American Journal of Networks and Communications
2013; 2(2): 47-55
Published online June 10, 2013 (http://www.sciencepublishinggroup.com/j/ajnc)
doi: 10.11648/j.ajnc.20130202.14

Cryptography: salvaging exploitations against data integrity

A. A. Ojugo[1], A. O. Eboka[2], M. O. Yerokun[2], I. J. B. Iyawa[2] , R. E. Yoro[3]

[1]Department of Mathematics/Computer, Federal University of Petroleum Resources Effurun, Delta State
[2]Department of Computer Sci. Education, Federal College of Education (Technical) Asaba, Delta State
[3]Department of Computer Science, Delta State Polytechnic Ogwashi-Uku, Delta State

Email address:

ojugo_arnold@yahoo.com(A. A. Ojugo), maryarnoldojugo@gmail.com(A. A. Ojugo), an_drey2k@yahoo.com(A. O. Eboka), agapenexus@hotmail.co.uk(M. O. Yerokun), iyawaben@hotmail.com(I. J. B. Iyawa), rumerisky@yahoo.com(R. E. Yoro)

To cite this article:

A. A. Ojugo, A. O. Eboka, M. O. Yerokun, I. J. B. Iyawa , R. E. Yoro. Cryptography: Salvaging Exploitations against Data Integrity. *American Journal of Networks and Communications.* Vol. 2, No. 2, 2013, pp. 47-55. doi: 10.11648/j.ajnc.20130202.14

Abstract: Cryptography is the science and art of codes that makes it possible for two people to exchange data in such a way that other people cannot understand the message. In this study – we are concerned with methods of altering data such that its recipient can undo the alteration and discover the original text. The original text is called plaintext (PT) while altered text is ciphertext (CT). Conversion from PT to CT is called encoding/enciphering as codes that result from this process are called ciphers. The reverse operation is called decoding/deciphering. If a user tries to reverse the cipher by making meaning of it without prior knowledge of what method is used for encoding as the data was originally, not intended for the user, the process is called cracking, while such a user is a called a cryptanalyst. Cryptography is about communicating in the presence of an adversary (cryptanalyst) – and it embodies problems such as (encryption, authentication, key distribution to name a few). The field of cryptography and informatics provides a theoretical foundation based on which we may understand what exactly these problems are, how to evaluate protocols that purport to solve them, and how to build protocols in whose security we can have confidence. Thus, cryptography is the only practical means of sending and receiving data over an insecure channel from source to destination in such a way that other users cannot understand the message unless it was intended for them. Data sent over public network is not safe and the more ciphertext a cryptanalyst has, the easier it is to crack the ciphers. Thus, it is good to change the coding mechanism regularly – because, every coding scheme has a key set.

Keywords: Ciphertext, Plaintext, Encryption, Decryption, Pseudo-Random Numbers, Ciphers

1. Introduction

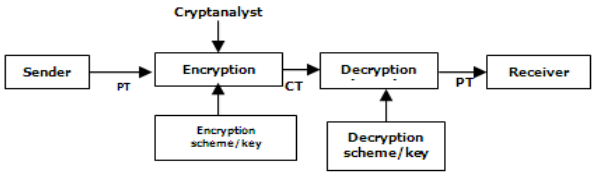
Information as a veritable tool for decision-making has been an integral part of our society and its transfer has led to advancements in data processing activities with advent of information and communication technology (ICT) devices. Conceptually, how data is recorded has not changed over-time (from paper to electronic). The dramatic change has been in the way it is copied and altered. Originally, paper data can be copied but its original can be distinguished from duplicates. With electronic data, it is impossible to distinguish original from copies [5]. Advent of network to ease data transfer has raised security alerts – though Internet was first used in military applications, but later employed in other facets to allow the sharing of expensive hardware and software resources. Now, data integrity and security has become a threat due to e-initiatives (such as e-Commerce, e-banking etc). These changes have upgraded security alert as well as its consciousness in users – as there are always intruders whose job, is to steal data. The use of Internet for data transfer has demerits that have led to the field of *Data Security* and *Cryptography* [5, 6].

Cryptography is the science and art of cipher/codes that allows two users to exchange data in such a way that other users cannot understand – through the use of data altering schemes such that only an intended recipient can undo and discover the original text sent by the sender. The original text is a plaintext (PT) while altered text is called ciphertext (CT). The conversion from PT to CT is encoding; while its reconversion is decoding. An unintended user that tries to undo the change without prior knowledge of encoding/decoding method used is a cryptanalyst – and the process of undoing alterations is *cracking* [1].

Cryptography is the only computationally secure and

practical means of transferring data over an insecure channel in such a way that other users cannot understand the message unless it was intended for them. Data sent over public network is not safe and the more ciphertext a cryptanalyst has, the easier it is to crack. Thus, it is a good idea to change the coding scheme regularly – as every coding scheme has a key set. If a different key-set is used daily, there may never be enough ciphertext to decode sent data. Though effective, its demerits is that the user also has to device a means of generating new keywords and making sure such keywords are sent over secure network to the intended recipient [1]. Cryptography is as old as writing but until the advent of computers – a major constraint in cryptography (as used during the war) has been the ability of the code clerk to perform needed transformations and switch from one cryptographic method to another (on battlefield) with little equipment, as it entails retraining a large number of persons. There was danger of the code clerk being captured, making it essential to change the cryptographic method instantly as the need arose [2].

System and elements used in these processes that make it impossible for a cryptanalyst to deduce meaningful data is called a *cryptosystem* – such that in encrypting, the transmitted data and encryption key is fed into the encryption algorithm before being sent so that on arrival of the data at its destination, the recipient passes the data via a decryption algorithm in order to have access to the transmitted data [5].



1.1. Cryptographic Goals and Tools

Figure 1: *A Cryptographic System*

The goals of cryptography includes to aid data confidentiality and privacy, integrity, authentication and non-repudiation – all services that prevents an entity from denying previous actions taken. All these are resolved via the use of digital signatures and some tools as in fig. 2 below, which are evaluated based on: (a) Security Level – is upper bound on the amount of work necessary to defeat the objective, (b) Functionality – primitives can be combined to meet various security goals, (c) Operation – tools can be applied in various ways with various input to exhibit different characteristics and different primitives help provides different functionality depending on its mode of operation, (d) Performance – is the efficiency of the primitive's mode of operation and the number of bits per seconds that it can encrypt, (e) Key Space Size – a set of keys generated and sent over secure line for encryption and decryption and (f) Implementation – difficulty of implanting its complexity in software and/or hardware environment [4].

The importance of these criteria is much dependent on the application and resources available that in some cases, there are tradeoffs of high-level security for better performance/memory. Fig. 2 are primitives and types of ciphers available, generally classified into *symmetric* and *public* key. Symmetric key ciphers include *block* (substitution, transposition and product) and *stream* ciphers.

1.2. Substitution Ciphers

In a substitution cipher, one character is substituted for another. Here is a simple example:

```
    A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
E = ---------------------------------------------------
    R Z B U Q K F C P Y E V L S N G W O X D J I A H T M
```

Figure 3 *shows the encoding key set E*

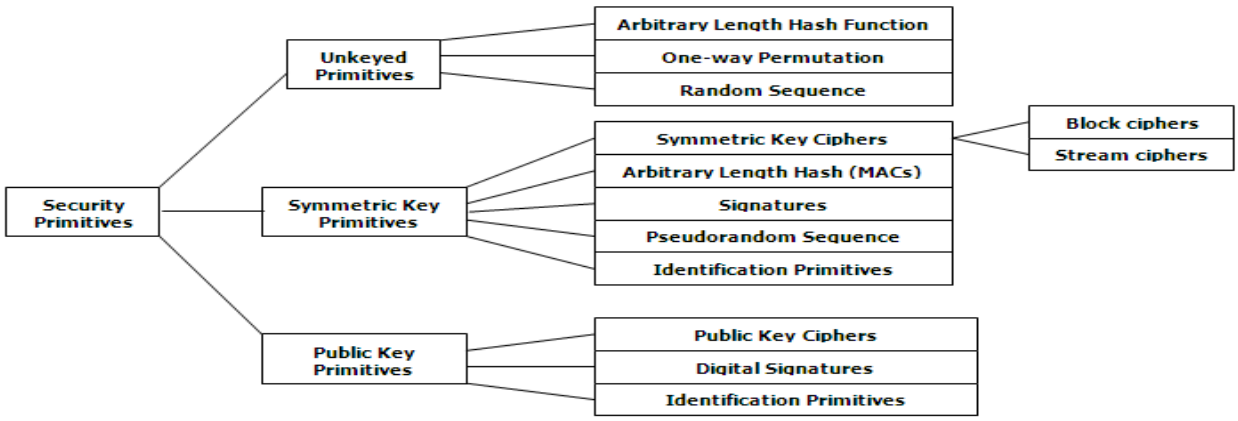


Fig. 2: *Primitive tools for an encryption model*

To encode data, we use E as in fig. 3 by selecting a character from upper line, and replacing it with those characters oppositely below – so that we encode the word "FORECAST" to be "KNOQBRXD". To decode, the user reverse the process by taking "K" in the lower line, and finding its matching letter above to get "F", which is same as first letter

– and so on. If the intended user has a lot of data to decode, it is easier to invert fig. 3 to get fig. 4, making it easier to decode.

```
    A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
E = ---------------------------------------------------
    W C H T K G P X V U F M Z O R I E A N Y D L Q S J B
```

Fig. 4: *Inverted key E rearranged with their corresponding opposite keys*

Substitution ciphers are easy to crack since English (or any other language) have certain letters that appear more frequently. A list of English letters approximately in percentage order of usage are: E: 12.7%, T: 9.1%, A: 8.2%, O: 7.5% and others are J: 0.2%, Q: 0.1%, Z: 0.1%. Thus, E T A O I N S H R D L U C M W F G Y P B V K X J Q Z.

Take the short passage that follows:

NOT NUA JMPETZ UTST ZENNELV EL NOT JEGELV SAAW, UMENELV KAS NOTES OAZNTZZ, UOA UMZ ZJEVONJX PTJMXTP. NOT PMCVONTS AK NOT KMWEJX UMZ UENO NOTW, AL NOT NOTASX NOMN ZOT UACJP QTTY NOT GEZENASZ ADDCYETP PCSELV NOT UMEN. NOT DOEJP UMZ YTSOMYZ ZEI XTMSZ AJP, ZLCR LAZTP, RCDQ NAANOTP MLP RTZYTDNMDJTP. ZOT WMELNMELTP M PTTY ZEJTLDT MLP NOT NUA JMPETZ YTTSTP PACRNKCJJX MN OTS. KELMJJX, ALT AK NOTW WCNNTSTP NA NOT ANOTS, "LAN GTSX Y-S-T-N-N-X, E KTMS," DMSTKCJJX ZYTJJELV NOT QTX UASP. UOTSTCYAL NOT DOEJP YEYTP CY, "RCN MUKCJ Z-W-M-S-N!"

The character frequencies for the passage above are shown in figure 5 below:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
25	0	14	10	28	0	3	0	1	23	10	18	25	44	31	24	4	5	22	60	14	7	7	11	13	23

To cryptanalyse the sample text, we start by guessing that: (1) Letter E and T is represented by either "T" or "N" – as they are two most frequently occurring letters and (2) O is either A or H. With the substitutions, we have the text below:

```
EAT E          T     T T    EE         EAT                  E          EAT
THE T          E     E E    TT        THE                   T         THE
NOT NUA JMPETZ UTST ZENNELV EL NOT JEGELV SAAW, UMENELV KAS NOTES

A   ET     A               E     T        T     EAT          ET        EAT          EA
H   TE     H               T     E        E     THE          TE        THE          TH
OAZNTZZ, UOA UMZ ZJEVONJX PTJMXTP. NOT PMCVONTS AK NOT KMWEJX UMZ UENO

EAT        EAT  EAT     EA      AT          TT EAT       E                  T
THE        THE THE     TH      HE          EE THE       T                  E
NOTW, AL NOT NOTASX NOMN ZOT UACJP QTTY NOT GEZENASZ ADDCYETP PCSELV

EAT       E. EAT              T            T                 T         E    EA
THE       T. THE              E            E                 E         T    TH
NOT UMEN. NOT DOEJP UMZ YTSOMYZ ZEI XTMSZ AJP, ZLCR LAZTP, RCDQ NAANOTP MLP

T    T E      T       AT    E     T        TT      T        EAT E          T   TT T
E    E T      E       HE    T     E        EE      E        THE T          E   EE E
RTZYTDNMDJTP. ZOT WMELNMELTP    M   PTTY ZEJTLDT MLP NOT NUA JMPETZ YTTSTP

E          E AT              T     EAT       EET T   E    EAT    EAT
T          T HE              E     THE       TTE E   T   THE    THE
PACRNKCJJX MN OTS. KELMJJX, ALT AK NOTW WCNNTSTP NA NOT ANOTS,

"  E    T      -T-E-E-       T          T         T        EAT   T          AT T      EAT
"  T    E      -E-T-T-       E          E         E        THE   E          HE E      THE
"LAN GTSX Y-S-T-N-N-X, E KTMS," DMSTKCJJX ZYTJJELV NOT QTX UASP. UOTSTCYAL NOT

A         T          E                  -E!"
H         E          T                  -T!"
DOEJP YEYTP CY, "RCN MUKCJ Z-W-M-S-N!"
```

"THE" appears more in English than "EAT" – only a guess. Now: (1) Line 5, only A or I stands alone in English and A appears more than I. So "M" is A, (2) Line 6, two-word that starts E "EX/EN" or starts with T is "TO". TO appears more, and (3) Line 6, word OTHE_ is missing R – so "S" is letter R. Thus, having:

```
THE T   O    A     E ERE    TT        THE           ROO         A   T    R THE R
NOT NUA JMPETZ U TST ZENNELV EL NOT JEGELV SAAW, UMENELV KAS   NOTES

HO   TE         HO    A     T     E  A E. THE    A    TER     THE     A     A       TH
OAZNTZZ, UOA UMZ ZJEVONJX PTJMXTP. NOT PMCVONTS AK NOT KMWEJX UMZ UENO
```

```
THE      O THE THE R     THAT        HE              EE   THE           T   R           E          R
NOTW, AL NOT NOTASX   NOMN    ZOT    UACJP QTTY    NOT    GEZENASZ ADDCYETP PCSELV

THE        A T. THE                  A        ERHA                  EAR E           T   TH      A
NOT    UMEN. NOT DOEJP UMZ YTSOMYZ ZEI XTMSZ AJP, ZLCR LAZTP, RCDQ NAANOTP MLP

E      E   TA      E   HE   A TA     E     A     EE        E          A   THE T       A   E     EERE
RTZYTDNMDJTP. ZOT WMELNMELTP     M    PTTY ZEJTLDT MLP    NOT NUA JMPETZ YTTSTP

T          AT H         A          E     THE         TTERE     TO THE    OTHER,
PACRNKCJJX MN OTS. KELMJJX, ALT AK NOTW WCNNTSTP NA    NOT    ANOTS,

"   T   E     -R-E-T-T-         EAR       ARE           E         THE     E        R.   HERE        THE
"LAN GTSX Y-S-T-N-N-X, E KTMS," DMSTKCJJX ZYTJJELV NOT    QTX UASP. UOTSTCYAL NOT

H          E           T   A              -A-R-T!"
DOEJP YEYTP CY, "RCN    MUKCJ Z-W-M-S-N!"
```

Also: (1) Line 1, "_ERE" is missing W. Replace "U" with W, (2) Line 1, "ROO_" is missing M, so replace "W" with M, and (3) Line 3, a two-word starting with O are OF, ON. "L" is either F or N. Replace L as N on line 4 in the triple word "AN_" to give AND. Thus, "L" is N and "P" is letter D.

```
THE TWO   AD   E     WERE    TT N    N    THE        N     ROOM, WA    T N    OR    THE    R
NOT NUA JMPETZ    UTST ZENNELV EL    NOT JEGELV    SAAW, UMENELV KAS     NOTES

HO TE     , WHO WA          HT       E A    ED. THE DA       HTER O THE       AM        WA    W TH
OAZNTZZ, UOA    UMZ ZJEVONJX PTJMXTP.    NOT PMCVONTS AK NOT    KMWEJX UMZ    UENO

THEM, ON    THE THEOR    THAT    HE    WO    D    EE THE          TOR     O        ED    D R N
NOTW, AL    NOT NOTASX NOMN ZOT    UACJP QTTY NOT GEZENASZ ADDCYETP    PCSELV

THE    WA T. THE          D WA       E    A            EAR    O D N       O    ED,          T    THED    AND
NOT UMEN. NOT DOEJP    UMZ YTSOMYZ ZEI XTMSZ AJP, ZLCR LAZTP, RCDQ NAANOTP    MLP

E    E TA      ED    HE    MA    NTA    NED    A    DEE        EN     AND    THE    TWO     A       E EERED
RTZYTDNMDJTP.    ZOT    WMELNMELTP     M    PTTY ZEJTLDT MLP     NOT    NUA    JMPETZ YTTSTP

T              AT    HER         NA          NE O     THEM    M     TTERED    TO    THE    OTHER,
PACRNKCJJX MN    OTS. KELMJJX, ALT AK NOTW WCNNTSTP    NA    NOT    ANOTS,

"N    T    E     -R-E-T-T-         EAR,"    A    E           E        THE       E     WORD. WHERE    ON THE
"LAN GTSX Y-S-T-N-N-X, E KTMS," DMSTKCJJX ZYTJJELV NOT    QTX    UASP.    UOTSTCYAL NOT

H          E           T   A              -M-A-R-T!"
DOEJP YEYTP CY, "RCN    MUKCJ    Z-W-M-S-N!"
```

Again we can see that in: (1) Line 2, the last two words (triple and quad) (UMZ/UENO) are WA_ and W_TH. Replace "Z" with S and "E" with I. (2) Line 5, replace "Y" with P and (3) Line 7, replace "A" with O. Thus:

```
THE TWO    ADIES    WERE    SITTIN IN    THE     I IN      ROOM, WAITIN    OR      THEIR
NOT NUA JMPETZ    UTST ZENNELV EL    NOT JEGELV    SAAW, UMENELV KAS     NOTES

HOSTESS    WHO WAS S I    HT      DE A ED.    THE DA      HTER    O    THE       AMI        WAS WITH
OAZNTZZ, UOA    UMZ ZJEVONJX PTJMXTP.    NOT PMCVONTS    AK    NOT    KMWEJX UMZ    UENO

THEM, ON THE THEOR    THAT SHE    WO    D    EEP THE     ISITORS    O       PIED D    RIN
NOTW, AL NOT NOTASX NOMN ZOT    UACJP QTTY    NOT GEZENASZ ADDCYETP    PCSELV

THE WAIT.    THE       I D    WAS    PERHAPS    I     EARS    O D, SN     NOSED,          TOOTHED    AND
NOT UMEN. NOT DOEJP    UMZ    YTSOMYZ ZEI XTMSZ    AJP,    ZLCR LAZTP,    RCDQ NAANOTP    MLP

ESPE TA      ED. SHE MAI NTAINED      A    DEEP SI    EN E AND THE    TWO     ADIES PEERED
RTZYTDNMDJTP. ZOT WMELNMELTP     M    PTTY ZEJTLDT MLP    NOT    NUA    JMPETZ YTTSTP

O     T          AT    HER       INA      ONE O    THEM M     TTERED TO    THE    OTHER,
PACRNKCJJX MN    OTS. KELMJJX, ALT    AK NOTW WCNNTSTP    NA    NOT    ANOTS,
"NOT    ER     P-R-E-T-T- I     EAR,"       ARE         PE      IN THE       E    WORD. WHERE PON    THE
"LAN GTSX Y-S-T-N-N-X, E KTMS," DMSTKCJJX ZYTJJELV NOT    QTX    UASP.    UOTSTCYAL    NOT

HI D PIPED    P       T    A           S-M-A-R-T!"
DOEJP YEYTP CY, "RCN    MUKCJ    Z-W-M-S-N!"
```

We see also in: (1) Line 1, replace "V" with G and "J" with L, (2) Line 2, replace "X" with Y, "C" letter U and "K" with F, (3) Line 3, replace "G" with V and "Q" with K, and (4) Line 4, replace "I" with X and "D" with C to give us the test be-

low.

THE TWO LADIES WERE SITTING IN THE LIVING ROOM, WAITING FOR THEIR
NOT NUA JMPETZ UTST ZENNELV EL NOT JEGELV SAAW, UMENELV KAS NOTES

HOSTESS WHO WAS SLIGHTLY DELAYED. THE DAUGHTER OF THE FAMILY WAS WITH
OAZNTZZ, UOA UMZ ZJEVONJX PTJMXTP. NOT PMCVONTS AK NOT KMWEJX UMZ UENO

THEM, ON THE THEORY THAT SHE WOULD KEEP THE VISITORS OCCUPIED DURING
NOTW, AL NOT NOTASX NOMN ZOT UACJP QTTY NOT GEZENASZ ADDCYETP PCSELV

THE WAIT. THE CHILD WAS PERHAPS SIX YEARS OLD, SNU NOSED, UCK TOOTHED AND
NOT UMEN. NOT DOEJP UMZ YTSOMYZ ZEI XTMSZ AJP, ZLCR LAZTP, RCDQ NAANOTP MLP

ESPECTACLED. SHE MAINTAINED A DEEP SILENCE AND THE TWO LADIES PEERED
RTZYTDNMDJTP. ZOT WMELNMELTP M PTTY ZEJTLDT MLP NOT NUA JMPETZ YTTSTP

DOU TFULLY AT HER. FINALLY, ONE OF THEM MUTTERED TO THE OTHER,
PACRNKCJJX MN OTS. KELMJJX, ALT AK NOTW WCNNTSTP NA NOT ANOTS,

"NOT VERY P-R-E-T-T-Y, I FEAR," CAREFULLY SPELLING THE KEY WORD. WHEREUPON THE
"LAN GTSX Y-S-T-N-N-X, E KTMS," DMSTKCJJX ZYTJJELV NOT QTX UASP. UOTSTCYAL NOT

CHILD PIPED UP, " UT AWFUL S-M-A-R-T!"
DOEJP YEYTP CY, "RCN MUKCJ Z-W-M-S-N!"

Having come thus far, we make one last substitution by: replacing "R" with letter B.

THE TWO LADIES WERE SITTING IN THE LIVING ROOM, WAITING FOR THEIR
NOT NUA JMPETZ UTST ZENNELV EL NOT JEGELV SAAW, UMENELV KAS NOTES

HOSTESS WHO WAS SLIGHTLY DELAYED. THE DAUGHTER OF THE FAMILY WAS WITH
OAZNTZZ, UOA UMZ ZJEVONJX PTJMXTP. NOT PMCVONTS AK NOT KMWEJX UMZ UENO

THEM, ON THE THEORY THAT SHE WOULD KEEP THE VISITORS OCCUPIED DURING
NOTW, AL NOT NOTASX NOMN ZOT UACJP QTTY NOT GEZENASZ ADDCYETP PCSELV

THE WAIT. THE CHILD WAS PERHAPS SIX YEARS OLD, SNUB NOSED, BUCK TOOTHED AND
NOT UMEN. NOT DOEJP UMZ YTSOMYZ ZEI XTMSZ AJP, ZLCR LAZTP, RCDQ NAANOTP MLP

BESPECTACLED. SHE MAINTAINED A DEEP SILENCE AND THE TWO LADIES PEERED
RTZYTDNMDJTP. ZOT WMELNMELTP M PTTY ZEJTLDT MLP NOT NUA JMPETZ YTTSTP

DOUBTFULLY AT HER. FINALLY, ONE OF THEM MUTTERED TO THE OTHER,
PACRNKCJJX MN OTS. KELMJJX, ALT AK NOTW WCNNTSTP NA NOT ANOTS,

"NOT VERY P-R-E-T-T-Y, I FEAR," CAREFULLY SPELLING THE KEY WORD. WHEREUPON THE
"LAN GTSX Y-S-T-N-N-X, E KTMS," DMSTKCJJX ZYTJJELV NOT QTX UASP. UOTSTCYAL NOT

CHILD PIPED UP, "BUT AWFUL S-M-A-R-T!"
DOEJP YEYTP CY, "RCN MUKCJ Z-W-M-S-N!"

From the above sample data, the key E is as seen in figure 6, though letters Z, J and Q are used as thus:

```
    A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
E = ---------------------------------------------------
    M R D P T K V O E F Q J W L A Y B S Z N C G U I X H
```

***Fig. 6**: Key E for example above*

This cipher is simple. [3] notes to secure such ciphers are:

a. Punctuations and separators can be encoded with alternative symbols.

b. Permutation simply breaks up data into equal letter chunk(s), adding junk letters where necessary, to extend and make equal the last chunk – so that each chunks encodes itself. For example, 21-letter chunk "THISCIPHERISNOTSECURE" is broken into 25-letter, extended with AAAA in 5X5 matrix. Thus, a user reads text by column instead of row as: TIISEHPSEAIHNCASEOUACRTRA.

***Table 1:** 5 x 5 matrix of letters for permutation*

T	H	I	S	C
I	P	H	E	R
I	S	N	O	T
S	E	C	U	R
E	A	A	A	A

a. Using 127 different symbols for "E", 91 for "T" etc. A cryptanalyst notices equally common symbols – making it subject to frequency attack if he/she has access to lots of text and letter pairs.

b. A user can also have codes for letter pairs and com-

mon-words that help make the task still more difficult. Its demerit is that with more combinations, the cipher becomes more difficult to decode. Addition of "nulls" to the cipher (garbage encoding) that must be ignored and tossed during the decoding can help balance frequencies as well as the use of special items that mean things like "ignore the next item", or "delete the previous item". In spite of all these suggestions, if a cryptanalyst has sufficient text, it is only a matter of time before someone could break it.

1.3. The Vigen`ere Cipher

This is a mixture of 26 different alphabets. Thus, this cipher technique has ciphers called "A", "B", "C" etc, which are read off for encoding in rows and column format. It can be used in two ways: either as a set using a particular keyword (to encode "ARNOLD" using cipher "G", we look up each of letter under the row "G" to derive the cipher "GXTURJ"), or we use individual ciphers for each letter in the plaintext through a keyword as in table 2 below [3]:

Table 2: *The Vigenere Cipher*

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Thus, if we wish to encode "SEND THE ONE MILLION THROUGH UNION BANK" with keyword "PASSWORD", it is as below. But first, note that the keyword "password" is not as long as the phrase – thus, the keyword "password" is repeated so that it becomes as long as the phrase. To encode, "P" cipher on "S" of "SEND", "A" cipher on "E", the "S" code on the "N", and so on to yield the figure 9 below – where the first column represents the text to be encoded, the second column is the keyword password repeated; while the third column is the ciphertext as given in table 3.

Table 3: *Encoded Plaintext using the Vigenere cipher to yield the Ciphertext*

S	E	N	D	T	H	E	O	N	E	M	I	L	L	I	O	N	T	H	R	O	U	G	H	U	N	I	O	N	B	A	N	K
P	A	S	S	W	O	R	D	P	A	S	S	W	O	R	D	P	A	S	S	W	O	R	D	P	A	S	S	W	O	R	D	P
H	E	F	V	P	V	V	R	C	E	E	A	H	Z	Z	R	C	T	Z	J	K	I	X	K	J	N	A	G	J	P	R	Q	Z

Vigenere cipher is more difficult to cryptanalyse and the longer the keyword, the more difficult to crack. If its keyword were too long and random, it becomes impossible to decode, as any decoding is as likely as any others. To use such cipher, keyword is usually an English word/phrase, not hard to remember. A long keyword of random letters is unbreakable – because any encoding can represent any text with some keyword. Thus, the word "WEASEL", with an appropriate "keyword" – can represent any 6 characters word. Clearly, if the key is allowed to be arbitrarily long and composed of arbitrary letters, then anything can stand for anything, and thus, code is quite secure.

2. Converting Text to Numbers

Most mathematical encryption methods are integer transformations – no matter how they are achieved. Some, have slight merits over others, and the most commonly used is ASCII (assigns a number to each character with 128 different characters, including upper/lower case alphabets, digits, punctuation amongst other characters as octal implementation). Thus, H in row 11 and column 0 has octal value 110. To convert to decimal, 110 (octal) = $1 \cdot 8^2 + 1 \cdot 8^1 + 0 \cdot 8^0 = 64 + 8 + 0 = 72$ (decimal) [3].

***Table 4**: ASCII Codes*

	0	1	2	3	4	5	6	7
00	^@	^A	^B	^C	^D	^E	^F	^G
01	^H	^I	^J	^K	^L	^M	^N	^O
02	^P	^Q	^R	^S	^T	^U	^V	^W
03	^X	^Y	^Z	^[	^\	^]	^^	^_
04		!	“	#	$	%	&	‘
05	(	)	*	+	,	-	.	/
06	0	1	2	3	4	5	6	7
07	8	9	:	;	<	=	>	?
10	@	A	B	C	D	E	F	G
11	H	I	J	K	L	M	N	O
12	P	Q	R	S	T	U	V	W
13	X	Y	Z	[	\	]	^	_
14	‘	a	b	c	D	e	F	g
15	h	i	j	K	l	m	N	o
16	p	q	r	s	t	u	V	W
17	x	Y	Z	{	|	}	~	DEL

ASCII encodes 7-bits data, whereas computers manipulate data as 8-bit. When ASCII is used, a character is put in one byte effectively but losses 1-bit; and with concatenation, the 7-bit or 8-bit is put side-by-side to represent group of letters – so that if a user wishes to encode two ASCII characters, he simply place their binary values next to each other to get a 16-bit number. Users are at home with base 10 (decimal) giving the encoding of figure 10. Note: XX entry is not used, while “SP” is Space character. U is 31; 7 is 97, etc. To encode the word: “CAR3”, it is represented by the 8-digit number 13-11-28-93 (i.e. 13112893).

***Table 5:** Decimal Alphanumeric Encoding*

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
1	SP	A	B	C	D	E	F	G	H	I
2	J	K	L	M	N	O	P	Q	R	S
3	T	U	V	W	X	Y	Z	a	B	C
4	D	e	f	g	h	i	j	k	L	M
5	N	o	p	q	r	s	t	u	V	W
6	X	y	z	.	,	:	;	‘	“	‘
7	!	@	#	$	%	^	&	*	-	+
8	(	)	[	]	{	}	?	/	<	>
9	0	1	2	3	4	5	6	7	8	9

2.1. Quasi/Psuedo-Random Numbers

Generating a very long key to use in a Vigenere has its problem, in that the key has to be transmitted in a secure way to the decoding user. If key is random, the more secure it is. A truly, random key can only be generated in radioactivity. Other methods are via quasi or Psuedo random mode (Knuth, 2000). This is achieved as thus: if p is a prime number, n is a number in range $0 < n < p$. Then, the sequence of numbers $nK \pmod p$ cycles all numbers between 1 and $p-1$, in a somewhat random order as K goes through 1, 2, .., $p - 1$. For example, if p = 17 and n = 3:

$3 \cdot 1 \pmod{17} = 3 \bmod 17 = 3$
$3 \cdot 2 \pmod{17} = 6 \bmod 17 = 6$
$3 \cdot 3 \pmod{17} = 9 \bmod 17 = 9$
$3 \cdot 4 \pmod{17} = 12 \bmod 17 = 12$
$3 \cdot 5 \pmod{17} = 15 \bmod 17 = 15$
$3 \cdot 6 \pmod{17} = 18 \bmod 17 = 1$
$3 \cdot 7 \pmod{17} = 21 \bmod 17 = 4$
$3 \cdot 8 \pmod{17} = 24 \bmod 17 = 7$
$3 \cdot 9 \pmod{17} = 27 \bmod 17 = 10$
$3 \cdot 10 \pmod{17} = 30 \bmod 17 = 13$
$3 \cdot 11 \pmod{17} = 33 \bmod 17 = 16$
$3 \cdot 12 \pmod{17} = 36 \bmod 17 = 2$
$3 \cdot 13 \pmod{17} = 39 \bmod 17 = 5$
$3 \cdot 14 \pmod{17} = 42 \bmod 17 = 8$
$3 \cdot 15 \pmod{17} = 45 \bmod 17 = 11$
$3 \cdot 16 \pmod{17} = 48 \bmod 17 = 14$
$3 \cdot 17 \pmod{17} = 51 \bmod 17 = 0$

The numbers cycles: 0, 3, 6, 9, 12, 15, 1, 4, 7, 10, 13, 16, 2, 5, 8, 11 and 14. 0 is not a number between 1 and p-1. This sequence appears to be random and the larger the prime, the longer the sequence. Using this to encrypt data: “Password: Ojugo” plus the space will have the numeric codes: 26, 37, 55, 55, 59, 51, 54, 40, 65, 10, 25, 46, 57, 43, 51 (as from figure 11). We use a combination of this method, to generate a sequence of pseudo-random numbers to use as the key. Let p = 16139 and n = 4352. As k goes 1 to 15, $4352*k \pmod{16139}$ becomes the 15-numbers:

$4352 \cdot 1 \pmod{16139} = 4352 \bmod 16139 = 4352$
$4352 \cdot 2 \pmod{16139} = 8704 \bmod 16139 = 8704$
$4352 \cdot 3 \pmod{16139} = 13056 \bmod 16139 = 13056$
$4352 \cdot 4 \pmod{16139} = 17408\ 16139 = 1269$
$4352 \cdot 5 \pmod{16139} = 21706 \bmod 16139 = 5621$
$4352 \cdot 6 \pmod{16139} = 26112 \bmod 16139 = 9973$
$4352 \cdot 7 \pmod{16139} = 30464 \bmod 16139 = 14325$
$4352 \cdot 8 \pmod{16139} = 34816 \bmod 16139 = 2538$
$4352 \cdot 9 \pmod{16139} = 39168 \bmod 16139 = 6890$
$4352 \cdot 10 \pmod{16139} = 43520 \bmod 16139 = 11242$
$4352 \cdot 11 \pmod{16139} = 47872 \bmod 16139 = 15594$
$4352 \cdot 12 \pmod{16139} = 52224 \bmod 16139 = 3807$
$4352 \cdot 13 \pmod{16139} = 56576 \bmod 16139 = 8159$
$4352 \cdot 14 \pmod{16139} = 60928 \bmod 16139 = 12511$
$4352 \cdot 15 \pmod{16139} = 65280 \bmod 16139 = 724$

Thus: 4352, 8704, 13056, 1269, 5621, 9973, 14325, 2538, 6890, 11242, 15594, 3807, 8159, 12511, 724.

To encode, we add these to the numbers in our sequence and take its result of modulo 100 as thus:

$26 + 4352 \pmod{100} = 4378 \bmod 100 = 78$
$37 + 4352 \pmod{100} = 4387 \bmod 100 = 87$
$55 + 4352 \pmod{100} = 4407 \bmod 100 = 7$
$55 + 4352 \pmod{100} = 4407 \bmod 100 = 7$
$59 + 4352 \pmod{100} = 4411 \bmod 100 = 11$
$51 + 4352 \pmod{100} = 4403 \bmod 100 = 3$
$54 + 4352 \pmod{100} = 4406 \bmod 100 = 6$
$40 + 4352 \pmod{100} = 4392 \bmod 100 = 92$
$65 + 4352 \pmod{100} = 4412 \bmod 100 = 12$
$10 + 4352 \pmod{100} = 4362 \bmod 100 = 62$
$25 + 4352 \pmod{100} = 4377 \bmod 100 = 77$
$46 + 4352 \pmod{100} = 4398 \bmod 100 = 98$
$57 + 4352 \pmod{100} = 4509 \bmod 100 = 9$
$43 + 4352 \pmod{100} = 4395 \bmod 100 = 95$
$51 + 4352 \pmod{100} = 4403 \bmod 100 = 3$

The encoded sequence becomes 78, 87, 7, 7, 11, 3, 6, 92, 12, 62, 77, 98, 9, 95 and 3.

The user only decodes data if he knows the value of p and n, and thus – generates same exact sequence of keys to undo

the encryption. To generate first number: subtract 78 from 4352 (= -4274), take modulo 100 (= -72). Since it is negative, we subtract from 100 to get 26 etc. Note, the only data passed to the recipient as key is the pair of p and n. No need to transmit long sequence of keys. The generator is modified by choosing a large prime p, two integers (m, n) and seed "starting number" X_0 – so that $Xi = (m*X_{i-1} + n)(\text{mod } p)$, if i > 0. So, if p = 161, m = 91, n = 541, and $X_0 = 0$, we generate the sequence (no matter how large p, m and n – the sequence cycles p thus) as:

$X_0 = 11$ and $X_1 = (91 \cdot 11 + 49)(\text{mod } 161) = 1050 \text{ mod } 161 = 84$

$X_2 = (91 \cdot 84 + 49)(\text{mod } 161) = 7693 \text{ mod } 161 = 77$ $X_3 = (91 \cdot 77 + 49)(\text{mod } 161) = 7056 \text{ mod } 161 = 133$

To decipher (p = 16139, m = 91, n = 541, $X_0 = 0$) the data 23, 52, 85, 91, 15, 6, 53, 61, 30, 72, 23:

With $X_0 = 0$. Thus, our first number is 23 = M.

$X_1 = (91 \cdot 0 + 541)(\text{mod } 16139) = 541 \text{ mod } 16139 = 541$

(52 – 541) mod 100 = -89 and 100 – 89 = 11 = A

$X_2 = (91 \cdot 541 + 541)(\text{mod } 16139) = 49772 \text{ mod } 16139 = 1355$

85 – 1355 mod 100 = -70 but 100 – 70 = 30 = T

$X_3 = (91 \cdot 1355 + 541)(\text{mod } 16139) = 10873 = 1355$

91 – 10873 mod 100 = -82 but 100 – 82 = 18 = H

$X_4 = (91 \cdot 10873 + 541)(\text{mod } 16139) = 5505$

15 – 5505 mod 100 = -90 (100 – 90) = 10 = SPACE

$X_5 = (91 \cdot 5505 + 541)(\text{mod } 16139) = 1187$

6 – 1187 mod 100 = -81 but 100 – 81 = 19 = I

$X_6 = (91 \cdot 1187 + 541)(\text{mod } 16139) = 11724$

53 – 11724 mod 100 = -71 but 100 – 71 = 29 = S

$X_7 = (91 \cdot 11724 + 541)(\text{mod } 16139) = 2251$

61 – 2251 mod 100 = -90 (100 – 90) = 10 = SPACE

$X_8 = (91 \cdot 2251 + 541)(\text{mod } 16139) = 11714$

30 – 11714 mod 100 = -84 but 100 – 84 = 16 = F

$X_9 = (91 \cdot 11714 + 541)(\text{mod } 16139) = 1341$

72 – 1341 mod 100 = -69 but 100 – 69 = 31 = U

$X_{10} = (91 \cdot 1341 + 541)(\text{mod } 16139) = 9599$

23 – 9599 mod 100 = -76 but 100 – 76 = 24 = N

3. Public-Key Cryptography

A major problem in cryptography is keys distribution as same keys cannot be used over and over – else, it becomes possible for cryptanalysts to crack the cipher. It is painstaking to transfer the keys – as incidents can occur, if the keys are mailed, cryptographically sent or hand-delivered. Examples include RSA, AES, Triple DES amongst others, are based on *trap-door* scheme that allows each cipher to have set of encoding and different decoding keys – so that if user A knows the decoding key, it is easy to make the encoding key. But user B is unable to make the decoding key if he/she only has the encoding key. To communicate, user A uses his trap-door to generate a decoding D_a and corresponding encoding key E_a. User B does same, but tells user A the encoding key E_b (but not D_b). User does same by telling B encoding key E_a (but not D_a). Thus, user A can send messages by encoding using E_b (only user B can decode) and vice-versa – because user B is the only one with access to decoding key D_b just as A is also the only user with access to D_a. To change to a new key, users make up new pairs and exchange encoding keys. If the encoding keys are stolen, the eavesdropper can only encode but not decode. Thus, encoding keys are public keys – since they are published, while the decoding keys are made private or secret [4].

3.1. RSA Scheme

Commonly used trap-door is RSA (Rivest, Shamir, and Adleman), based on number factoring. Number multiplication with computers is quite simple but it can be difficult to factor numbers. A computer can factor numbers – knowing the possible combinations by checking the order of the size of the square root of number to be factored. For example, it takes seconds for the computer to try out 38000 possibilities, but the larger the number to be factored the longer it takes to factor them. It is also not hard to check if a number is prime or to see if it cannot be factored. If not prime, it is difficult to factor. Thus, the RSA scheme finds two huge prime numbers (m and n) with up to 200 digits each, which the user keeps s secret (private key) – and multiplies them to get N (public key). It is easy for a cryptanalyst to get N by multiplying m and n; but impossible to find m and n [4, 8]. RSA works as thus (though the prime numbers are very large):

User A makes a public key, which B uses to send A messages. User A sends B just a number, which is assumed that A and B have agreed on a method to encode text as numbers using these steps below:

1. User A selects two primes p and q (say 23 and 41). Note: User A will use *much* larger in real life scenario and gets N = pq ((23)(41) = 943), known as public key that B (and rest of the world, if he wishes) knows.

He then also chooses another number relatively prime to $(p-1)(q-1)$ – in this case (22)(40) = 880. Thus, e = 7 and also part of the public key, so B also is told the value of e.

2. B has enough data to encode data to User A. If the data is the number W = 33, User B calculates the value of $C = W^e (\text{mod } N) = 33^7(\text{mod } 943)$. $W^e = 33^7 = 42618442977$ and 42618442977 (mod 943) = 244. The number 244 is the encoding that User B sends to User A.

3. User A then decodes 244 by finding a number d in that $ed = 1(\text{mod } (p-1)(q-1))$.

7d = 1(mod 880) and d = 503, since in reverse – we have 7*503 = 3521 = 4(880)+1 = 1(mod 880).

4. User A finds the decoding by calculating $C^d (\text{mod } N) = 244^{503} (\text{mod } 943)$ – just the binary expansion

503 = 256 + 128 + 64 + 32 + 16 + 4 + 2 + 1.

$244^{503} = 244^{256+128+64+32+16+4+2+1} \rightarrow 244^{256}. 244^{128} \cdots 244^{1}$

We are only interested in the result (mod 943), calculate all partial results via repeated squaring of 244 and get all exponents in powers of 2 as:

244^2 (mod 943) →244*244 = 59536 (mod 943) = 127 – with the workings below:

$244^1(\text{mod } 943) = 244$

$244^2(\text{mod } 943) = 127$

$244^4(\text{mod } 943) = 98$

$244^{16}(\text{mod } 943) = 100$

$244^{32}(\text{mod } 943) = 570$
$244^{64}(\text{mod } 943) = 508$
$244^{128}(\text{mod } 943) = 625$
$244^{256}(\text{mod } 943) = 223$
This becomes:
$244^{503} \text{ (mod } 943)$
$= 223 \cdot 625 \cdot 508 \cdot 570 \cdot 100 \cdot 98 \cdot 127 \cdot 224 \text{ (mod } 943)$
$= 33.$
User A decodes B's data to obtain the original data N = 35.

4. Discussions

Studies have shown that the Internet as a medium of data transfer is insecure and unsafe. Being aware that data sent over such public media lacks integrity – this has led to the field of cryptography. Our study thus, defines cryptography, its methods (symmetric and public key) and notes problem with each scheme.

Alternatively, public-key ciphers are safer but their major problem is that with the keys being public, a user can forge a message to authentic users pretending to be one of them. Thus, ***digital*** signature and certificate makes it possible to send messages so that a user is certain it is from a friend. This can be accomplished as thus: User A takes his name, pretends it is an encoded message, which can only be decoded using D_a (accessible only to User A) – and includes it in the real message encoded using E_b, which only user B can decode. User B receives it, decodes using D_b but discovers additional junk data (gotten by User A by decoding his name). User B simply encodes junk using A's public key E_a and makes certain that it is user A's name. User A alone, can make the text to encode to his name, such that when he receives the data – he is sure it is User B.

5. Summary / Conclusion

The proliferation of communication systems brought with it, demands from the private sector, for means of protecting digital data as well as data security services. Beginning with the work of Feistel at IBM in early 1970s, culminated in 1977 when U.S Federal information processing standard adopted Data Encryption Standard (DES) for encrypting unclassified data – making DES the most well-known cryptographic method and standard in history. Diffie and Hellman's work "New Directions in cryptography" saw the birth of public-key cryptography that today provides data security based on the intractability of the discrete logarithm problem. The search for public-key schemes and its improvements, continue with proofs of security at rapid pace. Security products, schemes and algorithms are developed to address the security needs of an information society.

6. Recommendation

Because keys in a public key scheme are made public, a user can forge message to users, pretending to be another users, which often can mislead authentic users. Thus, digital signatures/certificates are used to make it possible to send messages so that a user is certain that the sent message is from a friend (and not foe). An easy way to do this is to take user A's name and pretend it is an encoded message, which will be decoded using D_a. User A is the only one with D_a, so he includes this in the real message and encodes using E_b, which only user B can decode. When B receives it, he decodes using D_b but discovers additional junk characters (derived when user A decodes his name). User B simply encodes the junk using user A's public key E_a and makes certain that it is user A's name. Since user A is the only one who can make meaning of the cipher, he knows the message is from user B. Additional information can be encoded for certification to assure privacy.

References

[1] Adewumi, S.E and Garba, E.J., Data security: cryptosystems algorithm using data compression and systems of non-linear equations, 2002, Nigerian Computer Society, Vol. 13

[2] Zeng, K., Psuedorandom bit generators in stream cipher cryptography, 1991, IEEE J. Computers, 24(2), pp 45 – 54.

[3] Davis, K.L., The art of ciphers, 2000, J. Comp and Info. Syst., ISSN: 2032-3765, pp 32

[4] Knuth, D., The art of computer programming — seminumerical algorithms, 2000, New Jersey, Prentice Hall publications

[5] Mendez, A., Van Oorschot, P and Vanstone, S Handbook of applied cryptography, 1997, New Jersey, CRC Press.

[6] Stallings, W and Van Slyke, R., Introduction to business data communication, 2008, McGraw hill publications.

[7] Tanenbaum, A.S., Computer networks, 1996 New Jersey, Prentice Hall publications.

[8] Aghware, F.O., A modified RSA encryption as implemented in the Nigerian banking software, 2005, Unpublished Masters thesis, Nnamdi Azi kiwe University: Awka-Nigeria