Volume 5, Issue 3, March 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

The Application of Hybrid Cryptographic Algorithms for Cyber Warfare and Terrorism in a Nation Defence

Victor Onomza Waziri, PhD*, John K. Alhassan, PhD, Idris Ismaila, Idris Ismaila

Department of Cyber Security Science, School of Information and Communication Technology,

Federal University of Technology, Minna, Nigeria

Abstract: ***In this paper, we present the hybrid cryptographic scheme and its application in safeguarding the dissemination of both public and commercial data in static state or in transaction, which also expedites faster computational processes. The application is derivable from the asymmetric and symmetric hybrid encryption schemes. The asymmetric schemes are number-theoretic operations which are slower than the symmetric encryption schemes that always uses block enciphers. Often, it is the desire in most encryption schemes to encrypt long messages, but with the asymmetric key only; this could pose time depletion due to its slowness in process execution. To achieve accelerated coding preeminence, it is always appropriate to use the two well-known encryptions paradigms-the Public Key Infrastructure (PKI) and the Private Key Infrastructure (Secret Key). In practice, an encoder will first encrypt her private key using therecipient's publickey, and then sends her encrypted key embeddedin her encrypted message that is encrypted withherpublic key. The recipient upon receiving the contents of the messagewill decrypt thetransmitted encryptedkey using his private key since this was encrypted with his public key;then with the decrypted private key from the sender,he decrypts the message of the sender since the sender uses her public keyto encipher the message. This process is called hybrid encryption scheme. Our proposal is to scrutinize the functionality of this encryption scheme and then apply it on our discourse of Cyberspace terrorism warfare for national security top secret advantage. We present an ingenious algorithmic cryptosystem based on encryption and decryption Oracles for the construct.***

Keywords: Hybrid Cryptosystem, Random Oracle, Adversary, Indistinguishability, Symmetric key, Hybrid encryption, Non-adaptive Chosen Ciphertext Attack, Cyberterrorism, Cybercrime

I. INTRODUCTION

Upon conceiving the desire to write a paper based-on the topic above, the ugly problem of defining Cyberterrorism started rearing its hydra heads. What is Cyberterrorism? How can it be mitigated? There is no acceptable concept as to what this concept "cyberterrorism" could be construedso as to find a lasting solution to it. There are divergent mirages of definitions that seem to capture the minds of different people and their immediate cyber terrorism experiences within their ethnic nationalities all over the world. There is a lack of documented scientific support to incorporate various aspects of computer-related crimes into the genre of "Cyberterrorism", [`19]. Like most academic Researches, targeted definitions are usually hard to come by.

Making unequivocal definition on cyberterrorism that will appear more logical and acceptable to all hard to come by for divergent parameters or attributes are in conflict of acceptance. From the categories of these attributes, a list of attributes from tradition of computers and the Internet could be considered for each acceptable opinion context. From this methodology, online world and terrorism is synthesized to produce a broader but more useful assessment of the potential impact of computer-know-how based terrorists.

In spite of all the bountiful compact observations that we have made, there is no acceptable methodology by which a given country can take uniquely steps that could mitigate the activities or Hactivism based on the nomenclature "Cyberterrorism" or "cyberwarfare" that would safeguard its cyberspace. However, despite lack of acceptable evidential documented scientific defining supports, the terms clearly exist in common usage as a product of computer security and the Internet attacks. The term "cyber terrorism" was first coined and idolized in the 1980s by Barry [24] and it has gone viral in the last several years to refer to such phrases as: "Protect yourself from Cyberterrorist"; "Insure yourself against cyberterrorism:; "Funding forthcoming to fight cyberterrorism" [19], [20].

All said and done, we still lay languished in agony of what is Cyberterrorism, thus our solution is left to our own device, the application of Cryptology as our critical infrastructure at task at fighting against cyberterrorism in our cyberspace. Note that Cryptology is a field of data security modeling that is based-on Cryptography and Cryptanalysis. To overcome political terrorism, financial terrorism and general entrepreneur terrorisms, be it in the Internet or Computing devices, all data or information that are targeted from the computing devices and the Internet should be encrypted with strong cryptographic algorithms to mitigate data security. This, however, is a tip of an iceberg when compared to other devices applied through hactivismor activisms of malware creators. This is another fertile ground that needsproactive cyber security intensive research if the hydra heads of cyber terrorisms and cyber warfare must be tackled effectively in unison to achieve some complete cyberspace security.

Cryptography is seen as the art and science of secret writing that is formed with creativity actions and entrepreneurial talent, [5], [11], [12]. Cryptography is based on some mathematical techniques that provide useful mechanisms necessary to mitigate some related security information in the areas of confidentiality, data integrity, entity authentication and data origin authentication, [11].

There are two generic cryptosystems; Symmetric and public cryptosystems. Symmetric cryptosystems provides a single key that is used as secret key between two communicants, [1] and [18].

Asymmetric algorithms known also as Public Cryptosystems generate two random values for encryption and decryption. The product of the two keys does not need to be shared between the two parties; one is retained as a private key for decryption while the other is posted out to the public. Whoever wants to communicate any secret information uses the public key to carry out his/her encryption to the recipient of the asymmetric key. The private key is used by the provider of the public key to decrypt the encrypted ciphertext. The precursors of the private-public cryptosystem are, [23]. The modern asymmetric key was revolutionized by [23] and was built upon by [5] to develop the RSA encryption scheme for cryptographic encoding that have prominence based-on its number-theoretic secure factorization assumption. The asymmetric encoding process entails that the keys set is twain in nature and that one is private while the other is public. The public key together with a cipher (function) is used for encryption; while the private key is applied in decrypting the encrypted data. Hence, using the asymmetric scheme is synonymous to using a trapdoor function in which the reversal is impossible but can only be achieved by the recipient using the private key as antithetical function.

I.I The Asymmetric Key Cryptosystem Overview

Symmetric key cryptosystem is the most feasible algorithm to create; this is based on the fact that it is extremely fast in implementation when this is compared to the asymmetric cryptosystem computational process. Despite this excellent attribute in application, the distribution of the secret key over an insure channel is the most complicated challenges over the issues ofdistribution [5], [12], and [8]

By definition [`4], a public key encryption scheme consists of 3-tuples $Asym_{key}$={Gen, Enc, Dec} is a public key encryption scheme if the following algorithms hold:

1. Gen is probabilistic Polynomial Time (PPT) algorithm: $pk, sk \leftarrow GEN(1^K)$
2. Enc is a PPT algorithm: $c \leftarrow Enc_{pk}(m)$
3. Dec is PPT algorithm: $m \leftarrow Dec_{sk}(c)$

$$\forall m \in \{0,1\}^{\bullet}, \Pr[pk, sk \leftarrow Gen(1^{|m|} : Dec_{sk}(Enc_{pk}(m)) = m] = 1,$$

We summarize the generic cryptosystem development of asymmetric cryptosystem in these three steps:

a. Let Gen_{key} represents the algorithm for the scheme. In this process, the users of the scheme run the parametric generation algorithm on some acceptable parameter $1^{|m|} \in \{0,1\}^*$ to produce two distinct keys which we symbolize as a function $f(pk, sk)$; $f(pk)$ is the public key while trapdoor is $f(sk)$ is an associated inverse permutation. In this algorithm, $f(pk)$ is the public key function that will be used for the message encryption while the function "$f(sk)$" denotes the secret key that is also known as trapdoor permutation which is applied to decrypt the encrypted message called the ciphertext.

b. A user A that will want to send a message M to user B, will carry out an encryption process using the function $C = Enc_{pk}(M)$ and sends C to B.

c. Upon getting C, B will decrypt the ciphertext C to obtain m , the plaintext, using the function $Dec_{sk}(c) = M$

Definition I.I (Secure Asymmetric Cryptosystem)

The asymmetric cryptosystem $\{Gen, Enc, Dec\}$ is said to be single message secure if for all non-uniform PPT (Polynomial Probabilistic Time) machines D, there exists a negligible function $\in$ such that $\forall n \in N$ and $m_0, m_1 \in \{0,1\}^n$, D distinguishes the following distributions with probability $D \leq \in(n)$ that satisfies:

$$\{pk, sk \leftarrow Gen(1^n) : (pk, Enc_{pk}(m_0))\}$$

The definitions of CPA, CCA1, and CCA2 for indistinguishabilities security can be extended to public cryptosystem scheme; definitions and meanings are fully established in the next subsections and section 2 that will follow. If an encryption scheme is adjudged to be single-message secure, then it is also multi-message secure. An encryption scheme with a deterministic algorithm (even with state) would not be secure because a cyberterrorist can simply encrypt the message m_0 with pk and compare the encryption of m_0 with the challenge ciphertext (which is the encryption of either m_0 and m_1.

In the subsections that follow, we review the cryptanalytic features of CPA, CCA1, CCA2 and Non-malleability of the ciphertexts under asymmetric encryption paradigm.

Involving in cryptanalytic discourse is the oracle attack that has its root in Cryptography. It is a strong weapon that the terrorist utilize to encrypt a plaintext or decrypt an encrypted data .An oracle attack analyzes each interaction with a system to extract secure data or implementation details. By choosing the plaintext or ciphertext input to an encryptor or decryptor, respectively, and analyzing the output as it relates to a chosen input, it is often possible to deduce valuable information about the algorithm or secret item information, such as one of the keys, that is being used in the algorithm.

Such vulnerability in cryptosystem is termed an "oracle" because, like a visit to an ancient Greek Oracle at Delphi, every input, or question, receives an output or answer which is left up to the observer to decide if the answer is meaningful. Hence, analyzing CPA, CCA1, and CCA2 for indistinguishability, oracle attack plays the major role describing the strength of the encryption scheme and its decryption; of the three mentioned, IND-CCA2 is the strongest against terrorism attack based on the oracle assessment.

I.I.I Indistinguishability Chosen Ciphertext Attack (IND-CCA)

In this section, we are overviewing the landscape concept of security as it is defined in modern security deportment in line with ciphertext security. This would enable us appreciate the principle of hybrid encryption schemes and their application in today's information data security against cyberterrorism, [17] .

The property of indistinguishability is some very important concept for many encryption schemes. By abstraction, a ciphertext indistinquishabibility attribute possesses the property that an adversary will be unable to differentiate the pair of ciphertexts based on the message they encrypt. For instance, the property of indisticquishability under chosen plaintext attack is considered a basic prerequisite for most precisely provably secure public key cryptosystems. Other schemes exist that provide indistinguishability under chosen plaintext attack and adaptive chosen ciphertext attack. Indistiguishability under plaintext attack is equivalent to the chattels of semantic security. Semantic security is a construct in which most cryptographic proofs are centred that was promulgated [16]. It is considered asthe weaker in cryptanalysis than the indisticguishability constructs of IND-CCA1 and IND-CCA2.

A cryptosystem is mostly considered "secure in terms of indistinguishability" if no adversary A, given an encryption of a message randomly chosen from a two-element message space determined by adversary (a computer terrorist in our case) can identify the message choice with probability significantly better than that of random guessing (1/2). If a terrorist can succeed in distinguishing the chosen ciphertext with a probability significantly greater than ½, then the terrorist is considered to have an "advantage" in distinguishing the ciphertext using his warfare tool, and the scheme is "not" considered secure in terms of indistinguishability.

This obvious definition encompasses the notion that in a secure scheme, the adversary should garner no imformation from seeing a ciphertext. It therefore obviously is a construct that the terrorist should be able to do no better than if guessed randomly.

Security in the construct of indistinguishability has manifold definitions, depending on assumptions made about capabilities of the Attacker. The most common definition is the indistinguishability under chosen plaintext attack (IND-CPA). Indistinguishability under (non-adaptive) chosen ciphertext (IND-CCA) and indistinguishability under adaptive chosen ciphertext attack (IND-CCA2). Security under either of the latter definition implies security under the former. Put in a more brilliant clarity, a scheme which is IND-CCA secure is also IND-CPA secure; a scheme which is IND-CCA2 secure is secure in both IND-CCA and IND-CPA secure. Thus, by these round -lay-definitions, IND-CCA2 is the strongest of the three definitions of security. Details explanations of each security layout follow:

I.I.II Indistinquisahability Under Chosen-Plaintext Attack (IND-CPA)

A cryptosystem is said to be indistinguishable under Chosen Plaintext Attack if every polynomial time adversary has only a negligible "advantage" over random guessing. An adversary is said to have negligible advantage if it succeeds in making the clarification of the plaintext chosen from the ciphertext with a probability of (1/2)+epsilon(k), where by definition, epsilon(k) is a negligible function in security parameter "k", that is, for every (nonzero) polynomial function poly(k), there exists k_0 such that $|epsilon(k)| < |poly(k)| \forall k > k_0$.

The definition specified is specific to an asymmetric key cryptosytstem. However, it can also be adapted to the symmetric case by replacing the public key encryption function with the "encryption oracle", which retains the secret encryption key and encrypts arbitray ciphertexts at the terrorist's1 request.

I.1.III Indisguishabilityunder Chosen Ciphertext Attack/Adaptive Ciphertext Attack (IND-CCA, IND-CCA2)

The concept of indistinguishability under non-adaptive and adaptive Chosen Ciphertext Attack (IND-CCA, IND-CCA2) applies similar definition to that of the IND-CPA. The only difference that exists is that the adversary is given access to the decryption oracle which decrypts the arbitrary ciphertexts at the adversary's request, returning the plaintext. In the IND-CCA or non-adaptive paradigm, the adversary is allowed to query this oracle only up until it receives the challenge ciphertext. In adaptive construct, the adversary may continue to query the the decryption oracle even after it has received a challenged ciphertext, with a caveat that it may not pass the challenged ciphertext for decryption (else, the paradigm definition is insignificant)

I.I.IV Non-malleability

An encryption scheme is malleable is an adversary has the capacity to technically transforms a ciphertext into another ciphertext that decrypts routingly to a related plaintext. Put straight, given an encryption of plaintext m, it is possible to generate another ciphertext which decrypts to some function $f(m)$ without necessarily knowing the function f.

Though malleability may be useful in some other schemes such as the Gentry's (2009) fully homomorphic encryption scheme, (V. O. Waziri, et al., (2014)) it is often an undesirable property in most cryptosystem schemes because this can defeat the principle of collision-resistance since it allows an attacker to modify the contents of a message. This can bring about e-fraud exploitation to financial institutions.

Non-malleability is that given a ciphertext, it should be impossible for an adversary to clone or regenerate a different ciohertext so that the respective ciphertexts are related.

I.I.VThe importance of Non-malleability in Cryotosystems

This section is better understood with some expalanation based on existential unforgeability of signature schemes of some institutions be it private or governmental institutions. Existential unforgeable scheme could be exemplified through a mathematical analogy; for instance, consider the condition in which an adversary is given access to the scheme $(m_1, s(m_1)),...,(m_k, s(m_k))$ for some $s(m_i)$ that denotes a signature on message m_i, the adversary cannot construct a single valid $(m, S(m))$ pair for any new message m even that it may emanate from some gibberish message of function of $m_1, \ldots, m_k$. In simplified deduction, existential unforgeabibility for signature schemes is the construe "moral equivalence" of non-malleability for the structure of cryptographic security frame.

Non-malleability has a strong support in private-key cryptosystems. This due adduces to the need for hybrid encryption scheme for such schemes with common protocols such as the Kerberos or the Andrew Secure Handshake, use private key encryption as a sort of authenticationmechanism.

I.I Why Hybrid Encryption Scheme?

Internet is an interconnection network of computer network worldwide that autonomous computing nodes that are well defined, mutually agreed set of rules and conventions known as protocols that interact with one another through gateways meaningfully and allow resource sharing preferably in a predictable and controllable arrangement [18]), The implication of this interconnectivities reliance is that communication has some profound impact in today's businesses, political and economy of various nations. Thus, there is a pragmatic desire to communicate with high cautiousness of security now that the world communication security layer is depleting by the day. This is well buttressed with the advancement of rapid development of network technology, internet attacks by hackers, political and religious terrorists that are becoming so multipurpose. Hence it is imperative that traditional encryption algorithms that are based on single data encryptions for today's information security over the Internet be hybridized that confusion and diffusion of encrypted data be interwoven to increase the depleting layer of security under probabilistic polynomial time.

I.II Organization:

The structure of the rest of the paper sections are as follow: In section 2, we study the cryptographic encryption paradigm, section 3 studies three cryptosystems, the Elliptic Curvehttp://en.wikipedia.org/wiki/ellipticcurve cryptography and MD5 for as sources of hybridized symmetric key; asymmetric key study was strictly studied under the platform of dual RSA. The hybridization of these encryption schemes improves efficiencies and authentication of the secure data. Section 4 implements the hybridization of section 3 schemes theoretically. Section 5, gives the conclusive remarks and provides further related works.

I.III Contribution:

The visible contribution of the paper is to produce a gateway for further future researches on Cyberwarfare and Cyber Terrorist within Nigeria Cyberspace that is conceived to be lacking by professionals. Hence, the paper is mostly a partial survey study.

II. DEVELOPING HYBRID CRYPTOSYSTEMS

When developing a new hybrid encryption scheme, there are two basic criteria that a designer should want to ensure: Security and efficiency. However, security is in most cases, the obvious main concern that is expressed in terms of the attackers' goal against the scheme and the means it uses [25]. The standard security notion for a general purpose cryptosystem is indistinguishability against cypertext attacks against adaptative chosen attacks, IND-CCA for short. The proofs of security are polynomially reduced to trusted mathematical assumptions. In terms of efficiency attribute, two main aspects are considered. The first is the computational complexity of the algorithms that involves the scheme; while the second coniseration is the concrete security scheme, [10].

A hybrid encryption scheme is a computational process that harnesses the functionalities of two or more algorithmic features of an asymmetric encryption key using a two party's cryptosystems to establish a symmetric key that that can be applied to facilitate faster computational encryption scheme. That is, a hybrid encryption scheme applies public-key encryption to establish a symmetric key agreement.

The scheme could be properly understood through algorithmic constructs as follow:

As [7], let $(keyGen, \in, D)$ be a secure public cryptosystem for an encryption scheme $(\in', D')$ that is a secure private-key encryption scheme. We can construct a secure hybrid encryption scheme $(keyGen'', \in'', D'')$ in this pattern:

1. $keyGen''$ is the same as $keyGen$, generating a public-key pk and a secret key sk based on some secure parameter 1^{λ}.
2. $\in''_{pk}$ having the following properties:
   a. $sk' \leftarrow \{0,1\}^k$;
   b. $C_1 \leftarrow \in_{pk} (sk')$
   c. $C_{21} \leftarrow \in'_{sk'} (m)$
3. $D''_{sk}(C_1, C_2)$
   a. $sk' = D_{sk}(C_1)$
   b. $m = D'_{sk'}(C_2)$

The outlined scheme above can be proven semantically secure, with the assumption that the semantic security of the underlying public and private-key schemes. In this constraint write up, however, we will not give any proof in this paper.

II.I Methodology of Hybrid Encryption Scheme

Unfortunately in developing any hybridized encryption scheme needs many algorithmic paradigms which we are forced to implement hereunder that is based on asymmetric encryption theoretic operations [4]:

First, we need to encrypt a randomly chosen symmetric key using an asymmetric encryption algorithm and encrypt a message using a symmetric encryption algorithm and K. This gives the concept of hybrid encryption scheme that is asymmetric encryption

1. Algorithm for Encrypting the Symmetric key and the message m $\overline{\in}_{pk} (m)$

$K \leftarrow \overline{\in} K^s; C^s \leftarrow \in^s_K (M)$

If $C^s = \perp (false)$ *then return* $\perp$

$C^{\alpha} \xleftarrow{s} \in^{\alpha}_{pk} (K); C \leftarrow (C^{\alpha}, C^s)$

return C

2. Algorithm for Decrypting the symmetric key and the message m $\overline{D}_{pk}(C)$

Parse C *as* (C^{α}, C^S)

$K \leftarrow D^{\alpha}_{sk}(C^{\alpha})$

IF $k = \perp (false)$ *then return* $\perp$

$m \xleftarrow{s} D^{\alpha}_K (C^S)$

return M

We consider the theorem that evokes the security of the asymmetric and symmetric based on IND-CPA hybrid encryption scheme:

Theorem 2.1 (Hybrid Encryption with Respect to IND-CPA):

Let $AE = (GenKey^a, Enc^a, Dec^a)$ represent the asymmetric cryptosystem and $SE = (GenKey^s, Enc^s, Dec^s)$ the symmetric cryptosystem respectively, with the condition that the SE key is always embedded in the message space of AE. Let $A\overline{E} = (GenKey^a, \overline{E}nc, \overline{D}ec)$ the associated scheme as defined on the previous above. Then for any adversary B, there exist adversaries $A_{00,01}, A_{11,10}, A$ that have the following advantage

$$Adv^{ind-cpa}_{\overline{A\in}}(B) \leq Adv^{ind-cpa}_{A\in}(A_{00,01}) + Adv^{ind-cpa}_{A\in}(A_{11,10}) + qAdv^{ind-cpa}_{S\in}(A)$$

With the condition that $A_{00,01}, A_{11,10}$ have time complexity of B, and so can make the same number of queries with each having length k (symmetric key length), and that A has the time complexity of B and makes only one query.

Collorary 2.2 (IND-CPA):

If the components are IND-CPA, then the associated hybrid scheme is also IND-CPA and is a one-way secure public scheme Known-plaintext Atack (http://www.tech.faq.com/known.plaintext.attack.shtml)

Proof:

We are applying the hybrid- arguments for the proof. This, we shall achieve by stating a sequence of 4 experiments that are associated with adversary B :

$$(1)\ Exp_{AE}^{00}(B),\ (2)\ Exp_{AE}^{02}(B),\ (3)\ Exp_{AE}^{11}(B),\ (4)\ Exp_{AE}^{10}(B)$$

from which we define

$$p(\alpha,\beta)=\Pr[Exp_{AE}^{\alpha\beta}(B)=1]$$

Therefore, it will be the case that:

$$p(1,0)=\Pr[Exp_{AE}^{ind-cpa-1}(B)=1$$

$$p(0,0)=\Pr[Exp_{AE}^{ind-cpa-0}(B)=1$$

and therefore

$$Adv_{A\in}^{ind-cpa}(B)=P(1,0)-(0,0)$$

$$=p(1,0)-(1,1)+p(1,1)-(0,1)+p(0,1)-(0,0)$$

$$=[p(1,0)-(1,1)]+[p(1,1)-(0,1)]+[p(0,1)-(0,0)]$$

We further construct the adversaries $A_{00,01}$, $A_{11,10}$, A subject to the inequalities:

$$P(1,1)-P(0,1)\le Adv_{a\in}^{IND-CPA}(A)$$

$$P(1,0)-P(1,1)\le Adv_{a\in}^{IND-CPA}(A_{10,11})$$

Based on these inequalities, the theorem statement will now allow:

II.I.I The Terms Oracle Encryption and Decryptions

We need to understand the meaning of the term encryption or decrypting oracle before proceeding.

We now need to define the aforementioned experiments that use different oracles:

$H\in_{pk}^{00}(.,.)$, $H\in_{pk}^{01}(.,.)$, $H\in_{pk}^{11}(.,.)$, $H\in_{pk}^{10}(.,.)$,such that for all possible bits possible bits α,β , define the generic experiment over the bits:

$(pk,sk)\xleftarrow{s}K^{\bullet}$

$d\leftarrow B^{H\in_{pk}^{\alpha\beta}(pk)}$

Return d

1. Oracle

$H\in_{pk}^{00}(M_0,M_1)$

$K_0\xleftarrow{s}K^{\alpha},\ K_1\xleftarrow{s}K^{s}$

$C^{\alpha}\xleftarrow{s}\in^{\alpha}(K_0;M_0)$

if $C^{\alpha}=\perp$, *then return* $\perp$

$C^{\alpha}\xleftarrow{s}\in^{\alpha}(pk,K_0)$

$C\leftarrow(C^{\alpha},C^{s})$

Return

$H\in_{pk}^{01}(M_0,M_1)$

2.Oracle

$K_0\xleftarrow{s}K^{\alpha},\ K_1\xleftarrow{s}K^{s}$

$C^{\alpha}\xleftarrow{s}\in^{\alpha}(K_0;M_1)$

if $C^{\alpha}=\perp$, *then return* $\perp$

$C^{\alpha}\xleftarrow{s}\in^{\alpha}(pk,K_0)$

$C\leftarrow(C^{\alpha},C^{s})$

Return

Check to verify that:

$$P(1,0)=\Pr[Exp_{as}^{ind-cpa-1}(B)=1]$$

$$P(1,1)=\Pr[Exp_{as}^{ind-cpa-0}(B)=1]$$

We hereunder construct adversaries $A_{00,01}$, $A_{10,11}$, to safe space; we set each adversary expressions in two columns as shown hereunder:

Adversary $A_{01,00}^{\in_{pk}^{(LR(.,.,b)}}(pk)$, subroutine $O \in (M_0, M_1)$

$K_0 \xleftarrow{s} K^s$, $K_1 \xleftarrow{s} K^s$

$C^{\alpha} \xleftarrow{s} \in^s (K_0; M_0)$

if $C^s = \perp$, *then return* $\perp$

$C^{\alpha} \xleftarrow{s} \in_{pk}^{\alpha}(LR, K_0, K_1, b)$

$C \leftarrow (C^{\alpha}, C^s)$

Return

End subroutine

$d \xleftarrow{s} B^{o \in (.,.)}(pk)$

Return d

Adversary $A_{10,11}^{\in_{pk}^{(LR(.,.,b)}}(pk)$, subroutine $O \in (M_0, M_1)$

$K_0 \xleftarrow{s} K^s$, $K_1 \xleftarrow{s} K^s$

$C^{\alpha} \xleftarrow{s} \in^s (K_0; M_1)$

if $C^s = \perp$, *then return* $\perp$

$C^{\alpha} \xleftarrow{s} \in_{pk}^{\alpha}(LR, K_1, K_0, b)$

$C \leftarrow (C^{\alpha}, C^s)$

Return

End subroutine

$d \xleftarrow{s} B^{0 \in (.,.)}(pk)$

Return d

Check that:

$$\Pr[Exp_{A\in}^{ind-cpa-1}(A_{01,00}) = 1] = PR[Exp_{a\in}^{01}(B) = 1]$$

$$\Pr[Exp_{A\in}^{ind-cpa-1}(A_{01,00}) = 1] = PR[Exp_{a\in}^{00}(B) = 1]$$

$$Adv_{A\in}^{ind-cpa}(A_{01,00)} = P(0,1) - P(0,0)$$

Hereunder, we are defining the four experiments that use different Oracles

$$H \in_{pk}^{00}(.,.),\ H \in_{pk}^{01}(.,.),\ H \in_{pk}^{11}(.,.), H \in_{pk}^{100}(.,.)$$

For all $\forall\ \alpha, \beta$, let us define the following the Experiment that is carried out out by adversary B:

:

$(pk, sk) \xleftarrow{s} K^{\alpha}$

$d \leftarrow B^{HE_{pk}^{\alpha\beta}(.,.)}(PK)$

Return *d*

From the Public encryption that is carried out by A, the four oracles are as follows:

1. *Oracle* $H \in_{pk}^{00}(M_0, M_1)$

$K_0 \xleftarrow{s} K^s$; $K_1 \xleftarrow{s} \in^s (K_0, [M_0])$

if $C^s = \perp$ *then return* $\perp$

$C^{\alpha} \xleftarrow{s} (pk, [K_0])$

$C \leftarrow (C^{\alpha}, C^s)$

Return *C*

2. *Oracle* $H \in_{pk}^{01} (M_0, M_1)$

$K_0 \xleftarrow{s} K^s;\ K_1 \xleftarrow{s} \in^s (K_0, [M_0])$

if $C^s = \perp$ *then return* $\perp$

$C^\alpha \xleftarrow{s} \in^\alpha (pk, [K_1])$

$C \leftarrow (C^\alpha, C^s)$

Return C

3. *Oracle* $H \in_{pk}^{11} (M_0, M_1)$

$K_0 \xleftarrow{s} K^s;\ K_1 \xleftarrow{s} \in^s (K_0, [M_1])$

if $C^s = \perp$ *then return* $\perp$

$C^\alpha \xleftarrow{s} \in^\alpha (pk, [K_1])$

$C \leftarrow (C^\alpha, C^s)$

Return C

4. *Oracle* $H \in_{pk}^{10} (M_0, M_1)$

$K_0 \xleftarrow{s} K^s;\ K_1 \xleftarrow{s} \in^s (K_0, [M_1])$

if $C^s = \perp$ *then return* $\perp$

$C^\alpha \xleftarrow{s} \in^\alpha (pk, [K_0])$

$C \leftarrow (C^\alpha, C^s)$

Return C

Check that

$$P(1,0) = \Pr[Exp_{\overline{A}\in}^{ind-cpa-1}](B) = 1$$

$$Adv_{iS\in}^{nd-cpa}(A) = \Pr\left[Exp_{s\in}^{ind-cpa-1}(A) - 1\right] - \Pr\left[Exp_{s\in}^{ind-cpa-0}(A)\right] - 1$$

$$= \sum_{i=1}^{q} \Pr\left[Exp_{s\in}^{ind-cpa-1}(A) = 1 \middle| I = i\right] * \Pr[I = i] - \sum_{i=1}^{q} \Pr\left[Exp_{s\in}^{ind-cpa-0}(A) = 1 \middle| I = i\right] * \Pr[I = i]$$

$$= \frac{1}{q} \sum_{i=1}^{q} P(i) * \Pr[I = i] - \sum_{i=1}^{q} P(i-1) * \Pr[I = i]$$

$$= \frac{1}{q} . \sum_{i=1}^{q} P(i) - \Pr[i-1]$$

$$= \frac{1}{q} . [P(1,1) - P(0,1)]$$

Having seen the necessary security of the hybrid cryptosystem, it is also necessary to note that a symmetric encryption scheme can satisfy a definition weaker than the INC-CPA (as in the proof "A" makes only one query to the LR oracle)

For instance, the symmetric scheme can be deterministic; this becomes so because new symmetric key is picked for each message.

We have overviewed a lot of the fundamentals of hybrid encryption scheme in generic construct and also periscope the underlying crypt analytical concepts.

III. THE ELGAMAL CRYPTOSYSTEM AND THE HYBRID ENCRYPTION SCHEME

In this subsection, we describe theTaher El Gamal (1984) encryption that needs the concept of Galois field or finite cyclic group. First we introduce the finite group generally known as Abelian group.

Definition III.1 (An Abelian Group G)

In group theory, an AbelianGrough G is a set of finite set of elements along with a multiplication operator * (which is written multiplicatively that corresponds to integer multiplication) satisfying the following conditions:

Closure: For all $a,b \in G$. Using the multiplication operator symbol *, this could be expressed as $a * b = ab \in G$.

Associativity is such that for all $a,b,c \in G$, we have $(ab)c = a(bc) \in G$

Commutativity: For all $a,b \in G$ we have $ab = ba \in G$

Existence of Identity: There exists an element $1 \in G$ such that $1 * a = a \ \forall \ a \in G$. This element is called the identity of G.

Inverse For all $a \in G \ \exists \ a^{-1} \in G$ such that $aa^{-1} = 1$.

Order of Elements: Let $q = |G|$; this denotes the number of elements in G that is algebraically known as the order of G.

The [21] Public key algorithm makes an alternative to the RSA (1978) for the public key encryption.
The security of RSA depends on the theoretic assumption of difficulty of factoring the exponential large integer.

The Security of ElGamal algorithm depends on the theoretic assumption of computing discrete logarithms in a large prime modulus

The problem with ElGamal Key is that ciphertext is twice as long as the ciphertext. While its advantage is that the plaintext gives different ciphtexts (with near certainty) each time it is encrypted.

Generating the ElGamal Cryptosystem:

Using the traditional characters of Alice and Bob:

Alice Chooses:

i) A large prime P_A (some 200 to 300 digits)

ii) A primitive elements $\alpha_A \ Modulo \ P_A$

iii) A (possibly random) integer $d_A \ with \ 2 \le d_A \le P_A$

iv) Alice Computes:

$$\beta_A \equiv \alpha_A^{d_A} (\text{mod } p_A)$$

Alice's public key is (p_A, α_A, β_A), her private key is d_A

Bob Encryption: Bob encrypts a short message $M (M < p_A)$ ad sends it to Alice like this manner:

i) Bob chooses a random integr k (which he keeps secret), and then discard k.

ii) Bob computes $r \equiv \alpha_A^k (\text{mod } p_A)$ and $t \equiv \beta_A^k M (\text{mod } p_A)$, and sends his encrypted message (r,t) to Alice

Bob sends his encrypted message (r,t) to Alice.

When Alice receives the encrypted message (r,t), she decrypts it (using her private key d_A) by computing tr^{-d_A}, that is :

$$\begin{aligned} tr^{-d_A} &\equiv \beta_A^k M (\alpha_A^k)^{-d_A} (\text{mod } p_A) \\ &\equiv (\alpha_A^{d_A})^k M (\alpha_A^k)^{-d_A} (\text{mod } p_A) \\ &\equiv M (\text{mod } p_A) = M; \ \ \forall \ M < p_A \end{aligned}$$

Even if the Cyberterrorist Eve intercepts the ciphertext (r,t), she cannot perform the calculation above because she does not know d_A.

$$\beta_A \equiv \alpha_A^{d_A} (\text{mod } p_A), \text{ so } d_A \equiv L_{\alpha A}(\beta_A)$$

Even if a Cyberterrorist Eve finds the Alice private key d_A, she cannot compute a discrete logarithm in the large prime p_A, that is presumably a computation that is too difficult to be practical,

Note:

Bob should choose a different random integer k for each message he sends to Alice. In case M is a longer message, so it is divided into blocks, he should choose a different k for each block.

Suppose he encrypts two messages (or blocks) $m_1 \ and \ m_2$, using the same k, producing ciphertexts

$$(r_1, t_1) = (\alpha_A^k, \beta_A^k M_1), \ (r_2, t_2) = (\alpha_A^k, \beta_A^k M_2)$$

Then $t_2, t_1^{-1} \equiv M_2 M_1^{-1} (\text{mod } p), \ M_2 \equiv t_2 t_1^{-1} M_1 (\text{mod } p)$, Should the Cyber terrorist Eve acquires both ciphertexts messages and discovers one plaintext messages M_1, she can compute the other plaintext message M_2

III.1 The Cryptosystems for the Model Building

We have overviewed a lot of the fundamentals of hybrid encryption scheme in generic construct and also periscope the underlying crypt analytical concepts. We therefore summarize the general algorithm for a hybrid encryption in plain language as in [17], [18]:

A hybrid encryption scheme [10], is a model that uses a multiple of ciphers together, each to its best advantage. It may be constructed using two separate cryptosystems:

1. A key has encapsulation scheme which is a public-key or any other type of cryptosystem;
2. A data (message of information) has encapsulation scheme which is a symmetric-key cryptosystem

Thus the twain itemized, a hybrid is itself a public-key system that has public and private keys which is the same as the key encapsulation scheme. In place of public key system, digital signature like message digesting function with symmetric scheme can be harmonized to make advantage of a hybrid crypto system. Impress it in your mind that for some very long messages, the bulk of the work in encryption/decryption is done by the more efficient symmetric-key scheme, whereas the inefficient public-key scheme is used only to encrypt/decrypt a short key value. The process for the hybrid unified into these sequences:

1. Bob acquires the public-key of Alice;
2. Generate a fresh symmetric key through public cryptosystem scheme;
3. Encrypt the message using the symmetric key;
4. Encrypt the symmetric key using Alice's public key; and
5. Bob embeds and sends the message and the encrypted symmetric key to Alice

To decrypt this hybrid cipher text, Alice does the following computational operations:

1. Alice applies her private key to decrypt the symmetric key; and
2. Alice applies the decrypted symmetric key to decrypt the message

IV. IMPLEMENTATION OF HYBRID CRYPTOSYSTEM OF CYBER WARFARE

The desire to transmit data so that the data attains maximum security is uppermost in modern communication systems. Various cryptographic models have been devised to meet this data security with some having some secure theoretic promise. There are however others at present that are considered to provide high cryptographic security on information on controlled networks. The algorithms are expected to provide data security and users authenticity. However, the new design hybrid protocols provide a combination of both symmetric and asymmetric cryptographic techniques as discussed in some sections above that also enhances efficiency and more ingenuous tight security.

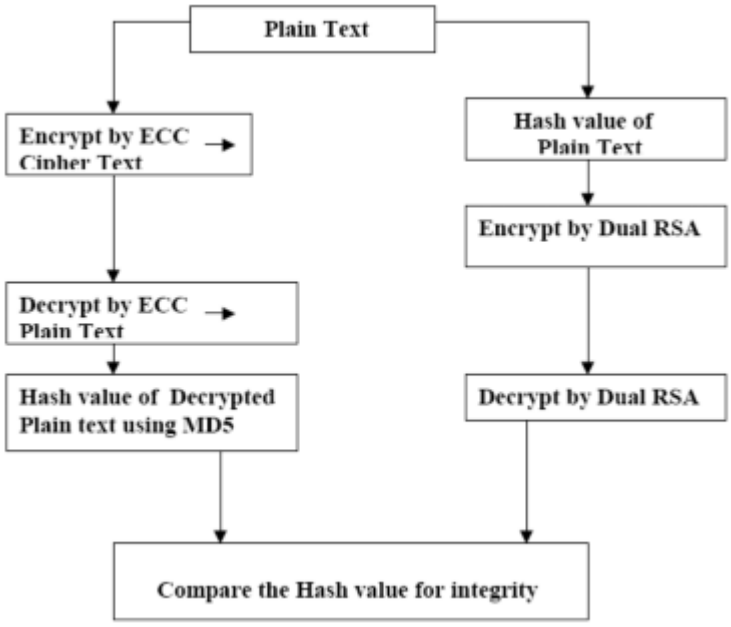

Fig. 1: Simple Hybrid Protocol; Courtesy of [20]

In section III, we put across the Symmetric key the Elliptic Curve Cryptography, and the MD 5 cryptosystems. Figure 1 depicts the symmetric Key that applies the MD5, elliptic curve symmetric that are hybridized the dual RSA asymmetric Cryptographic scheme that could enhance the confidentiality, Authentication and Integrity of the data.
The figure also comprehensively discussed the primitives that can be achieved with the help of this security Protocol Architecture. The elliptic Curve and the MD5 are used to achieve data security based on Confidentiality and Integrity.

IV.I Implementation of Hybrid Encryption Scheme Mitigation on Cyberterrorism

We have strategically sieved the contents of cyber terrorism through cryptographic and cryptanalytic schemes. We at this point provide some useful suggestions that can assist in forestalling Cyber terrorism and Cyberwarfare that can be

apolitical, social, religious or financial aggrandizement within some country and the foreign cyber-attacks; but, albeit, briefly for want of space and time.

We already know with strenuous affirmation that today's business environments is compliance-driven competitive and increasingly fraught from financially motivated hackers and frustrated employees. In view of this, this has created some cautious needs to make effective, practical, automated and risk-mitigating ways that could manage symmetric and asymmetric keys throughout their operational lifecycle. This would ensure that only authorized clients or users have the mandate to access,and that, the unauthorized users are thwarted from having access to the keys. User and Application access to these resources of encrypted dated must be controlled, managed and audited periodically so that authorized access to the resources is quick and reliable. This would prevent cyberterrorists attacks form having nefarious upper hand.

The application of strong crypto system together with strong secure-key encryption management system should stand to ensure all security goals are met in polynomial time. The hybrid cryptographic algorithms should provide a maximized efficiency, correcting or complementing other's weaknesses.

Any encryption scheme should operate within the allowable standard to the local environment. Any terrorists caught should be forced to give up his operational private-key by the Law enforcement agencies.

All institutions should have their data secure through encryptions to maintain data security.

As good as hybrid encryption is to any nations, it has its difficulty in modeling the schemes. For any nations to have power defenders in cyber terrorism and warfare, the incoming generations should be heavily trained in the physical sciences; most especially in Mathematics and Physics. Pure Mathematics, Modern Mathematics syllabi must be reviewed to include the traditional mathematics that relies strongly in Boolean and abstract algebra and should be practically taught by competent instructors. In physics, quantum physics and solid physics should be given high places academically with applicable practical carry out incessantly.

Educational planners based-on issues that all undergraduate students must take both social arts and the sciences must be deemphasized in our syllabi. Science students should be granted much time in the field of sciences or engineering, to create the requisites for strong knowledgeable applications in their chosen careers that can complement the application of Cryptology.

Government must take the threats of cyber terrorism seriously with proactive decision and active actualization of decisions taken. National security issues concerns must take prompt actions within the realm of the nation security concern.

There is the need to have a discussion of cyber vulnerabilities today in Nigerian cyberspace, before the failure occurs as both religious and political cyber terrorisms are now the order of the day. Merely enacting Cyber laws that merits punitive measures on the offenders by the national assembly is not good enough. Practical actualizations through cautious learning and avoidance of crimes that would merit the punitive measures should be ethically taught to the users. This would avoid the aphorism of "no ignorance in Law".

The issues of computer frenzy on critical infrastructures are not being handled with critical security. The use of computers security must be fully addressed in all the nation's security outfits and in practice in our various institutions

.Reports of all cyber threats must be accepted with critical evaluation which must be examined with high level of "Shaving Factor" in cyber terrorism discussions. Swift actions should be the watchword in any observable Cyber terrorism or Cyber warfare..

V. CONCLUSION FURTHER RELATED WORKS

Fighting Cyber Terrorism and Warfare is a logical fight in the computing cyberspace and the Internet, there is no need for physical confrontations as it is the antics in the Military way from ancient to the present days. We hope that in the nearest future, wars should be fought by wits based on technological tools and advancements in software. The strategies are based cardinally on hard and efficient computing algorithms based on malicious software. Combating such strategies could be confronted through the application of intelligent devices that are developed through the mechanism of intelligent computational processes. For instance, today cyber terrorisms are based on the application of cryptographic, steganography; biometrics models a part from having access to the Internet and computer vulnerabilities that are occasioned from implemented software with vulnerabilities. Most Internet of Things (IoT), being new products in commercial markets possess some vast vulnerabilities that cyber terrorists can apply as efficient tools to combating their reprehensible warfare.

In light of the above constructions, current cyber security researches should expand to meet the yearnings that will enable abstractive battle against Cyber Terrorists.

REFERENCES

[1] B. Schneier, (1996), "Applied Cryptography", New York: John Willey and Sons

[2] C. Gentry (2009), "A Fully Homomorphic Encryption Scheme", A Dissertation Submitted To The Department Of Computer Science And The Committee On Graduate Studies of Stanford University In Partial Fulfillment Of The RequirementsFor The Degree of Doctor Of Philosophy"

[3] D. Boneh and G. Durfee (2000), Algorithmic Number Theory: 4th International Symposium, ANTS-IV Leiden

[4] E. Fujisaki, T. Okamoto, "Secure Integration of Asymmetric and Symmetric Encryption Schemes", XTT Laboratories, 1.1 Hikarinooka, Yokosika, 239-0847, Japan

[5] H. S. Lia, (1998), "Cryptography and Public Policy", Journal of Government Information, pp 135-148

[6] H. Kuzushko (2003), "MD5 Algorithm"

[7] J. Katz and Y. Lindell (2007), Introduction To Modern Cryptography, Chapman& Hall/Crc Cryptography and Network Security

[8] J. Booke, J. Mcdonald, T. Austin (2000,2004), "Architectural Support for Fast Symmetric Key Cryptography, Architectural Support for Programming and Operating Systems", Association of Computing Machinery

[9] J. Stone (2004), "Independent Component Analysis", A tutorial Introduction, Mi Press, Cambridge , MA.

[10] J. J. Quisquarter and Couvreur (1989),"Fast Decipherment Algorithm for RSA Public Key Crypto System, Electronoc Letters, Vol 435

[11] M. A. Lia, A. Yahya, (2010),"Public-Key, Steganography Based on Matching Method", European Journal of Scientific Research

[12] M. Willet (1984); "Cryptography Old and New" ScienceDirect, Computers and Security, pp 177-186

[13] N. Gura, A. Patel, A. Wander, H. Eberle, and S.C. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs". Proceedings of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004), 6th International Workshop, pages 119–132, 2004

[14] R. Pass (2009), Lcture 14: Trapdoor Permutation

[15] L.. Ronald Rivest, L. Addleman, and Mi. L. Dertouzos (1978); "On Data Banks and Privacy Homomorphism, Chapter on ata Banks and Privacy Homomorphisms, pages 169-180, academic press 1978

[16] S. Goldwasser and S. Micali (1982): " Probabilistic encryption", In Journal of Computer and System Sciences, Vol28, no. 2, pp270-299

[17] S. Gard ,S. Verma (209), "Importanant of Public Key Cryptography algorithm", IEEE International Advance Computing Conference

[18] S Kumar, T. Wollinger, (2006), "Fundamentals of Symmetric Cryptography", Embedded in Cars, pp. 125-143

[19] S. Gordon, R. Ford (White Paper), "What is Cyberterrorism?",Symmantic Security Response, Independent Consultant

[20] S. Subasreeand N. K. Sakthivel (2010), "Design Of A New Security Protocol Using Hybrid Cryptography Algorithms", Subasree&Sakthivel Design of a New Security Protocol

[21] T. El Gamal (1984), "A public key cryptosystem and a signature scheme based on discrete logarithms" In Proceedings of CRYPTO 84 on Advances in cryptology, pages 10{18. Springer-Verlag New York, Inc., 1985

[22] V. O. Waziri, J.K. Alhassan, O.Morufu& I.Ismaila (2014), "Big Data Analytics and the Epitome of Fully Homomrphic Encryption Scheme for Cloud Computing Security", International Journal of Developments in Big Data and Analytics Voolume 1 No.1, 2014, pp 19-40

[23] W. Diffie, M. E. Hellman (1976):"New Direction in Cryptography", S. I. IEEE, Transactions on Information Theory, pp. 644-654

[24] B. Collin (1997), "Future of Cyberterrorism: The physical and virtual Worlds Converge". Journal of Crime and Justice International Vol.13(2) pp.15 to 18

[25] D. Matematica, et al. (www.dgalindo.es/FOfinall.JI.pdf)

