Towards the Use of Cryptographic Techniques for National Security:

Models, Methods, & Applications

Sunday E. Adewumi, PhD
Professor of Computer Science
Federal University
Lokoja, Nigeria
adewumis@gmail.com

SUMMARY

The financial services industry is no exception in the search for efficiency and productivity improvements, competitive advantage through information and communications technologies (ICTs). Notable are commercial banks that have opted for various ICT initiatives towards reducing back office processing costs, improving service delivery and business management practices through data analysis (Ferguson, 2000).

ICTs in African banks date back to the data processing era where mainframes were used for transaction processing operations; however, the explosion of computer systems synonymous with the personal computer (PC) and PC-based servers led to the diffusion of IT systems. Where mainframes facilitated centralised processing, the distribution of PC-based servers in bank branches enabled branch automation. Further advancements in banking automation were facilitated by enhanced communications networks that interconnected bank branches for centralised processing and multi-branch banking. The evolution of the data telecommunications through services such as the Internet and global systems for mobile (GSM) have further extended the reach of banking to consumer self-service.

This chapter, ICT in banking: application, impacts, and challenges provides an overview of the role ICT plays in the delivery of banking services alongside common impacts and challenges in Africa. Following this introduction, a foundational overview of banking activities, ICT, and its role in banking is presented prior to the discussions on application of ICT components in the execution of banking services in the third section. In addition to its application in banking services, the third section also presents relevant architectural, processing, and infrastructural considerations applicable in banking. Section four and five illustrate ICTs impact and challenges respectively drawing on implementation examples from the Continent. The concluding section summarises the chapter and future developments.

Keywords: ICTs, Banking, GSM, Financial services, Africa, Difussion

1. INFORMATION AND DATA SECURITY

In this section, we provide general overview of cryptography with some basic concept that may generally be required by the learner.The issue of security in today's information transmission is a priority area as information transcend beyond a networked computers in a local organization to across borders. Cryptography, with its many cryptographic methods is one way the world is responding to information and data security.The primary objective of cryptography is to enable two people say Ade and Bola to communicate effectively over unsecure channels (such as telephone, intranet and Internet etc) see Figure 1.

It is assumed that there is always an intruder who eavesdrops for the purpose of accessing the message being transmitted and manipulates it for evil or economic gain. The protection of data is of today's uttermost priority. In its simplest form, a sender S sends a plaintext P; the plaintext is encrypted with an encryption key Ke to ciphertext C and then transmitted through an unsecured channel where it is assume that a cryptanalyst (a 'listener') is waiting to intercept the message being transmitted. When the message reaches the receiver R (the owner of the message), a decryption algorithm is invoked to recover the plaintext. Some of the methods in use for transforming a plaintext to a ciphertext are discussed under this section.

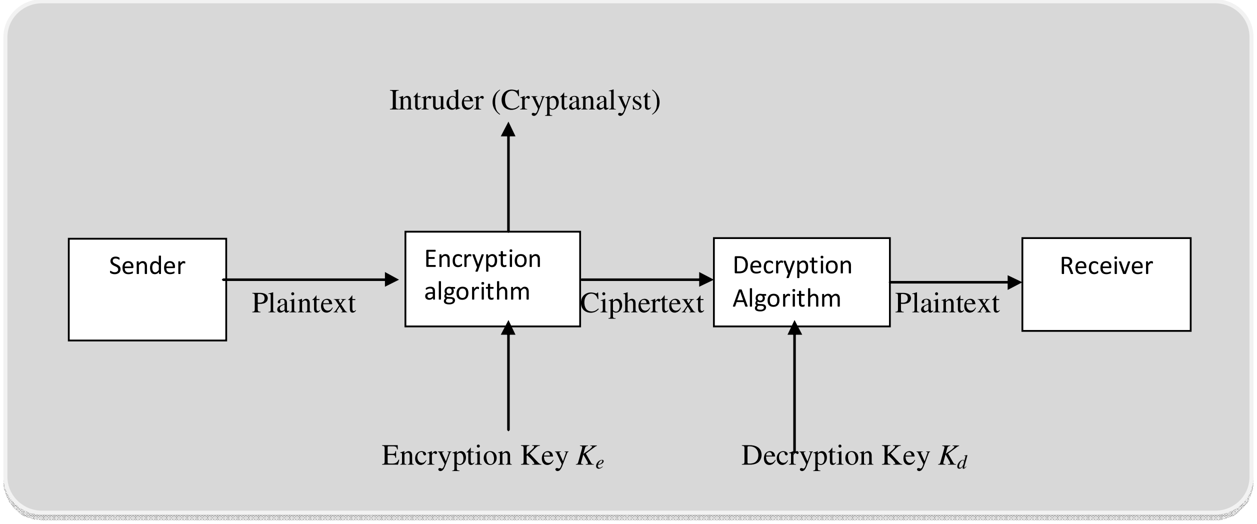

Figure 1: The Encryption Model for secured data transmission

It is assumed that, during the transmission, intruder (the enemy) hears and copies the ciphertext, but he/she neither understands nor knows what the decryption algorithm is, and usually makes it impossible to decipher the message.

In any cryptosystems, three fundamental assumptions are made:

- The intruder 'hears' the message
- The cryptanalyst (the intruder) knows the encryption algorithm;
- The medium of transmission is insecure.

1.1 Basic Definitions

The art of breaking ciphers by the intruder is called ***cryptanalysis***; while the art of devising ciphers known as cryptography and breaking them known as ***cryptanalysis*** is collectively known as ***cryptology***.

There is always the need to create a state of confusion (delay) for the ***Cryptanalyst*** whose intention it is to break in and have access to the data being transmitted. The Chinese proverb that says ***it is sometimes good to be unclear*** readily applies in encryption.

The art of cryptography as a means for safeguarding and protecting private information against unauthorized access is as old as writing itself.

Until the advent of computers, one of the main constraints on cryptography had been the ability of the code clerk to perform the necessary transformation, often on battlefield with little equipment; as early uses of cryptography were for the military. An additional constraint has been the difficulty in switching over quickly from one cryptographic method to another, since this entails retraining a large number of people. However, the danger of a code clerk being captured by the enemy has made it essential to be able to change the cryptographic method instantly, if need be. (Zeng et al, 1991; Tanenbaum, 1996).

People have tried to conceal information in written form since writing was developed and examples survive in stone inscriptions and papyrus showing that many ancient civilizations including the Egyptians, Hebrews and Assyrians all developed cryptographic systems. The first recorded use of cryptography for correspondence was by Spartans who (as early as 400 BC) employed a cipher device called a "scytale" to send secret communications between military commanders. It consists of tapered baton around which was wrapped a piece of parchment inscribed with the message. Once unwrapped the parchment appeared to contain an incomprehensible set of letters, however when wrapped around another baton of identical size the original texts appears.

The Greeks were therefore the inventors of the first transposition cipher and in the fourth century BC the earliest treatise on the subject was written by a Greek, Aeneas Tacticus, as part of a work entitled *On the Defence of Fortification.* Another Greek, Polybius later devised a means of encoding letters into pairs of symbols *using* a device known as the *Polybius checkerboard* which contain many elements common to later encryption systems (Oliver, 2001)

Cryptography is the only practical means of sending information over an insecure channel; normally in a networked environment. These channels may be computers, telephone lines, satellite etc. The increasing use of electronic means of data transfer from one point to another coupled with the growth in networking and Internet communication has extended the need to protect vital information. This vital information could be military, diplomatic, academic (for example, question papers in schools), banking (Electronic Fund Transfer, ATMs), sensitive databases (for example, Hospital Management) and e-initiatives.

Cryptosystem defines all the elements that are involved with the provision of secured communication between any two points. The process involves the sender sending a plaintext; the plaintext is transformed into a form not readable or in a disguised form called a ciphertext. The process of transforming a plaintext to ciphertext is called *encryption* or simply as *enciphering*. When this ciphertext arrives at its intended destination, it is then transformed from the ciphertext to the plaintext called decryption or deciphering.

For the receiver to be able to read the message and at the same time avoiding the plaintext being accessed by an unauthorized individual, the sender must transform the plaintext into ciphertext using some specific parameter. This parameter is called the encryption key K_e. The receiver then deciphers (interpret the ciphertext) using the decryption key K_d. In a public key cryptosystem, K_e is made public but K_d is not public. It must be kept secret, known only to the receiver. The key K for cipher and deciphering should be common to the sender and receiver.

When encrypting, the information being transmitted, and the encrypting key is fed into an encryption algorithm. When the encrypted data gets to the receiver, it is passed through a decryption algorithm so as to enable the reader have access to the information being transmitted.

In the early part of their existence, computer networks were primarily used by university researches for information transfer among academics, and by corporate organization for sharing resources such as printers, scanners, and other sharable resources in a distributed environment. Under these conditions, security was not on the priority as such shared information and resources do not pose any security risk to the sender or the receiver. Nowadays, the use of computer has gone beyond their early intentions.

They now found use in the e-initiative (e-Banking, e-commerce, e-shopping etc). These phenomenal changes have brought about the need for a secured channel for data and information transmission from network to network. The need to protect information is even more imperative as more and more are depending on technology to transact business. Our lives now depend to a large extent on technology to prosecute our daily chores.

Computers processing speed have doubled every 1½ to 2½ years (going by Moore's law). It therefore shows that a code that took a thousand years to break with the computers available in 1960 would take a year to break with the computer available in 1980, but will take few hours to break in 2001 (Peha, 1998). Computer speed has changed tremendously since 2001. Computer speed has continue to obey Moore's law to the extent that ciphers that take hours to break in 2001 will probably take minutes by today's computer. This calls for security consciousness on the part of users of computer systems.

Security is a broad topic that ranks almost first in a computer networked environment. In its simplest form, it is concerned with making sure that intruders cannot read, or worse still modify messages intended for other recipients. It is as a result of this concerned for people trying to access remote services that they are not authorized to use, that the subject of cryptography has emerged. Security also deals with the problems of modification on relayed messages and denial (non-repudiation) by people who want to claim that they never sent certain messages. Most security problems are intentionally malecious by people who want to gain some benefit or cause harm (Tanembaum, 1996).

1.2 Overview of Information Security

Cryptography is the study of Mathematical techniques related to the aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication (Menezes et al, 1997).

From time immemorial, an elaborate set of protocols (rules for communication) and mechanism for communication has been created to deal with information security issues when the information is conveyed by physical documents (such as letter writing). Mathematical algorithm and protocol alone will not always achieve the objective, but procedural techniques and the enactment of laws guiding the communication help. Letters through the Post Office for example, is provided sealed envelopes delivered by an accepted mail service. The physical security of envelope is, of practical necessity, limited and so laws are enacted which makes it a criminal offense to open an unauthorized mail. Sometimes, security is achieved not through the information itself but through the physical document recording it. For example, paper currency requires special inks and material to prevent counterfeiting.

Conceptually, the way information is recorded has not changed much over time. Information used to be stored and transmitted through paper, much of it is now stored on magnetic media and transmitted via telecommunication systems (wired and wireless). What has changed dramatically is the ability to copy and alter information. One can make indistinguishable several copies of a piece of the original information stored electronically. The means to safeguard electronic information is beyond the physical medium and depends on the digital information itself. Physical medium has ability to record documents as original.

Digital Signature

One of the fundamental tools used in information security is the digital signature. A signature scheme is method of signing a message stored in electronic form. A signed message can be transmitted over computer network. A conventional signature is always a part of the paper document being signed while signature is usually not part of digital document but signature is bind to the message. Verification is done in conventional signing by comparison with the authentic signature. Digital signature is verified by publicly known verification algorithm.

A digital signature is constructs that authenticates both the original and contents of a message in a manner that is provable to a disinterested third party (Bishop, 2003). A digital signature scheme consists of two components: a *sign algorithm* and *verification algorithm.*

A sender can sign message (*S*) using a secret signing algorithm. A signature scheme is a five-tuple (*P, A, K, S, V*), where the following conditions are satisfied:

1. *P* is finite set of possible messages
2. *A* is a finite set of possible signatures
3. *K*, the keyspace, a finite set of possible keys
4. For each $k \in K$, there is a signing algorithm $sig_K \in S$ and a corresponding verification algorithm $ver_K \in V$. Each $sig_K : P \to A$ is a function such that the following equation is satisfied for every message $x \in P$ and for every signature $y \in A$:

$$ver(x, y) = \begin{cases} true & if \;\; y = sig(x) \\ false & if \;\; y \neq sig(x) \end{cases}$$

For every $k \in K$, the function sig_K and ver_K should be polynomial-time functions with ver_K being a public function and sig_K a secret function.

The functions should be such that it is computation infeasible to forge the signed signature on message *S*. Physical signature can be forged but a digital signature should be such that cannot be forged.

1.3 Cryptographic Techniques

Any form of cryptographic technique can generally be divided into two:

1. Symmetric-key (Private-key)
2. Public-key

1.3.1 Symmetric-key (Private-key)

A symmetric-key (Private-key) cipher involves a sender (*A*) and a receiver (*B*) choosing a key *k* which eventually gives rise to an encryption rule e_k and a decryption rule d_k. In this type of cryptosystems, d_k is either the same as e_k or d_k is easily derived from e_k. Systems based on this type of encryption have a drawback. The drawback is, it requires a prior communication of a key *k* between the sender (*A*) and receiver (*B*).

In most practical systems of this nature $e = d$ from which the term symmetric-key is derived. Symmetric-key algorithm can be further subdivided into two, namely:

- Block ciphers
- Stream ciphers

1.3.1.1 Block Ciphers

In this scheme, plaintext messages are broken into strings (blocks) of fixed length *l* over an alphabet *A* and each block is encrypted one at a time. Two classes of block cipher have also being identified, namely *substitution ciphers* and *transposition ciphers*.

Substitution Ciphers

Substitution ciphers are block ciphers which replace symbols (or groups of symbols) by other symbols or groups of symbols. In this method, each or group of letters is replaced by another or group of letters to disguise it. One of the oldest known substitution ciphers is the *Caesar cipher*, due to Julius Caesar. The *Caesar cipher* algorithm allows the ciphertext alphabet to be shifted by *K* letters in a circular mode. This method is also referred to as *monoalphabetic substitution* (Tanenbaum, 1996).

The general method of shift is as follows: A letter in the message (plaintext) corresponding to nth letter in the alphabet is replaced by the $(n + k)$th letter in the alphabet with *K* being an integer (for example, K = 7) with blank as the 27th.

A substitution cipher has been defined by (Stinson, 1995) as follows:

Let $P = C = \mathbf{Z}_{26}$. K consists of all possible permutation of the 26 symbols 0, 1,…, 25. For each permutation π є K, define

$$e_\pi(x) = \pi(x),$$

and define $d_\pi(y) = \pi^{-1}(y)$

Where π^{-1} is the inverse permutation to π

Cryptograms (puzzle) in newspaper are example of substitution cipher. As an example the following plaintext can be converted to ciphertext as indicated below:

Table 1.1: Encryption with Caesar key K = 7

Plaintext	IF THE RIOT PERSISTS ATTACK
Ciphertext	**PMG OLGYPV GWLYZPZ ZGH HJR**

After the encryption using the Caesar cipher with k=7, the plaintext *IF THE RIOT PERSISTS ATTACK* becomes PMG OLGYPV GWLYZPZ ZGH HJR

Cryptanalysis of Substitution ciphers

Although this system looks secured, they can be easily broken by the cryptanalyst who after studying the alphabetic pattern, formulate what will lead to the original plaintext; using the basic statistical properties of the alphabet. Letter **e** for example, is the most commonly used letter of the alphabet followed by **t, o, a, n, i** etc. TH, IN, ER, RE, and AN are the most common two letter combination, referred to as **digrams**. THE, ING, AND, and ION are the most common three letter combinations referred to as **trigrams**. The cryptanalyst, who wants to break a ciphertext, will first study and count the frequencies of letters used. When that has been done, he assigns the most common to **E**, the next common to **T** and so on.

The next step for him will be to look at the digram and assign TH, IN ER, and so on. He can then put **E** in front of **th** to derive **thE**, this is done until all manipulations have been completed. He will then start with the Trigrams until all alphabetic manipulations using the trigrams have been completed. He may then be able to rebuild the plaintext from the ciphertext. Another approach the cryptanalyst could use is to guess words or phrases. Adewumi & Garba (2007) have suggested a method of disguising messages by converting them to systems of linear equations in the form Ax=b and find A^{-1} such that equation now becomes $A^{-1}x=b$, a disguised form of Ax=b and still transmit them as if they are of the form Ax=b. An example from the use of this method is as follows:

Adewumi & Garba (2003a, 2003b, 2003c), have also demonstrated how a message can be converted to system of equation (Linear and non-linear) in form of *Ax=b*, this is a form of substitution ciphers. It has also been demonstrated that matrix inversion can be used to disguise messages.

The example below demonstrates the use of matrix inversion to encrypt and decrypt messages.

ATTACK NOW can be encrypted as a 2 x 2 systems of equations thus:

A T T A C K
$(x_1+0)+(x_2+18)+(x_2+18)+(x_1+0)+(x_1+2)+(x_2+9)$
N O W
$(x_1+13)+(x_2+13)+(x_1+22)$

The derivation of the above variables x_1, x_2, x_3 and constants have been described and demonstrated in (Adewumi & Garba, 2003a,c).

If we use the delta coding to hide the various distances of each letter, and taking $x_1=1$, $x_2=2$, $x_3=3$; the word **ATTACK NOW** is transformed into the form Ax=b as:

$$\begin{aligned} 3x_1 + 3x_2 &= 9 \\ 2x_1 + \ x_2 &= 4 \end{aligned} \qquad \ldots (1)$$

$$\text{The matrix A} = \begin{pmatrix} 3 & 3 \\ 2 & 1 \end{pmatrix} \qquad \ldots (2)$$

If we carry out row operations on this matrix, we

$$\text{obtain the } A^{-1} = \begin{pmatrix} -1/3 & 1 \\ 2/3 & -1 \end{pmatrix}$$

Equation (1) is sent as

$$-\frac{1}{3}x_1 + x_2 = 9$$

$$\frac{2}{3}x_1 - x_2 = 4$$

This is the same as sending $A^{-1}x = b$, but this to an intruder, will look like $Ax = b$.

To decrypt, we use the algorithm for finding the inverse of *A* after obtaining:

$$A = (A^{-1})^{-1}.$$

Once the values of x_1 and x_2 have been obtained, we use delta coding algorithm described in (Adewumi & Garba 2003a, 2003c) to recover the position of the various letters used in the plaintext.

Transposition (Permutation) ciphers

Another class of symmetric-key ciphers is the simple transposition cipher which simply permutes the symbols in a block. In this method, the plaintext is divided into blocks and in turn each block is enciphered independently. Under the control of a fixed key, different occurrences of a particular plaintext block will always be encrypted as the same ciphertext block.

Generally, a transposition ciphers can be represented as follows:

Let *m* be some fixed positive integer. Let *P* = C = $(\mathbf{Z}_{26})^m$ and let *K* consists of all permutations of all permutations of {1, …, *m*}.

For a key π, we define

$$e_\pi(x_1,\ldots,x_m) = (x_{\pi(1)},\ldots,x_{\pi(m)}) \text{ and}$$

$$d_\pi(y_1,\ldots,y_m) = (y_{\pi^{-1}(1)},\ldots,y_{\pi^{-1}(m)}),$$

where π^{-1} is the inverse permutation to π.

Table 1 is an example of transposition cipher. The general approach is that, the cipher is keyed by a word or phrases not containing any repeated letters. For example, if we take BAUCHI as the key, then the entire column can then be numbered according to their position in the alphabet. The 'A' in BAUCHI will be 1 because 'A' is the first (number 1) letter of the alphabets; B = 2 because B is the second (number 2) letter of the alphabet and so on. With this in mind, the plaintext will be written horizontally, in rows. The ciphertext will then be read column by column, starting of course from the column whose key letter is the lowest.

Table 1: An Example of Transposition Cipher

B	A	U	C	H	I
2	1	6	3	4	5
T	R	A	N	S	E
E	R	O	N	E	M
I	L	L	I	O	N
N	A	I	R	A	T
O	A	C	C	O	U
N	T	F	I	F	T
E	E	N	T	W	E
L	V	E	F	R	O
M	S	I	X	F	I
V	E	S	E	V	E
N	A	B	C	D	E

Plaintext:
TRANSFERONEMILLIONNAIRATOACCOUNTF
IFTEENTWELVEFROMSIXFIVESEVEN

Ciphertext:
RRLAATEVSEATEINONELMVNNNIRCITFXEC
SEOAOFWRFVDEMNTUTEOIEEAOLICFNEISB

Cryptanalysis of a transposition ciphers

For a cryptanalyst to break a block cipher, he or she must first know that he is deAdeng with transposition cipher. One method for a crytanalyst is by observing the frequency of E, T, A, O, N, I … to see if they fit the normal pattern of a plaintext. If they do, it is then deduced that the cipher is a transposition, reason being that in this kind of cipher, every letter represent itself.

Once this is established, the next ordinary thing to do is to guess the number of columns involved. This can be achieved, if for example, the cryptanalyst suspects that a word like ***illionnaira*** occurs somewhere in the message, he can then observe the digrams like IN, LA, LI, IR, OA occur in the ciphertext as a result of the phrase wrapping round. If a key length of five were used, the digrams would have been LN, LA, II, OR, NA. Each key length will produce a different digrams from the ciphertext.

With persistent hunting for the key length, the cryptanalyst may be able to determine the key length and thereby recover the plaintext from the ciphertext. This cipher shown in Table 1.2 produces a fixed length block of input and produces a fixed-length block of output. The cipher in table 1.2 can be seen as 66 character block cipher, with the following output 2, 8, 14, 20, 26, 32, 38, 44, 50, 56, 62, 1, 7, 13, 19, 25… 62. This is to say that the second input R, is the first to be the output followed by the eight, R, and so on.

1.3.1.2 Stream Ciphers

A stream cipher generates a keystream $z = z_1z_2\ldots$, and use it to encrypt a plaintext string $x = x_1x_2\ldots$ according to the rule

$$y = y_1y_2 \ldots = e_{z1}(x_1)e_{z2}(x_2)\ldots$$

Assuming $x_1x_2\ldots$ is the plaintext string and suppose $k \in K$ is the key, the function f_i is used to generate z_i (the i^th^ element of the keystream), where f_i is a function of the key, K, and the first *i*-1 plainmtext characters: the keystream element z_i is used to encrypt x_i, yielding $y_i = e_{zi}(x_i)$.

So, to encrypt the plaintext string $x_1x_2\ldots$, we would successively compute z_1, y_1, z_2, y_2, …

Decrypting the ciphertext string y_1y_2… can be accomplished by successively computing z_1, x_1, z_2, x_2

Examples of stream ciphers

Vernam cipher

In 1917, Vernam G, invented the remarkable simple *one-time pad* in which the secret key is a sequence of randomly generated bits as shown in table 3.

This process takes a message of length *n,* enciphered it by *XOR*ing with the secret key of the same length thereby transforming it to the ciphertext. This is later deciphered by *XOR*ing with the same secret key transported to the legitimate receiver via a safe channel (Zeng, et al, 1991; Falaki and Adewale, 1998).

During the 2nd world war, many of these codes were reported broken by some cryptanalysts of those days. It was reported for example, that the Japanese messages planning the bombing of Pearl Harbor were deciphered but were not acted upon (Martin, 1991).

Table 2 Example of a Onetime Pad.

Plantext P:	**10011100111101…**
Secret key K:	**01100011000010…**
Ciphertext C:	**11111111111111…**

For a cryptographically secure one-time pad, the following three requirements must be met:

1) 1. The period of the keystream must be large enough to accommodate the length of the transmitted message;
2) The output bit must be easy to generate;
3) The output bit must be hard to predict.

That is, given the generator and the first *n* output bit, a(0),...,a(*n-1*), it should be computationally infeasible to predict the (*n+1*)th bit a(*n*) in the sequence with better than a 50–50 chance given a portion of the output sequence, the cryptanalyst should not generate other bits either forward or backward (Zeng et al, 1991).

Linear Congruence Generators (LGC) Algorithm

This is a method for generating random number for use in the one time pad. The method is based on the recurrence of the form $x_{i+1} = ax_i + b \ mod \ m$. Here, (a, b, m) are the parameters describing the generator and can be utilized as secret keys. X_0 is the seed, which must be supplied. If the parameter are carefully chosen, the numbers x_i will not repeat until all integers of the closed interval [0, m–1] have occurred. For example, the sequence generated by $x_{i+1} = 5x_{i-1} + 3$ mod 16 with $x_o = 1$ is {1, 8, 11, 10, 5, 12, 15, 14, 9, 0, 3, 2, 13, 4, 7, 6, 1, 8…} has been described in (Zeng et al, 1991)

Boyar (1989) has shown that sequences generated by this method are not cryptographically secure. He observed that given a long sequence of this nature, one can reconstruct the parameters *m, a, b* thereby rendering the algorithm worthless.

1.4 PUBLIC-KEY CRYPTOSYSTEM

In cryptosystems, the main problem has always been the key distribution. However strong a cryptosystem is, once an intruder steals the secret key, the system is worthless. The cryptosystems we discussed before now are called a *symmetric key(private-key) system.* With this approach, the sender and the receiver use the same key, and they have to keep their shared key secret from every one else. The biggest problem in this scheme is the shared key management.

With this method, communicating with several people and ensuring that each person can read messages intended for them, different secret keys are needed for each person. In the 1970s, Cryptographers developed *Public key Cryptography* in other for them to get around the problem of managing keys. Under this scheme, each person has two keys; the Private (secret) and Public keys – freely available to any one who cares to known. In this case, the public key system is asymmetric – different keys are used for encryption and decryption (Beekman, 1999).

In 1976, two researchers at Stanford University, Diffie and Hellman (1976) proposed a radical new kind of cryptosystem, one in which the encryption and decryption keys were different and the decryption key could not be derived from the encryption key. In their proposal, the (keyed) encryption Algorithm, *E* and the (keyed) decryption algorithm, *D*, had to meet the following requirements:

(i) $D(E(P)) = P$.

(ii) All (*D, E*) pain are distinct.

(iii) It is exceedingly difficult to deduce *D* from *E*

(iv) *E* cannot be broken by a chosen plaintext attack.

If we represent the plaintext by the letter **P**, **C** as the cipherxt, E_k as the encryption key D_k as the decryption key, then C = E_k(P), meaning that the encryption of plaintext **P** using key *K* gives the ciphertext *C.* in the same manner, **P** = D_k(C) represents the decryption of **C** using key ***K*** to get back the plaintext **P**. In a more general form, it can be represented as $D_k(E_k(P)) = P$.

Example of public ciphers

The RSA Algorithm

Rivest et al, (1978) at M.I.T. discovered an algorithm known as RSA (Rivest, Shamir, Adleman) the initials of their names. Their method was based on the principles of number theory and now summarized below:

(i) Choose two large primes say *p* and *q*, (this number should not be less than 10^{100})
(ii) Compute $n = p\ x\ q$ and $z = (p–1)x(q–1)$
(iii) Choose a number relatively prime to *z* and call it *d*.
(iv) Find e such that e x $d = 1$ mod z.

These parameters are computed in advance. The encryption begins by dividing the plaintext into blocks so that each plaintext P, falls into the interval 0<*p*<n. Encrypting message P, compute C=P^e(mod n).

Compute P=C^d(mod n) to decrypt; the parameter *e* and *n* are required, while to decrypt, *d* and *n* are required. This implies that the public key consists of the pair (*e,n*) while the private key is made of the pair (*d,n*). The inability to factorize large numbers, before now, makes the system secure. With the elliptic curve factorization algorithm, systems of this nature must be improved upon to make them secure. If the publicly known *n* can be factorized, then, it is easy to reconstruct *p* and *q*, which will eventually lead to the formation of *z*. Once *z* and *e* are known, *d* can be found.

Rivest and colleagues have observed that factoring a 200-digit number requires 4 billion years as at 1978, this will definitely be less now as a result of increase in computer speed. Factoring a 500-digit will require about 10^{25} years. As an example, we take p=3 and q=11 giving n=33 and z=20. A suitable value for d is 7. Since 7 and 20 have no common factor. Therefore e can be found by solving the equation 7e = 1 (mod 20), this will yield e=3. This example is represented in table 1.4.

Table 3: An example of RSA

Plaintext (*P*)				**Ciphertext (*C*)**		
Symbolic	Numeric	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Symbolic
A	1	1	1	1	1	A
T	20	8000	14	105413504	20	T
T	20	8000	14	105413504	20	T
A	1	1	1	1	1	A
C	3	27	27	10460353203	3	C
K	11	1331	11	19487171	11	K

RSA is disadvantaged in that it is slow when large volumes of data are to be encrypted and factoring large number can pose some problem.

2. SECURITY PLANNING

Planning, according to Lucey (2005) is the managerial process of deciding in advance what is to be done and how it is to be done. Planning is not an end in itself; its primary purpose is to provide the guidelines necessary for decision making and resulting action throughout the organization. Planning is done on both a formal and informal basis and the planning process uses information from internal and external sources. The process gathers, translate, understands and communicates information that will help to improve the quality of current decisions which are based on future expectations.

A security plan provides an organization with means of preventing and mitigating the effects of any security incident by relating what approaches have been effective in that environment in the past. Effective security planning must combine technology with good business and social practices. No matter how advanced and well implemented the technology is, it is only as good as the methods used in

Implementing the appropriate security standards is a key issue for most organizations. To implement security standards, devise a security plan that applies a set of security technologies consistently to protect your organizations resources.A security plan should be all encompassing in terms of physical protection and software related protection that is required to deny access to unauthorized information, backup of data, prevent unauthorized access to classified information.

A security plan will guide against common security *perpetrator* such as hackers who may want to test out someone's security system or steal information; businessmen who may want to discover competitors strategic marketing plan and use it; an ex-employee who may want to take revenge for being fired by the company; spy to learn enemy's military strength; terrorist who may want to break security codes, steal warfare secrets and destroy strategic targets. The single objective of a security plan is to enable staff act in an effective way so as to prevent and mitigate the effects of security breaches in an organization. A security plan contains an agency's plans and procedures related to security, and include other information required for staff members to implement them.

A security plan has several components. A security plan can both be physical and procedural. Physical plan may include such as the use of locks, bars and iron doors to prevent unauthorized persons to an ICT installation. While procedural planning should first identify attack patterns then suggests procedural means of solving problems in case it happens. Attacks may be

i) Denial of service
ii) Infrastructural attacks
iii) Attack against or using routers as a platform
iv) Exploitation of trusted relationship between routers

3. SECURITY POLICIES

Lucey (2005) define policies as formal expressions of the organization's culture and belief systems. The security policy of an organization therefore deals with the culture and belief systems that ensure the protection of the information assets of an organization. These assets may be recorded on paper and or stored on different form of media.

A policy must determine what assets need to be protected, determine what attacks need to be mitigated, how to mitigate the attacks including technology and procedural, and how to detect attempted attacks. In order to do justice to the above, several attempts must be made to assess the assets values, determine what attacks to be mitigated, the mitigation strategy and the attack detection.

3.1 Some Policy Issues

3.1.1`Key Management and Public Key Infrastructure (PKI) Policy

Public Key Infrastructure has a single purpose of establishing a trust which is to bind encryption keys and identities together.

To have a robust PKI infrastructure the following are required:

i) The creation of appropriate bindings between public/private keys and identification.

ii) The user of a *private certificate* must provide security mechanism to protect the private information.

iii) Even though the *public certificates* do not have the same criticAdety, the security policy should address the procedures for releasing the public certificate for use.

iv) A mechanism for tracking the *lifetime expiration date* in advance to actual expiration needs to be addressed.

v) Policies/procedures for replacement and *renewal of older certificates* or revoked certificates need to be developed.

Diffie-Hellman Key Exchange

Diffie-Hellman is the best known key agreement protocol. The algorithm is represented in Figure 3.

i) U chooses α_U at random, $0 \leq \alpha_U \leq p\text{-}2$

ii) U computes $\alpha^{\alpha U}$ mod p and sends it to V

iii) V chooses α_V at random, $0 \leq \alpha_U \leq p\text{-}2$

iv) V computes $\alpha^{\alpha V}$ mod p and sends it to U.

v) U computes and V computes

Figure 3.1: Diffie-Hellman Key exchange.

As an example, the following example is used to underscore the concept a key exchange scheme

A Key Exchange Challenge Response Algorithm

1. Sender *S* and Receiver *R* agrees on two very large prime numbers say *p* and *q,* with (p-1)/2 also a prime number. Usually, these prime numbers should be more that 100 digits in length.
2. Sender *S* picks a very large number *α* and keeps it secret
3. Receiver *R* similarly picks a very large number *β* and keeps it secret.
4. Sender *S* initiates conversation by sending his message, which is converted to system of equations. In addition, he sends (p, q, q^{α} mod p) to the receiver *R*.
5. When receiver *R* receives the message from the sender *S* containing a challenge for identification; the receiver will respond to the challenge from the sender with a message containing (q^{β} mod p). This computation is however done manually, as only the result of (q^{β} mod p) is required in the challenge and not the formula. The system takes the supplied number by the receiver and raised it to the power of *α*, that is, $(q^{\beta} \bmod p)^{\alpha}$.
6. Using the law of modular arithmetic,

$$(q^{\beta} \bmod p)^{\alpha}$$

$$= (q^{\alpha} \bmod p)^{\beta}$$

$$= q^{\alpha\beta} \bmod p$$
$$\alpha, \beta \in N$$

= *m (*The secret number for communication between ***S*** and ***R*).**

3.2 Intrusion Detection

Any developed policy worth its salt must include the ability to detect and attempt to prevent intrusion. Issues to deal with in intrusion are:

i) How to detect that an intrusion has occurred and how to report/coordinate the fact that there has been an intrusion.

ii) Intrusion detection is a local issue and may vary based upon the communication media/technology/protocol that is being employed. There are two types of intrusions to be considered: passive (e.g. eavesdropping) and active where the intruder is actively attempting to access a particular computational resource.

Passive intrusion is difficult if not impossible to detect. Thus intrusion prevention becomes a key issue. Passive intrusion (e.g. eavesdropping by a network analyzer) can be prevented through the use of encryption and monitoring/controlling network access (e.g. managed switches). In a radio environment, intrusion can't be prevented, but eavesdropping can be prevented through the use of encryption that prevents a real security issue of information disclosure.

The active intruder can be detected through means that are local to the resource. However there needs to be a framework in which the detection can be coordinated, verified, and reported. There are no relevant standards in regards to intrusion detection frameworks. However, the closest is the Communication in the Common Intrusion Detection Framework (CDIF). The following are key attributes of an integrated intrusion detection technology/framework that should be considered:

- A detection framework must be able to communicate over the wire in a standardized manner.

- A intrusion detection technology must be able to securely contact the proper peer components.
- There must be a mechanism to locate peer components in a secure manner.
- There must be a mechanism for verifying each partner's authenticity and access privileges.
- Additionally, an intrusion detection technology should integrate with the audit framework/technology.

Smart Cards

Smart cards can be used to contain personal identification information (e.g. username/passwords), digital certificates, biometric information, and other types of information. Therefore, the credential types they contain typically address the credential aspects of a smart card. The major policy issue, specifically related to smart cards, is the development of policies/procedures relating to the serialization of the smart cards.

Digital Certificates

There is a major issue regarding digital certificates, and that is the handling of revocation. Certificate Authorities (CAs) typically maintain Certificate Revocation Lists (CRLs) that are updated on a twenty-four (24) hour interval. A certificate that has been placed on a CRL is no longer trustworthy and therefore should not be useable. Policies and procedures should be developed to specify a periodicity to check the CAs CRLs and how to disseminate this information within the security domain. The NERC DEWG has expressed a major concern in this area and further policy study in order to develop a specific recommendation is warranted.

3.3 Identifying attack patterns

Attack may be any of these two – active and passive attacks. An active attacker usually attempts to delete, add, or try to alter the transmission on a channel. A passive attacker on the other hand, monitors the communication channel to threaten confidentiality. Intruders, who may be *active* or *passive,* use different attack patterns to intrude into a network. Such identified patterns are:

- Network packet sniffers
- IP spoofing
- Password attacks
- Distribution of sensitive internal information to external sources
- Man-in-the-middle attacks
- Scanning for potential victims
- Increasing Threat from Infrastructure Attacks
- Exploitation of a trusted link
- The use of malicious codes
- Attacks on the Internet Domain Name System (DNS) such as:
    - Cache Poisoning
    - Compromised Data
    - Denial of Service
    - Domain Hijacking

3.4 Methods for reducing network intrusion

1 The following practices can minimize network intrusion:
2 Ensure all accounts have passwords that are Ensure all accounts have passwords that are difficult to guess.
3 One time passwords are difficult to guess. One time passwords are preferred.
4 Use cryptography
5 Use secure programming techniques when writing Use secure programming techniques when writing software
6 Regularly check for updates, fixes and patches
7 Regularly check for security alerts

Available technologies for reducing network intrusion are:

1 • One time passwords
2 • Firewalls
3 • Monitoring Tools
4 • Security Analysis Tools
5 • Cryptography

4.0 DESIGN ISSUES IN SECURITY SYSTEMS

4.1 Techniques to preserve confidentiality against active attacks

4.1.1 Signature /certificate schemes

A signature is used in everyday life to bind the signer of a document to the document s/he endorses. It is usually a fundamental issue for non-repudiation.

The purpose of a digital signature is to provide a means for an entity to bind its identity to a piece of electronic information. Signing involves transforming the message and some secret information held by the entity into a tag called a signature. A digital signature has two parts – the signing and the verification algorithms. Just like the verification of a physical signature is done by comparing it to an authentic signature, the digital signature however usually verify a publicly verification algorithm.

In a signature scheme, the following holds:

i) *M* is a set of messages that can be signed

ii) *S* is the set elements called the signatures

iii) S_A is a transformation from the message set *M* to the signature set *S*, and is called a signing transformation for entity *A*. The transformation S_A is kept secret by *A*, and will be used to create signatures for messages from *M*.

iv) V_A is a transformation from the set *M x S* to the set {true, false}. V_A is called a verification transformation for *A*'s signatures, is publicly known, and is used by other entities to verify signatures created by *A*.

4.2 Secret sharing schemes

Secret sharing schemes are popularly used in mission-critical situations like the launch of missiles, opening of bank vaults, corporate secrets, start of war, key management, securing classified documents etc. In a (*p,n*) secret sharing scheme, any *p* –out-of-*n* participating members can reconstruct the original shared code but not less than *p* participating members can do so. The shareholders must form a *quorum* to be able to reconstruct the original shared value. When a *quorum* is not formed, any combination of < *p* participants cannot reconstruct the shared code.

To provide an appropriate use of secret sharing scheme, we illustrate it with this example. Assuming a 9-man Election Tribunal Justices desire to protect their judgment from public knowledge before judgment is delivered. They decided to lock up their judgment in a cabinet. They agree that any five judges can open the cabinet to retrieve the document, but not less than 5 can do so. To achieve this, they will need ${}^9c_5 = 126$ padlocks to secure the cabinet. This is prohibitive and impracticable in real life. A secret sharing algorithm will achieve the justices' desire without having to purchase 126 padlocks to secure the cabinet.

A secret sharing scheme is a method of sharing a key *S* into pieces (called shadows) among a set of *p* participants called the shareholders such that any *p* shareholders forming a quorum can reconstruct the value of *S* but no group of less than *p* participants can do so. Usually, a person known as the *Dealer* (*D*), $D \notin S$ chooses the key *S*. The dealer gives some partial information called shares to each participants which must be secretly distributed such that no shareholders knows the share that has been given to another shareholder.

When there is need to reconstruct the key *S* some participants' ≤ *p* will pull together their shares to reconstruct *S*. This scheme is represented below by Shamir's (*p,n*) –threshold scheme in Z_m [Stinson, 1995]

1. *D* chooses *w* distinct, non-zero elements of Z_m, denoted by x_i $1 \le i \le w$, for $1 \le i \le w$, *D* gives the value x_i participant p_i. The values x_i are public
2. Suppose *D* wants to share a key $S \in Z_m$. *D* secretly chooses (independently at random) *p-1* elements of¦.
3. For $1 \le i \le w$, *D* computes $y_i = a(x_i)$ where
$$a(x) = S + \sum_{j=1}^{p-1} a_j x^j \bmod m.$$
4. For $1 \le i \le w$, *D* gives the share y_i to p_i.

Suppose that participants $p_1, \cdots, p_n$ want to determine *k*. They know that $y_{ij} = a(x_{ij})$, $1 \le j \le n$, where $a(x) \in Z_m[x]$ is the (secret) polynomial chosen by *D*. Since a(x) has degree at most p-*1*, a(x) can be written as $a(x) = a_0 + a_1 x + \cdots + a_{p-1} x^{p-1}$, where the coefficients $a_0, \cdots, a_{p-i}$ are unknown elements of Z_m, and $a_0 = S$ is the key.

For a *(p,p)*-threshold scheme, where all participants must pull shares together before *k* can be reconstructed. A *(p,p)*-threshold scheme is described below:

1. *D* secretly chooses (independently at random) p-*1*elements of ;using a chosen polynomial
2. *D* computes

$$y_p = S - \left[\sum_{i=1}^{p-1} y_i\right] \bmod m \;\ldots (1)$$

3. For $1 \le i \le w$, *D* gives the shares y_i to P_i

The formula use by *p* participants to compute *S* can be represented by $k = \left[\sum_{i=1}^{p-1} y_i\right] \bmod m \;\ldots (2)$

Shamir (1979) identified some properties of a (*p, n*) threshold scheme as follows:

1) The size of each piece does not exceed the size of the original data.
2) When p is kept fixed, D_i pieces can be dynamically added or deleted (e.g., when executives join or leave the company) without affecting the other *D*, pieces. (A piece is deleted only when a leaving executive makes it completely inaccessible, even to himself.)
3) It is easy to change the D_i pieces without changing the original data *D*
4) Adewumi and Garba (2008) have use this scheme to devise a method that uses a polynomial of the form

$$f(x) = 7x^2 + 8x + 40[mod41]$$

to share codes amongst shareholders (participants) and it was also shown how shareholders could come together to reconstruct the shared message when participants submit their shared code for this reconstruction.

4.3 Multilevel security schemes for Relational DB

Current protocols for exchange of secure data (Http and wireless protocols). Operational tools necessary for analysis and resolution of problems w.r.t effective filters and firewalls, tracing sources of attack and systems recovery.

5. Security Controls

Control is the activity which measures deviations from planned performance and provides information upon which corrective action can be taken either to alter future performance so as to conform to the original plan, or to modify the original plans.

Cyber crimes are crimes committed via the use of a computer for the purpose of using:

- The computer as a target – attacking the computers of others (spreading viruses is an example).
- The computer as a weapon – using a computer to commit traditional crime that we see in the physical world (such as fraud or illegal gambling).
- The computer as an accessory – using a computer as a fancy filling cabinet to store illegal or stolen information.

We will be looking at a few of this cyber crimes and their implication

Virus attacks

A virus is a program that has been written to affect the normal operation of a computer. These viruses are written by programmer for different reasons and spread by different media to get the host computer to affect its normal operations. The aim of the programmers that write these virus programs most of the time is to compete to find out who is better than the other. Other reasons include a disgruntled staff of an organization who is trying to get back at his organization for discrepancies between the programmer and the organization. But the long-term effect of these viruses will disrupted the normal operation of organizations. There are over a million known viruses and the number increases everyday as new viruses come out on a daily basis. The greatest media of transmitting these viruses is the information super highway **the internet**. The internet connects users worldwide leaving their computers vulnerable to malicious attacks. It is also transferred by means of movable media like diskettes, usb etc. Viruses can come with email attachments, downloadable free files on the net such as software, music or by just surfing the web.

There are anti-virus software that can help remove viruses. Eg Norton MacAfee

Symptoms of Viruses

a) System becomes extremely slow
b) Undisclosed music playing in the background
c) Display of funny characters on the screen
d) Replication of files

e) Messages coming on the screen
f) Computer refuses to boot
g) Loss of data
h) Etc

Hacking

This is unauthorized access by a user in into a system for the purpose of retrieving data, manipulating data or deleting data. Hackers are major treat to any organization that has sensitive data that are connected in any form on a network, especially the internet. Hackers log into systems such as bank systems to transfer to their account, delete vital information that may fold up an organization or retrieve information and make it accessible to the public on the internet. The populations of hackers are usually students within the ages of 10 to 25 and hack in to systems just for the fun of it.

Unfortunately hacking into a system is relatively not too difficult as there are online sites that give tutorials on how to hack into systems and give free software to achieve these purposes.

Most of this software's can remotely take over your computer system, shutdown or restart the computer remotely, format the host machine, delete registry information and retrieve sensitive data. The term hacker, previously applied to rough and ready breed of computer enthusiasts, became synonymous with computer crimes. In 1989 computer users braced for the infectious outbreak of a **columbees day** virus that was set to do its dirty work on a Friday the thirteenth. It would attack the hard disk of unprotected personal computers erasing crucial elements that could be restored only by a process that would erase everything else on the disk. This incident proved not to be as serious as was feared, partly because many wary computers steal the long standing pattern of poor computer security and control prevails in many place. In many companies, existing protection and control were far adequate for the several reasons:

i. Control is inconvenient. Most techniques that deter illegitimate users are equally effective at hindering legitimate users,
ii. companies want to be seen as secure and in control many computer crimes have gone unreported because chief executive worry about what would happen to their company's image should they acknowledge that the were a victim.
iii. You cannot just throw technology at a security problem, you must always be aware that security control is primarily a human problem, not a technical one.
iv. The greatest threat to your computer and data comes from inside your organization and not outside. The person most likely to invade your computer is not a youngster in some other parts of the country, but an employee who is currently on your payroll
v. The next most likely threat is an employee who until recently was on the payroll. That means the best security control techniques are not usually those that rely on technology, but those that concentrate on the human elements
vi. Awareness of the problem is not enough. As always, it is a necessary first step towards a solution, but it is not the final step

The result has been an increased emphasis on computer security control. It also meant that security control is increasingly the responsibility of all managers, not just those who have the charge of computer systems. As personal computers proliferate, so do the security risks, not only from the machines but also from their operators

5.1 Safety of Management Information Systems

Rapid changes in technology are reshaping the way organizations do business, but they also raise new risks for these organizations. The Internet, wireless communications, and today's computer software applications no longer just support the business with information. Safety of Information Systems has to do with access controls which should prevent unauthorized use of (EDP) Electronic Data Processing equipment, data files and computer software (programs). The specific control includes both physical and procedural safeguards. Access to computer hardware should be limited to authorized individuals, such as computer operators. Physical safeguards include the housing of equipment in an area that is separate from user departments. Access to the area should be restricted by security guards, door locks, or special keys.

Access to data files and programs should be designed to prevent unauthorized use of such data.

Access to program documentation and data files should be limited to individuals authorized to process, maintain, or modify particular systems.

Adewumi (2006) have suggested a number of measures to safeguard information transfer in Nigeria.

These measures include:

1. Registration of all cyber cafes in Nigeria
2. Design of an email tracking system to monitor and sniff all emails emanating from Nigeria to regulate the incidences of mail scams. The suggestion identified Economic and Financial Crime Control (EFCC) as the agency to handle this system.

In this model, a growth rate was determined which we hoped will cause scams messages to fizzled out this country if well implemented by government.

General controls

Evolving technology changes the way controls are implemented. These days, business controls have moved into Information Technology (IT) infrastructure and beyond, into the systems of third parties where control is not under the direction of many parties that must rely on it. General IT controls can be described in various forms and they relate to the environment in which application exists and are being used. Internal control assessment is important to decisions about control reliance and assurance testing.

The various forms of controls are described below:

Data and procedural controls

Data and procedural controls provides a framework for controlling daily computer operations, minimizing the likelihood of processing errors, and assuring the continuity of operations in the event of a physical disaster or computer failure. The control functions involve:

i. Receiving and screening all data to be processed
ii. Accounting for all input data
iii. Following up on processing errors/update
iv. Verifying the proper distribution of output.

The ability to maintain the continuity of computer operations involves:

i. the use of off-premises storage for important files, programs, and documentation.
ii. physical protection against environmental hazards.
iii. formal record retention and recovery plans for data and; arrangements for use of BACKUP facilities at another location in the event of a disaster.

A good procedural security programme should include:

- A written policy that spells out employees' responsibility provides a means to detect violations, and have enough management control to make sure it is properly implemented.
- Existing management control should be reviewed regularly to make sure they kept up with the development of your computer systems.
- Your procedures should maintain control over processes, computer use and access to programs and data
- Requires regular test of your security system, make such it is adequate and employees are observing the proper procedures.
- Be prepared to take action against any one caught misusing the system. This can range from minor disciplinary action to criminal charges if necessary. Be ready to take action even if it might mean bad publicity for the company.
- Management official and members of the technical staff should stay in touch to discuss security needs and problems

Preventive controls protect organizations against undesirable events, but they are rarely 100 percent effective. Examples of these systems include automated systems that:

(i) Bar unauthorized systems access
(ii) Require identification and passwords to access or enter data .Restrict user overrides
(iii) Prevent books from being closed when are missing transactions.

Detective controls

This type of control identifies events that have already occurred; they include warnings, exceptions, and edit checks. Detective controls are a major focus of evaluation because detection of errors by audit testing may point out weaknesses in controls. Since speedy detection is vAded, these controls should alert users or management to irregularities and unexpected errors as soon as they occur. They also provide a redundant view of potential errors to provide assurance that protection is functioning. This type of controls must be carefully design to avoid false alarms and time consuming analysis about whether a problem exists. Monitoring is an important detective controls that warns of problems and reports real-time status for positive confirmation that operations are running smoothly.

Application controls

The following three groups of application control are widely recognized:

i) Input controls
ii) Processing controls
iii) Output controls

Input Controls

These are designed to provide reasonable assurance that data received for processing have been properly authorized. Processing Controls are used to provide reasonable assurance that the computer processing has been performed as intended for the particular applications. These controls should prevent data from being lost, added, duplicated, or altered during processing. Processing controls take many forms, but most common are programmed controls incorporated into the individual applications software.

Output Controls

They are designed to ensure that the programming result is correct and that only authorized personnel receive the output. Control over the distribution of output is usually maintained by the data control group.

Administrative control

Security control is a management responsibility. On the front line of today's security efforts are managers in marketing, purchasing or training; even manager whose departments do not use computer at all. Everyone in the organization shares the responsibility. Even the most sophisticated security measures can be rendered useless by a user's careless mistakes. Managers must teach and motivate their subordinates to avoid these errors. More importantly, from the viewpoint of a non-technical manager, the most serious security threat in nearly every organization comes from the disgruntled employee or ex-employee. The manager who maintains a certified, well-motivated work force does as much for security as the technician who installs an access control system.

Several factors have combine to extend the responsibility for internally controlled computer security to non-technical managers as follows:

- The rise in the use of personal computers has increased. Millions of office workers now have PCs on their desk. Many are linked to other PC via local area networks (LANs), many also have links to the bank of data in corporate networked systems. The increasing use of database servers on both PCs and large computers will make the organization's data even more vulnerable to error and sabotage.

- Those millions of PCs also have millions of people who know how to operate them who are far from being an expert. At best these people have learned the mechanics of application programs they use regularly in their jobs. Many other employees, however, have become computer experts. What was once a specialized profession has been joined by a host of learned semi-professionals, untold numbers know enough to cause real trouble?
- The vast increase in computers and computer users has been accompanied by an equally vast increase in the amount of information stored and processed in computers. This is the information age, as no doubt you have heard. Organizations live and die by the information they process and most of that priceless information is stored in computer.

Other important issues in administrative control involve the organizations, procedures and records you establish. They should be set up so that activities proceed according to management's wishes, and leave audit trails of accountability as they do so. It also includes most of the personnel controls designed to prevent present human factor.

Controlling the human factor involves a full range of security factors, including such basic security precautions as limiting access to sensitive data. In addition, you should consider personnel controls such as:-

a) Providing clear job descriptions
b) Separating duties so no one has beginning to end control over the entire system analysts, operators, and data entry employees are separate positions, each working with only a part of the system. Control is more difficult in a

microcomputer system where one person takes all these functions.

c) Enforcing minimum length vacations. This has been a standard practice in banking. An embezzler usually needs frequent access to the books to keep covering up the theft. An enforced two-week vacation interrupts the criminal sequence.

d) Having key employees bonded

e) Rotating employees among shifts, computers, or projects

f) Maintaining logs of which uses programs and data files

g) Maintaining physical security. Consider establishing areas where even programmers and systems analysts are not allowed to enter

h) Maintaining a password system that will admit only those who have current authority to use the computer

i) Collecting key identification cards and other security items as soon as departing employees leave

j) Developing a motivation campaign to make all employees aware of your security needs

k) Establish a system of internal auditors, independent of any computer-using department

After the job is over, many employers continue to look the other way even after current employees are caught in security violations. Again, the inability to admit that you have a problem gets in the way of a solution.

Internet Threats

Favored techniques for compromising targeted systems include identifying known vulnerabilities in software and exploiting those vulnerabilities using readily available software tools. Many attacks succeed because organizations fail to apply software patches provided by vendors to remedy known vulnerabilities in their products. Sometimes vulnerabilities are discovered and exploited before a patch is available, but most exploits succeed because maintaining software patches on the computer is manually and/or otherwise improperly handled.

Once a vendor stops supporting the older version of an operating system, software patches are no longer provided when new vulnerabilities are discovered. To reduce costs, software vendors have drastically shortened the time frame to support older operating systems. System users are therefore required to upgrade to newer operating systems to not only get the new functionalities, but to reduce the exposures created by having older, unsupported systems within the enterprise. Failure to upgrade unsupported systems can introduce unacceptable risks to the organization.

The internet, in its ever-evolving state, is becoming a serious method of business communication and data transfer. As such, banks and other financial institutions are beginning to use the Internet as a new vehicle for doing Internet allows banks to offer both new services and new levels of convenience for existing services, and allows the consumer to interact from any computer capable of making the appropriate connection. Because of this popularity, there are many policy decisions involving security, technology, and other matters that financial institutions have to consider before making full-featured banking services available on the Internet. With the introduction of banks that exist solely on the Internet and have no physical presence of consumers to interact with the institution, regulators should be requiring all the same safeguards required of real banks. This move would create uniformity among all financial institutions.

Security and transaction fraud are important issues that banks have to deal with, because the remote access nature of the Internet obviously makes a bank’s identification to customers a more serious risk as compared to walk-up services. Banks developing security technology will lower their risk, but as with all technology, increases on one of the balance often raise the level of sophistication on the other side as well. Recent studies show that potential consumers on the Internet are unwilling at this stage in its technological evolution to give personally identifiable information for fear of fraud (not to mention direct marketing).

6. CONCLUDING REMARKS

The concern over accessibility to financial records is a real and serious one, and has long been a concern in the banking industry and other financial institutions. The appearance of banks on the Internet simply magnifies the problem by potentially exposing bank information to the full range of Internet users. This paper provides an overview of the role ICT plays in the delivery of banking services alongside common impacts and challenges in Africa. Following this introduction, a foundational overview of banking activities, ICT, and its role in banking is presented prior to the discussions on application of ICT components in the execution of banking services in the third section. In addition to its application in banking services, the third section also presents relevant architectural, processing, and infrastructural considerations applicable in banking. Section four and five illustrate ICTs impact and challenges respectively drawing on implementation examples from the Continent. We concluded by summarising the discourse and provide directions for future development

REFERENCES

Adewumi, S.E. and Garba E.J.D (2003a), *A cryptosystems algorithm using systems of non-linear Equations.* Iranian Journal of Information Science and Technology **1**(1): 43-55.

Adewumi, S. E. and Garba E. J. D. (2003c), *Securing Transborder Messages: An Encryption Standard for developing countries.* In Proceeding of the Fourth Annual Global Information Technology Management World Conference. June 8-10, 2003. Calgary, Alberta, Canada. 84-87

Adewumi, S. E (2006) Safe Nigeria: *An Agenda For Reducing Internet Scam Experiences (ARISE).* Journal of Information and Communication Technology (ICT) EBSU Abakaliki, ISSN 0794-6910. **2(2)**; 17-20.

Adewumi, S. E; Garba E. J. D (2007) *An Algorithm For Encrypting Messages Using Matrix Inversion.* Science World Journal, Faculty of Science, Kaduna State University. Vol 2, No 4. www.scienceworldjournal.org

Adewumi, S.E. and Garba E.J.D (2008), *An improved Secret Sharing Algorithm.* Science World Journal 3(1): 39-41.

Beekman, G. (1999)**,** Computer Confluence *Addison – Wesley Longman Inc. California.* pp. 170-171, 290-300.

Bishop M. (2003) *Computer Security – Art and Science.* Pearson Education(Singapore) Pte Ltd Indian Branch, Delhi 110 092 India.

Falaki, S. O. and Adewale O. S. (1998)**,** *A review of Architecture of the Post- RiscProcessors* in Kehinde L.O and Adaguno E. R Proceedings of Computer Association of Nigeria **9: 1**6-24.

Lucey T. (2005) *Management Information Systems.* BookPower High Holborn, 50-51 Bedford Row, London.

Oliver P. (2201), Crytptology: A mathematics Essay. Available at http://www.ridex.co.uk/cryptology/# Toc439908874

Menezes, P., van Oorschot, Vanstone S. (1997) *Handbook of Applied Cryptography*. CRC Press. Available at www.cacr.math.uwaterloo.ca/hac

Peha, J. M. (1998), *Encryption issues* available at:http://www.ece.cmu.edu/~peha/encrypt.pdf

Stinson D. (1995) *Cryptography: Theory and Practice.* CRC Press

Tanenbaum A. S. (1996)**,** *Computer Networks* Prentice Hall, New Jersey pp. 577-766

Zeng K, Yang C, Wei H, Rao T.R.N (1991) *Pseudorandom Bit Generators in stream-cipher cryptography*. IEEE trans. computers **24**(2): pp. 8-17