from solving modulus equation, except that the real modulus equation is more complicated because the numbers belong to uncountable sets. The proposition (12) shows us that the set of the solutions belong to uncountable interval of numbers.

The advantage of using the real numbers here is that the equations of the modified Diffie-Hellman protocol are nonlinear equations. Mostly, the real length of any solution for the nonlinear equation in this modification is infinity. If the real length is infinity then there is no solution to the real congruence equations that are related to the nonlinear equation, as we saw in example (2).

IV. Conclusion

The main reason to go through this research was to modify Diffie-Hellman protocol to make it work on real numbers and more specifically on the decimal numbers. The main step of the modification depends on using the modulo on the real numbers. We could not implement the modulo on the real numbers without studying and analyzing the theory of the congruence on the real numbers.

The sub section (II-A), is the extended theory of the greatest common divisor. In this section we redefine the greatest common divisor, definition (4). This definition needs to define new term which it is the length of the real number, definition (1) and redefine the divisor, and this produce two definitions, namely, the real divisor, definition (2) and the ZRL-divisor, definition (3). The meaning of "not a divisor" has changed in this extension and redefined, definition (2). As we know in the topic of the divisibility on the integer numbers, there are always a finite number of divisors for every integer number except the zero, moreover, all the divisors should be less than the number itself. When we extend this topic to the set of the real numbers, we found that there are infinitely many divisors for every real number and the divisors could be greater than the number itself. We could extend most of the theorems from the set of integer numbers to the set of real numbers. We proved most of the theorems

that we illustrated in this section except. New properties of the greatest common divisor was added in theorem (1).

Sub section (II-B) is extended the theory congruence. We covered the properties of the real congruent in theorem (2), and we introduced the proofs for most of the properties. We discussed the solution of the real congruence equation. The definitions (9), (10) and (11) highlight important result about the unaccountability and this was introduced and proved in proposition (12).

The modification of Diffie-Hellman protocol is introduced in section (III). The steps of the modification depend on two points. The first point is the secret agrement among the partners on the decimal number. The second point is using the real congruent to calculate the sharing secret key, Equations (12) and (13). All the numbers in the modified Diffie-Hellman protocol are unknown numbers.

ACKNOWLEDGMENT

The authors would like to thank the Institute for Mathematical Research, University Putra Malaysia for the supporting to accomplish this research.

REFERENCES

[1] Burton, D. M. The Theory of Congruences. In *Elementary Number Theory*, 4th ed. Boston, MA: Allyn and Bacon, pp. 80–105, 1989.
[2] Conway, J. H. and Guy, R. K. Arithmetic Modulo. In *The Book of Numbers*. New York: Springer-Verlag, pp. 130–132, 1996.
[3] Cormen, T. H., Leiserson, C. E., Rivest, R. and Stein, C. Greatest common divisor. In *Introduction to Algorithms*, MIT Press and McGraw-Hill, 2nd edn., pp. 856–862, 2001.
[4] Diffie, W. and Hellman, M. *New Directions in Cryptography*. IEEE Transactions on Information Theory IT-22: pp. 472–492, 1976.
[5] Hejhal, D. A., Friedman, J., Gutzwiller, M. C. and Odlyzko, A. M. *Emerging Applications of Number Theory*. New York: Springer. 2nd edn., 1999.
[6] Hrbacek, K. and Jech, T. Finite, Countable, and Uncountable Sets. In *Introduction to Set Theory*. New York, 3rd edn., pp. 65–93. 1999.
[7] Gilbert, J. and Gilbert, L. *Elements of Modern Algebra*. 6th ed. Thomson, brooks/cole, pp. 57–117, 2005.
[8] Nagell, T. Theory of Congruences. In *Introduction to Number Theory*. New York: Wiley, pp. 68–131, 1951.
[9] Niven, I. and Zuckerman, H. S. *An Introduction to the Theory of Numbers*. New York: John Wiley and Sons. 4th edn., 1980.
[10] Rand Alfaris. Modified Diffie-Hellman Protocol. In *A New Decimal Cryptosystem Based on Decimal Numbers*. Ph.D. Thesis, University Putra Malaysia, pp. 55–81, 2008.
[11] Rand Alfaris, Muhamad Rezal Kamel Ariffin and Mohamed Rushdan Md Said. *Rounding Theorem the Possibility of Applying Cryptosystems on Decimal Numbers*. Journal of Mathematics and Statistics, Vol. 4(1), pp. 15–20, 2008.
[12] Séroul, R. Congruences. In *Programming for Mathematicians*. Berlin: Springer-Verlag, pp. 11–12, 2000.

Rand Alfaris Doctor of Philosophy (2008), in Pure Mathematics/Number theory/Cryptography. Institute for Mathematical Research- University Putra Malaysia.

Publications:

Rand Alfaris, Ariffin, M. and Said, M. (2008). Rounding Theorem-The Possibility of Applying the Cryptosystems on Decimal numbers. Journal of Mathematics and Statistics, Science Publications, New York, USA. 4 (1): 15-20.

Rand Alfaris and Shajaran Khan. (2008). Sine Square Distribution- A New Statistical Model Based on the Sine Function. Journal of Applied Probability and Statistics (JAPS), Montgomery, USA. 3(1): 163-173.

The Security of the Decimal Cryptosystem (Submitted).

Awards:

Bronze medal in exhibition of RMC-Malaysia 2006.
Silver Medal in exhibition of RMC-Malaysia 2008.