INFORMATION SECURITY ON THE COMMUNICATION NETWORK IN NIGERIA BASED ON DIGITAL SIGNATURE

O. S. Adebayo (MCPN), V. O. Waziri (PhD) and J.A Ojeniyi (MNCS)
Cyber Security Science department, Federal University of Technology Minna, Nigeria
waleadebayo@futminna.edu.ng, onomzavictor@gmail.com, ojeniyijoseph@yahoo.co.uk

S. A. Bashir (MNCS)
Computer Science department, Federal University of Technology Minna, Nigeria
basirsulaiman@futminna.edu.ng
Amit Mishra
Mathematics and Computer Science department, IBB University, Lapai, Nigeria
i.amitmishra@gmail.com

Abstract - This paper presents simple abstraction concepts for some digital signature scheme algorithms that include ElGamal Signature scheme, Schnorr Signature scheme, Elliptic Curve Signature (ECS), and Digital Signature Standard (DSA). It also examines the security of this digital signature scheme to measure its effectiveness and improve on the variability. The algorithms are essential in securing application in dispatching the documents on the communication network. We try to explain the algorithms in simple form and the examples are experimented in C++ programming language which presupposing little or easy mathematical background comprehension and easy computations.

Keywords - ElGamal Signature scheme, Signature Scheme, Elliptic Curve Signature, Information Security, Digital Signature

I. INTRODUCTION

Information security has become a serious concern in disseminating secured data over the Internet. One of the great advantages of Internet is the transmission of message and data on the Internet. However, these pretty pieces of data and some worthy information can be intercepted by the enemies, read and modified which invalidate the originality and authenticity of the document. A document sending to a particular destination can also be forged in one way or the other, which could undermine the essence of the message. Digital signature has therefore, become a necessary tool to sign an on line's messages electronically and authenticate the originality of its document in order to identify the identity of the sender and check the activities of hackers. A signature (binary construed) is used in everyday situations such as writing a letter, withdrawing money from a bank, signing a contract, etc.

Digital signature is a signature scheme of signing a message stored in electronic form [1] as against the "Conventional" handwritten signature attached to a paper document used to specify a person responsible for the signature. A signed message over the Internet can be transmitted over a computer and other communication network systems. In signing an electronic message, an algorithm that is used to sign the message must "bind" the signature to the message as against the conventional signature, where a signature is part of physical data or Information.

The problem of signing an online message is in two categories. The first problem is the problem of signing a document while the second problem is that of verification. A conventional signature could be easily verified by simply compared with the original or authentic signature. For example, a customer paycheck could be verified by a cashier by comparing the signature on the check with the original one in the bank for verification. Digital signature, on the other hand requires publicly known verification algorithm, thus a digital signature can be verified by anybody and therefore, a need to use a secure signature scheme in order to prevent the possibility of forgeries and abdication by intruders.

The major challenge associated with digital signature is its feature of reused. A copy of digital message is identical to the original and can be easily reused by anybody. For example, if Ade authorizing Ola to withdraw certain amount of money from his account, in order to prevent Ade from withdrawing the amount several time, the digital message should contain certain information, such as date in order to prevent it from being reused.

Digital signature scheme has two important components; namely, Signing and Verification algorithms. Message x that is signed by Ade using a signature algorithm Sigk, which depends on his private key can be verified by

Corresponding Author: **Olawale Surajudeen Adebayo (MCPN, MNCS)**

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Ola using a publicly known verification algorithm Verk. Consider a pair (x, y) where x is a message and y indicate a signature on a message x, then the resulting verification algorithm Verk x = y is true if a message x has been validly signed and y = Verk; x is false if x is a forged signature or not previously signed.

This paper examines various signature schemes algorithms that are being used on the insecure Internet to sign a message electronically (that is, signing and verification algorithm). The security requirements of the scheme are also highlighted. The rest of the paper is as follows: In section 2 deals with related literatures review, section 3 emphasizes on the methods for the sampled modern public key infrastructure (PKI); while section 4 deals with experimental performance of the stipulated algorithms in section 4, and finally in section 5, we present some fundamental suggestions for future research works.

II. RELATED WORK

The notion of digital signature exists as a result of quest to reduce or eradicate the spate digital data forgery on the insecure communication network. To this end, [5] developed an algorithm known as ElGamal signature scheme, which is non-deterministic. This implies that for any given message x, there exist many valid signatures Y as a vector and a message can be signed with varied private keys while the verification can be done using the public key algorithm. This algorithmic process is known as the public Key cryptographic infrastructure.

The National Institute of Standard and Technology (NIST), [7] would later modified the ElGamal signature scheme and produced another algorithm known as Digital signature scheme, Today, the vulnerability of the communication network is pervasive and required high security attentions, which necessitates the use of a large modulus p (a prime number that is one of the public keys used to verify signed message). This was brought about the development of variants of ElGamal signature scheme. All the variants adopted the use of 2048 bits, which is effective for powerful application like smart card and biometric machine as against the 1024 bit modulus p used in ElGamal signature. [4] proposed another variant of ElGamal signature scheme, which reduces greatly the size of the signature.

[2] proposed Digital Signature Algorithm (DSA), which is another modification of the ElGamal signature scheme, adopts some ideas used in Schnorr signature scheme in order to increase the security of the signature. In order to present to a layman in a simplest form the idea of encryption and decryption [6] illustrated how cryptography could be used to enhance security on the internet. On the other hand, the idea of decrypting ciphertext without the knowledge of encryption was presented by [3] where they presented differential cryptanalysis of DES like cryptosystem.

III. METHODOLOGY

In this section, we present the useful sampled algorithm in these sequential orders: The two important components of Signature Scheme as mentioned earlier are signing algorithm and verification algorithm. An online message x that is signed by Ade using a signing algorithm, with his private key can be in order way round verified by Ola with a verification algorithm using a public key.

The Signature Scheme that is being used on the Internet as a product of cryptosystem, with its signing and verification algorithm in order to secure and protect information from sender to a destination is given by the generic definition:

A Signature Scheme is a five-tuple (P, A, K, S, V), where each notation is given below.

P: is a finite set of possible messages

A: is a finite set of signatures

K: the keyspace is a finite set of possible keys

For each k Є K, there is signing algorithm Sig_k Є S, and a corresponding verification algorithm Ver_k Є V. Each Sig_k: P → A, and Ver_k: P x A → (true, false) are functions such that the following verification algorithm are satisfied for message x Є P and signature y Є A on the message

$$Ver\ (x,y) = \begin{cases} true\ if\ y = Sigk \\ false\ if\ y \neq Sigk \end{cases}$$

Where a pair (x, y) with x Є P and y Є S is called a signed message

IV. THE ELGAMAL SIGNATURE SCHEME

The ElGamal signature algorithm was presented by [5] in order to sign an online message x by Ade and sent across the network to a second person Ola for verification and authentication. According to ElGamal, Ade signs the message x with his secrete random number k and private key a, which is only known to him, while Ola can verify the authenticity of the message x by using the public key p, α, and β. The ElGamal signature scheme is a non-deterministic algorithm where the verification algorithm is able to accept as many valid signatures as possible for any given message.

Let us examine the message x sent from Ade to Ola over an insecure communication network. The desire of Ade is to send the message safely over the network without any interception or disruption by intruders. However, a message sent over a communication network can be intercepted, examined, and modified due to the insecure nature of this network. Thus the problem of making a message authentic by signing it and subjecting it to verification electronically was developed by ElGamal. He designed a signature algorithm Sig_k (x, k) for Ade, that can be used sign message x, with his private key (a) and secret number (k), and verification algorithm Ver_k (x, (γ, δ)) in order to ascertain the authenticity and originality of the message x from Ade.

Corresponding Author: **Olawale Surajudeen Adebayo (MCPN, MNCS)**

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The algorithmic sequence of the **ElGamal Signature Scheme** is given as follow:

Given that p is a prime over Zp where p = Zp*, A = Zp* x Zp-1, and
K = {(p,α,a,β); $\beta \equiv \alpha^a \pmod p$},

where the values p, α, and β large prime number, public key, and private key trspectively. The values P, A, Zp are as defined previously.

The signature Sig_k (x, k) = (γ, δ) (1)
where
$$\gamma = \alpha^k \pmod p \quad (2)$$
and
$$\delta = (x - a\gamma)\, k^{-1} \bmod p\text{-}1 \quad (3)$$

k here is a (secret) random number used by Ade to sign the signature.

For x, γ ∈ Zp and δ ∈ Zp-1, the verification of the algorithm is given as

$$Ver_k (x, (\gamma, \delta)) = True \Leftrightarrow$$
$$\beta^{\gamma}\gamma^{\delta} = \alpha^x \pmod p \quad (4)$$

It is worthwhile to note that if the signature was constructed correctly, then the verification will succeed, since
$\beta^{\gamma}\gamma^{\delta} = \alpha^{a\gamma}\, \alpha^{k\delta} \pmod p \equiv \alpha^x \pmod p$ (5)

Using the fact that
$$a\gamma + k\delta = x \pmod{p-1}$$

The verification can be accomplished by using only public information.

V. VARIANT OF ELGAMAL SIGNATURE SCHEME

Various challenges characterize the ElGamal signature scheme and these range from authentication to privacy issues. The categories of Signature scheme, which are modification of the ElGamal Signature Scheme, were developed. Among these are Digital signature Scheme, Schnorr Signature Scheme, Elliptic curve Signature Scheme to mention a few. Due to the security requirement of signature scheme, various changes were made to ElGamal signature. It is highly imperative to be cautious regarding the security of a signature scheme, in which a signed message could perform a vital financial and legal transaction as opposed to a cryptosystem where a message might be encrypted and decrypted only once using any cryptosystem which is known to be secure at the time the message is being encrypted. Again, a signed message is very likely to be verified over a period of time after the message has been signed.

Since the **ElGamal Scheme** is no more secure than the **Discrete Logarithm** problem, this necessitates the use of a large modulus *p, which* should have at least 512 bits and the length of *p* should be 1024 bits in order to provide security into the foreseeable future. However, for potential applications, such as smart cards application among others, a shorter signature is desirable.

A. The Schnnor Signature Scheme

[9] proposed a signature scheme in which the size of the signature is greatly reduced. Schnorr proposed that suppose that p and q are primes such that $p\text{-}1 \equiv 0 \pmod q$, where p is taking as 2^{1024} and q is approximately 2^{160}. It modifies the ElGamal signature so that a $\log_2$ q-bit-message digest is signed using a $2\log_2$ q-bit signature, while the computations are done in the Zp. The Signature scheme is assumed secured based on the fact that the discrete logarithm specified in subgroup of set of prime closure (Z_p^*) is more secured. The α which is one of the public key use in verifying signed message is taking as qth root of 1 mod p i.e. $\sqrt[q]{1 \bmod p}$.

The algorithm of Schnorr Signature Scheme is described below:

Given that p is a large prime number such that the discrete log problem in Z_p^* is intractable, and q is a prime that divides p-1. Then the followings are in order by definitions:

$\alpha = \sqrt[q]{1 \bmod p}$,
p = {o.1}*,
A = Zq x Zq, and
K = {(p, q, α, a, β): $\beta \equiv \alpha^a \pmod p$}
where

$0 \le a \le q\text{-}1$, p,q,α and β are the public key, and a is the private key.

For K = (p, q, α, a, β), and for a secret key k, $1 \le k \le q\text{-}1$,
$Sig_k (x, k) = (\gamma, \delta)$
where
$\gamma = h(x \,\|\, \alpha^k \pmod p)$ and
$\delta = k + a\gamma \bmod p$
For x∈ {0,1}*, and γ,δ ∈ Zq, the signature can be verified through the following algorithmic process:
$Ver_k (x, (\gamma, \delta)) = True \Leftrightarrow h(x \,\|\, \alpha^{\delta}\beta^{-\gamma} \pmod p) = \gamma$

A. The Digital Signature Standard (DSA)

The Digital signature Algorithm, 1994 (DSA) proposed by [2] is another modification of ElGalma Signature Scheme, which incorporates some characteristics of Schnorr Algorithm. The DSA was first published in the

Corresponding Author: **Olawale Surajudeen Adebayo (MCPN, MNCS)**

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Federal Register in May 19, 1994 and was finally adopted as a standard on December 1, 1994. D**SS** modifies the **ElGamal Scheme** in an ingenious way so that a 160-bit message is signed using a 320-bit signature, but the computations are done using a 512-bit modulus *p*. However, due to the criticisms from various quarters over the fixing of prime p value as 512-bits, the NIST altered the description of the standard and various modulus sizes can b e used. The first change made is by changing the "-" to a "+" in equation 3 above, so that δ becomes

$\delta = (x + a\gamma)\, k^{-1} \bmod (p-1)$ (6)

This changes the verification condition to the following:

$\alpha^{x}\beta^{\gamma} \equiv \gamma^{\delta} \pmod p$ (7)

If gcd $(x+a\gamma, p-1) = 1$, then $\delta^{-1} \bmod (p-1)$ exists, and the equation (7) becomes:

$\alpha^{x\delta-1}\beta^{\gamma\delta-1} \equiv \gamma \pmod p$ (8). Also, the message x in DSA should be hashed using SHA-1 before it is signed with a 320-bit signature over 160-bit message digest.

B. The Elliptic Curve DSA (ECDSA)

The Elliptic Curve Digital Signature Scheme as discussed by [11] and [12] is a modification of the Digital Signature Algorithm (DSA) to the setting of elliptic curves. There are two points P and Q on the elliptic curves, which are define over Zp for some given prime number p. The private key of ECDSA is the discrete logarithm value $m = \log_A B$. In order to compute and verify a signature in this ECDSA, a (secret) number k is chosen randomly and the value of kA is computed.

Let p be a prime and E be an elliptic curve defined over Fp. Let A be a point on E having prime order q, such that the Discrete Logarithm problem in A is infeasible. Let

$P = \{0,1\}^*$, $A = Zq^* \times Zq^*$, and define

$K = \{(p, q, E, A, m, B) : B = mA\}$,

Where $0 \le m \le q-1$. The value p, q, E, A and B are the public key, and m is the private key.

For a finite set of possible keys (keyspace), K and a (secret) random number k, $1 \le k \le q-1$,

$Sig_k(x, k) = (r, s)$,

where

$kA = (u, v)$

$r = u \bmod q$

$s = k^{-1}(SHA\text{-}1(x) + mr) \bmod q$

note: if either r or s = 0, then the new value of should be selected.

For all $x \in \{0, 1\}^*$ and $r, s \in Zq^*$, verification $Ver_k(x, (r, s))$ = true if and only if $u \bmod q = r$

Where $w = s^{-1} \bmod q$

$i = wSHA\text{-}1(x) \bmod q$

$j = wr \bmod q$

$(u, v) = iA + jB$

VI. MANUAL EXPERIMENTATIONS

These are some arithmetic examples and practical experiment based on the research work as stated as the examples depicted below:

A. Example (ElGamal Signature Scheme)

Suppose we take $p = 467$, $\alpha = 4$, $a = 101$, we wish to verify the signature of Ade on a message x = 100 and his (secrete) random key, k = 213 and whether Ola should accept this signature; then

We compute:

$\beta = \alpha^{a} \pmod p = 4^{101} \pmod{467} = 449$

$\gamma = \alpha^{k} \pmod p = 4^{213} \pmod{467} = 374$

Suppose further that Ade chooses the random value k = 213, it is noted that great common divisor gcd(213, 466) = 1 and 213-1 mod 466 = 431

hence,

$\delta = (x - a\gamma)\, k^{-1} \bmod p\text{-}1 = (100 - 374 * 101) * 431 \bmod 466$
$= (100 - 37774) * 431 \bmod 466 = -37674 * 431 \bmod 466 = -16237494 \bmod 466 = -190 + 466 = 276$

The computational analysis yields:

$\delta = 276$, $\gamma = 374$

The signature 100 can therefore be verified by Ola or anyone by checking whether congruent $\beta^{\gamma}\gamma^{\delta} = \alpha^{x} \pmod p$ i.e

$\beta = 449$, $\delta = 276$, $\gamma = 374$, $x = 100$, $p = 467$ and $\alpha = 4$
then,

$449^{374}374^{276} = 4^{100} \bmod 467 = 229 \bmod 467$

This implies that the signature of Ade is valid and can be accepted by Ola or anyone that the message is sent to receive. Otherwise the signature should be rejected.

B. Example (DSA)

Suppose Ade uses DSA with q = 101, p = 7879, α = 170, a = 75 and β = 4567. We wish to determine Ade's signature on a message x such that SHA-1(x) = 52, using a random value k = 49 and find out whether the signature is authentic or forged.

Note: The value p, q, α, β, a, are as defined previously in the signature algorithm

Corresponding Author: **Olawale Surajudeen Adebayo (MCPN, MNCS)**

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Solution

Given that q = 101, p = 7879, α = 170, β = 4567, a = 75, SHA-1 (x) = 52, k = 49

The first step is to determine the signature of Ade on the message x by computing the following:

$\gamma = \alpha^k \pmod p \bmod q$ (2)

$= 170^{43} \bmod 7879 \bmod 101 = 85$

$\delta = (\text{SHA-1}(x) + a\gamma)\, k^{-1} \bmod q \bmod q$

$= (52 + 49 * 85)\, 49^{-1} \bmod 101 \bmod 101 = 84$

The signature (85, 84) of Ade can therefore be verified by computing the following:

$\delta^{-1} = k^{-1} \bmod q = 49^{-1} \bmod 101 = 33$

$e_1 = \text{SHA-1}(x)\, \delta^{-1} \bmod q$

$= 52 * 33 \bmod 101 = 100$

$e_2 = \gamma\delta^{-1} \bmod q$

$= 85 * 33 \bmod 101 = 2805 \bmod 101 = 78$

and

$\text{Ver}_k(x, (\gamma, \delta)) = \text{true} \Leftrightarrow \alpha^{e1}\beta^{e2} \bmod p \bmod q$

$\Rightarrow \quad 170^{100}4567^{78} \bmod 7879 \bmod 101 = 85$

Therefore the signature (85, 84) on message 100 should be accepted by Ade.

C. Example (Schnnor Signature)

Given that q = 101, p = 88q + 1 = 7879 where 3 is a primitive element in Z_{7879}, we want to verify the signature of Ade on a message x = 50, while he chooses random value k as 50 and a = 75 where all the values are as defined earlier. Then, we compute:

$\alpha = 3^{88} \bmod 7879 = 484$

but α is a qth root of 1 modulo p. then

$\beta = \alpha^a \bmod 7879 = 484^{75} \bmod 7879 = 4448$ and

$\alpha^k \bmod p = 484^{50} \bmod 7879 = 3764$

we can therefore compute the hash function h(x ‖ 3764) on a message x where 3746 is represented in binary (as a bit string). Thus

$h(x \,\|\, 3764) = 97$ and

$\delta = 50 + 75 * 97 \bmod 7879 = 53$

and the signature $(\gamma, \delta) = (97, 53)$

The signature can therefore be verified by computing and comparing the following:

$\text{Ver}_k(x, (\gamma, \delta)) = \text{True} \Leftrightarrow h(x \,\|\, \alpha^{\delta}\beta^{-\gamma} \pmod p) = \gamma$

$\Rightarrow \quad 484^{53}4448^{-97} \bmod 7879 \neq \gamma$

The signature (97, 53) therefore cannot be verified on a message 50 over a given secrete key 75.

D. xample (Elliptic Curve Signature)

Consider the following elliptic curve $y^2 = x^3 + x + 6$, defined over Z_{11} with p = 11, q = 13, m = 23 A = (2, 7) and B = (2, 7), x with SHA-1 (x) = 6, k = 5. We wish to verify whether a given signature (r, s) should be accepted or rejected.

Solution

We need to compute the following:

$(u, v) = 5\,(2, 7) = (3, 6)$

that is,

$(u, v) = iA + jB$

$r = u \bmod q = 3 \bmod 13 = 3$

$s = k^{-1}\text{SHA-1}(x) + mr) \bmod q$

$= 5^{-1}\,(6 + 23 * 3) \bmod 13 = 15 \bmod 13 = 2$

$w = s^{-1} \bmod q = 2^{-1} \bmod 13 = 7$

$i = w\text{SHA-1}(x) \bmod q = 7 * 6 \bmod 13 = 3$

$j = wr \bmod q = 7 * 3 \bmod 13 = 8$

Signatue (r, s) = (3, 2)

To verify the signature:

$\text{Ver}_k(x, (r, s)) = \text{true}$ if and only if $u \bmod q = r$

that is,

$u \bmod q = 3 \bmod 13 = 3.$

Hence, the signature is accepted

VII. REPORT ON THEORETICAL WORKED EXAMPLES

The first theoretical example on Elgamal signature where the left hand side equation is equivalent to the right hand side i.e. $449^{374}374^{276} = 4^{100} \bmod 467 = 229 \bmod 46$, shows that the signature of Ade is valid and can be accepted by Ola or anyone. Otherwise the signature should be rejected. Also, the second example on DSA signature scheme where $170^{100}4567^{78} \bmod 7879 \bmod 101 = 85$ signified that the signature (85, 84) on message 100 is valid and should be accepted by Ade. However, the signature (97, 53) example of the schnnor signature example over a message 50 cannot be verified and therefore be rejected. The last example of elliptic curve signature also illustrates that the signature can be verified over an elliptic curve and since the calculated value of u mod q = r, then the signature should be accepted.

VIII. AUTOMATA EXPERIMENTS BASED ON C++

This section computes the various problems above using the equivalent algorithm:

Initialize the variable L,M,N,P;
Initialize variable A,B,R,a,K,X,Y,T,S as float
Collect the value of modulus P
Collect the value of primitive element A
Collect the value of value of B
Calculate a = (log(B))/(log(A))
Display the private key a
Collect the value of R
Display R
Collect the value of value of S
Calculate K = (log(R))/(log(A));
Collect the value of of K
Collect the value of message X

Corresponding Author: **Olawale Surajudeen Adebayo (MCPN, MNCS)**

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

```
        Display the verification details
         L = pow (B,R);
        M = pow (R,S);
         N = pow (A,X);
        If ((L*M)%P==N%P){ Then
        Display the signature is true
        Else display the signature is false
         Display the verification is complete
 return 0
End
```

A. Security Requirements for Signature Scheme

In order to make digital signature a reliable algorithm, it is highly essential for the algorithm to be logically "secured" in order to prevent various forms of attack from adversaries. This section examines the goal of an adversary, attack models and the security provided by signature scheme. Some possible attack models against digital signature are here under-listed:

i) Known message attack: This attack occurs when adversary possesses a list of messages previously signed by his host, i.e. (x1, x2,)… (xn, yn) where xi's are random messages of Ade and yi's are his signatures on the messages so that yi = Sigk (xi), I = 1, 2, 3….

ii) Key- only attack: This is a vulnerable situation where public key of Ade is in the possession of adversary.

iii) Total break: occurs when adversary is able to determine the private key of signer Ade and create valid signature on any message over signature function Sig_k.

iv) Selective forgery where adversary is able to create a valid signature on a chosen message based on some probabilistic functions.

v) Existential forgery: Adversary is able to create valid signature for at least one message on a pair (x, y), where x is a message, y is a signature and Verk (x, y) = true while message x has not been previously signed.

IX. SECURITY ISSUES IN ELGAMAL SIGNATURE SCHEME

It is worthwhile in signature schemes to note that a message x signed and sent by Ade can be forged by another party. Suppose Ola attempt to forge a signature of Ade on a message x, without knowing the value of his private key a, he can choose the value γ and try to compute the corresponding δ, however, doing this require him to compute the discrete logarithm log $\alpha^x\beta^{-\gamma}$, which may be a little bit impossible. Alternatively, he can choose δ and compute γ, by solving the equation $\beta^{\gamma}\gamma^{\delta} \equiv \alpha^x \pmod p$. The implication of this is that for any unknown value γ or δ, presently there is no feasible known solution. However, this is not sufficient to conclude that the value of signature (γ, δ) cannot be computed.

In another way round, if an adversary chooses γ and δ and attempt to find the value of message x, solving an instances of discrete logarithm problem became another challenge i.e. computing the value $\log_{\alpha}\beta^{\gamma}\gamma^{\delta}$. However, if an adversary can choose γ, δ and random message x simultaneously, then he can perform what is known as existential forgery, where he can create one signature for at least one random message x while x has not previously being signed. i.e. Ver k (x, y) = true where the message x has not been previously signed.

Summarily, the (secret) random value k used in computing the signature should be concealed because if k is known, an adversary can compute a private key $a = (x - k\delta)\ \gamma^{-1} \bmod p-1$. Also, k must not be used to sign two different message x.

X. FUTURE RESEARCH WORKS

In order to design a very secure signature algorithm, it is highly recommended that the (secret) random value k used in computing the signature should be concealed because if k is known, an adversary can compute a private key $a = (x - k\delta)\ \gamma^{-1} \bmod p-1$. Also, k must not be used to sign two different message x.

XI. DISCUSSION AND CONCLUSION

This paper has presented and examined various signature scheme algorithms with a view to simplify its complex mathematical aspect for a layman understanding. The signature scheme since its existence has became a veritable tool in securing the information on the Internet. However, it is quite notable that an information security is a continuous exercise that is subjecting to empirical analysis. The algorithms implemented in C++ programming language basically for better understanding and easier computation of perceived difficult aspects of cryptology.

Anybody can therefore; lay his hand on the implementation and compute the equivalents of various digital signature algorithms. The programming implementation also displays the speed of each of the algorithm.

XII. REFERENCES

[1] Douglas R. Stinson, "Cryptography Theory and Practice". University of Waterloo Ontario, Canada, Chapman & Hall/CRC. 2006.

[2] Menezes, A. J. and *Vanstone*, S. A., "Advances in Cryptology", volume 537 of Lecture Notes in Computer Science, Berlin, Springer, 1991.

[3] Biham E. and. Shami, A "Differential cryptanalysis of DES – like cryptosystem". *Journal of Cryptology*, 4, pp. 3-72, 1991.

[4] Schnorr, C. P. "Efficient Identification and Signatures for Smart Cards". *Proceedings of CRYPTO '89*. PP. 239 – 252.

Corresponding Author: **Olawale Surajudeen Adebayo (MCPN, MNCS)**

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

1989.

[5] ElGamal, Taher, "A public key cryptosystem and a signature scheme based on discrete logarithms". *Advances in cryptology: Proceedings of CRYPTO 84*. Lecture Notes in Computer Science. **196**. Santa Barbara, California, United States: Springer-Verlag, pp. 10–18. doi:10.1007/3-540-39568-72, 1985.

[6] Waziri, V.O "Information Security on the Internet in Nigeria with some functions of Cryptography", 10th Annual Conference proceding, Nigerian Computer Society, Nicon Luxury, Abuja, Nigeria, 2011.

[7] National Institute of Standards and Technology. Fact Sheet on Digital Signature Standard. Online, 1994. Accessible online at National Institute of Standards and Technology Website: http://www.nist.gov/public_affairs/releases/digsigst.htm.

[8] Anderson, R. "Security Engineering: A Guild to Building Dependable Distributed System", John Willy and Sons.

[9] Steinfeld R., Wang H., and Pieprzyk J., "Efficient extension of standard Schnorr / RSA signatures into universal designated-verifier signatures, Public Key Cryptography-PKC", LNCS Springer-Verlag, 2947, pp.86-100, 2004

[10] Zhang, F. and Kim, K., "A universal forgery on Araki et al. 's convertible limited verifier signature scheme", IEICE Trans. Fundamentals, ol.E86-A, 2, pp. 515-516, 2003.

[11] Hankerson, D., Menezes, A., and Vanstone, S.A., "*Guide to Elliptic Curve Cryptography"*, Springer-Verlag, 2004.

[12] Blake, I., Seroussi, G. and Smart, N., "*Elliptic Curves in Cryptography"*, London Mathematical Society 265, Cambridge University Press, 1999.

[13] Adebayo, O. S. and Waziri, V. O. "Information Security on the Communication Network in Nigeria Based on Digital Signature" In proceeding of 3rd Internation Conference on Mobile e-Services" Ladoke Akintola University, Ogbomoso, Nigeria, 25th – 27th, 2011.

AUTHORS PROFILE

Olawale Surajudeen Adebayo (MCPN, MNCS, MIACSIT) is a lecturer in the department of Cyber security science department, Federal University of Technology, Minna, Niger State Nigeria. He bagged B.Tech. in Mathematics and Computer science from Federal University of Technology, Minna and the MSc. in Computer science from University of Ilorin, Kwara state, Nigeria. He is presently a PhD student in the department of cyber Security science, Federal University of Technology, Minna.

His current research interests include: Information security, Cryptology, Machine learning, Data mining and computational intelligent. He has published some papers in the above-mentioned research areas.

He is a member of Computer Professional Registration Council of Nigeria (CPN), Nigeria Computer Society (NCS), Global Development Network, International Association of Computer Science and Information Technology and many others.

Corresponding Author: **Olawale Surajudeen Adebayo (MCPN, MNCS)**

http://sites.google.com/site/ijcsis/
ISSN 1947-5500