**30TH INAUGURAL LECTURE**

# MATHEMATICS FOR SECURITY AND WORLD PEACE

*Michael, Olusanya Ajetunmobi*
**B.Sc (Hons.), M.Sc. (Ife), Ph.D (Ib).**

**PROFESSOR AND HEAD**
Department of Methematics
**Faculty of Science**
**Lagos State University**
**Nigeria 2006.**

**The Vice - Chancellor,**

**Deputy Vice - Chancellor,**

**The Registrar,**

**Bursar, Librarian,**

**Provost, College of Medicine**

**Dean of Science,**

**Deans of other Faculties,**

**Professors,**

**Distinguished Members of the Senate,**

**Academic Staff of LASU,**

**Other Staff of LASU,**

**Ladies and Gentlement of the Press,**

**Distinguished Ladies and Gentlemen.**

## INTRODUCTION

Of recent an Inaugural Lecture has become a form of "Iwuye" Ceremony or as an ordination of a high Priest in the fold of academic professors. This inaugural lecture deviates from these recent traditions. The faculty of science was established in 1984 with two departments: the department of Biological and chemical sciences and the department of physical and mathematical sciences. For 22 yrs, this is the first Inaugural lecture coming from the defunct department of physical and mathematical sciences (P & M) so this inaugural lecture holds it a point of duty to let the society know the nature of the mathematical disciplines and how things are done in mathematics. Using the language of the military, this inaugural lecture is a *"Flag Showing"* lecture and not an Iwuye ceremony.

Mr. Vice – Chancellor, sir, this inaugural lecture will therefore be in three parts. The first part will attempt to give a definition of mathematics as an academic discipline. The second part will focus on the principal research activities of the inaugural lecturer, while the third part will focus on the involvement and the contribution of the inaugural lecturer to the development of the LASU MBA programme and consequently the use of mathematics for the security of the data of these honourable MBA members of our society. This latter part informs the topic of this inaugural lecture; which is Mathematics for Security and World Peace.

## WHAT IS MATHEMATICS:

In 1974, during the mathematics week at the University of Ife Ile-Ife (now Obafemi Awolowo University), Dr. Omololu Olunloyo was invited to give a talk to the mathematics students. During the Question and Answer Session, the first question fired at him by a mathematics student was "What are the usefulness of mathematics?" For some thirty seconds, the lecturer was silent, when he eventually recovered, he replied: What is the usefulness of the Shakespeare plays? The hall was dead quiet, may be disappointed. They had expected an "Ordinary" answer to shed some light on the several mathematics courses taught within the department. I was then a Year 3 mathematics student at the University of Ife.

Today, thirty two years after, I am to give an inaugural lecture as a professor of mathematics. It is therefore natural and ethical that I should give an explanation to the answer offered by Dr. O. Olunloyo.

Many prominent mathematicians and mathematics teachers have given various definitions of mathematics. Among such definitions as presented by Adu [1] are:

B.W. Russell (1901) "Mathematics may be defined as the subject in which we never know what we are talking about, nor whether what we are saying in true."

D. Hilbert (1862 – 1943) "Mathematics is nothing more than a game played according to certain simple rules with meaningless marks on papers"

Salimanu [5] also recorded more definitions, facts and observation about mathematics.

- ***Albert Einstein:*** "It is mathematics that offers the exact natural sciences a certain measure of security, which without mathematics they could not obtain".
- ***Eric Temple Bell:*** "Mathematics has light and wisdom of its own, above any possible application to science, and it will richly reward any intelligent human being to catch a glimpse of what mathematics means to itself"
- ***Dienes (1961):*** "Mathematics is generally about the structure of relationships, while symbolism is merely a way of communicating parts of the structure from one person to another"
- ***Skemp (1971):*** "Mathematics is a system of abstraction, classification and logical reasoning."
- ***Alfred North Whitehead:*** "Mathematics in its widest significance is the development of all types of familiar, necessary deductive reasoning"
- ***Boulding (1956):*** "Mathematics attempts to organize highly general relationship into a coherent system… It studies all thinkable relationships abstracted from any concrete situation or body of empirical knowledge."
- ***Boehm (1958):*** "Pattern is the only relatively stable thing in a changing world…. Mathematics is about patterns, classifications and their study"
- ***Ojerinde (1999):*** "Mathematics is the communication system for those concepts of shapes, size, quantity and orders used to describe diverse phenomena both in physical and economic situations.
- ***Aminu (1985):*** "Mathematics is the language of science, the essential nutrient for thought, logic, reasoning and therefore progress".

- ***Nelist and Nuhea (1986):*** "Mathematics is a set of precise and logical language, which not only leads to interesting activities but can be applied (or interpreted) to

  everyday life used as description or models in science and other areas.

From the above various definitions, it becomes very clear that some see mathematics as a systematic study of certain things – a science, others see it as the study of some basic truths – a philosophy, while some still see it as "light and wisdom of its own" – an art.

A mathematician can then claim to be a scientist, a philosopher or an artist depending on his approach to the study of mathematics. Mr. Vice-Chancellor, sir, I have therefore given an explanation to the answer given by Dr. O. Olunloyo – Mathematics is like the shakespear plays – an art. A course that can be a whole world of invention and discovery [Adu:1]. A subject in which we never know what we are talking about, nor whether what we are saying is true [Adu:1].

A pseudomodel (or generalized model) is any representation of things that looks reasonable or interesting to a mathematician. These reasonable things can be reality or just anything. When they are reality a pseudomodel becomes a model.
Mr. Vice – Chancellor sir, I now make bold to define mathematics.

Mathematics is the construction and the systematic study and method of the determination of the solution to pseudomodels.

This definition asserts the three components of mathematics: Art, Philosophy and Science. The construction of a pseudomodel is an art as well as philosophy while the method of solution is scientific.

Some years back, some of the first generation universities in Nigeria award Bachelor of Arts (B.A) Degree in Mathematics indicating that the major focus in mathematics was Arts while others award Bachelor of Science (B.Sc.) indicating that the major focus in mathematics was a combination of Arts & Sciences.

Today, in Nigeria and in general, in the whole world, advancement is in the direction of Science and Technology and the major tool used for the analysis and management of information is mathematics. This has made most mathematicians, particularly the applied and the applicable mathematicians, to be very close to the scene of activities. It is therefore very logical for most authorities to see and feel only the science component of mathematics. It is

therefore not surprising that every Nigerian University, including LASU awards B.Sc. (Hons.) in mathematics.

This inaugural lecturer has a B.Sc. (Hons) degree in mathematics while he trained and studied under a most distinguished mathematician with B.A. (Hons) degree in mathematics.

## MATHEMATICS COURSES

Mathematics as a course of study can be broadly divided into pure mathematics, applied mathematics and applicable mathematics.

Pure mathematics is the abstract course that has no place for real life situations. The components include Abstract algebra, Analysis and Geometry, Topology and their variances. They form the core of mathematics.

Applied mathematics, although, derives all its machinery from pure mathematics, formulates ideas that explain the observations in the natural world. This is the type of mathematics that is familiar to most physical scientists and mathematical economists.

If mathematics is seen as an exact subject, then reference is being made to pure and applied mathematics.

Applicable mathematics is much recent and it deals with the formulation and solution of everyday problems encountered in the industry and the military. Examples of courses in Applicable mathematics include Operations Research, Numerical methods, and their variances. Applicable mathematics often gives approximate solutions to problems. Most other disciplines call applicable mathematics a variety of names such as Quantitative techniques, Quantitative analysis, Mathematics for managers etc.

Most researchers and students in social sciences, and Management sciences are familiar with applicable mathematics, and some of the problems (models) encountered are Scarce resource allocation (including assignment and transportation problems), Queuing, Inventory management or stocks control, financial mathematics (including simple interest, compound interest, annuity, present value etc.) and forecasting.

## ALGEBRAIC TOPOLOGY

A topological space is a set in which we have enough of an idea of when points are near each other so that we can talk about continuous transformation.

Topology is the study of the properties of such spaces which are invariant under the group of homeomorphisms. Such properties include compactness and connectedness.

Two topological spaces are homeomorphic if one space can be stretched, twisted and otherwise deformed without being torn or cut, to look just like the other. Thus the following topological spaces are homeomorphic:

- a big sphere and a small sphere
- the boundary of a circle and the boundary of a square.

The main problem of topology is to find useful, necessary and sufficient conditions, other than just the definition, for two spaces to be homeomorphic. Sufficient conditions are hard to come by in general. Necessary conditions are a dime a dozen, but some are very important and useful. A topological space has associated with it various group structures, namely homology groups, cohomology groups homotopy groups and cohomotopy groups. If two spaces are homeomorphic then the associated group structures are isomorphic.

Thus a necessary condition for topological spaces to be homeomorphic is that their associated group structures must be isomorphic. This statement is equivalent to the statement: If the associated group structures are not isomorphic then the topological spaces are not homeomorphic.

The main problem of topology is then reduced to the computations of these group structures. This branch of pure mathematics is called ALGEBRAIC TOPOLOGY.

One constraint often experienced is that during conversion from the topological space to the associated algebraic objects, some of the topological structures may be lost. We therefore seek for new algebraic objects, which hopefully can be analysed to obtain more of the topological structures.

***One of the new "rich" groups is the cohomology group which has an additional multiplicative structure and hence defining a ring. The topological K-ring of Grothendieck, Atiyah and Hirzebruch is a generalized cohomology group.***

Mr. Vice-Chancellor, sir, I am an ALGEBRAIC TOPOLOGIST working in topological K-theory. The specific topological **spaces**, which I study are called Flag manifolds and Flag Bundles which are generalized form of the more familiar projective and Grassmann manifolds and bundles.

The study of **Flag manifolds and Flag bundles** is enriched by the fact that they are examples of several general spaces, which form major areas of

research in Algebraic Topology. In this connection, flag manifolds and flag bundles are examples of general spaces such as Finite CW – Cell complexes, homogeneous spaces and fibre bundles.

**Let** $(n_1, n_2, \ldots, n_r)$

**be a partition of an integer n such that**

$$n = \sum_{i=1}^{r} n_i$$

**Then an incomplete flag called**

**the generalized complex flag manifold,**

$F(n_1,n_2,\ldots, n_r;n)$ **is identified with**

**the homogeneous space**

$$U(n) \Big/ U(n_1)\, xU(n_2)x....xU(n_r)$$

**where** $U(n_k)$ **is the unitary group of order** $n_k$ **.**

**In the same vein, we identify the Grassmann manifold**

$(F(k,n-k;n)$ **as** $U(n) \Big/ U(k)\, xU(n-k)$

**This Grassmannian is often denoted by** $G_k(n)$**.**

**When** $k = 1$ **we have the complex projective space**

$\mathbf{P}^{n-1}(\mathbb{C})$ **of dimension** $(n-1)$

**When** $n_i = 1$ **for** $1 \leq i \leq r$**,**

**we have the complete flag manifold** $F(1,1,\ldots, 1;n)$

**often denoted by** $F(n)$**.**

**The flag manifold of length r is** $F(1,1,\ldots1,n-r;n)$

**denoted by** $F_r(n)$**.**

**Given the k – dimension**

**complex vector bundles** $E \xrightarrow{\lambda} X$

**then there is associated the**

**projective bundle** $P(E) \to X$ **with fibre** $\mathrm{P}^k(\not\subset)$

**Examples of these projective bundles include the following:**

$F_2(n) \to F_i(n)$ **with fibre** $F_1(n-1) = P^{n-2}(\not\subset)$

**and**

$F_3(n) \longrightarrow F_2(n)$ *with fibre* $F_1(n\text{-}2) = P^{n-3}(\not\subset)$

Mr. Vice – Chancellor sir, my principal research work is based on the computations of the KO – rings of certain homogeneous spaces and in particular the KO – rings of Flag manifolds of length r and projective bundles over flag manifolds.

**MY RESEARCH CONTRIBUTIONS**

My striking research contributions in Algebraic topology which paved the way forward for my other computations are: the reproof of a classical theorem by M. Fujii (Publ. Sec. Mat (U.A.B) vol. 29 n.2-3 Nov. 1985, pp 111-117. MR. 87i:55006) and a reproof of a classical theorem by S.G. Hoggar (NJS), vol. 21 n. 1 & 2 Dec 1987, pp 94 – 98. MR. 92i: 55007) using the Atiyah – Hirzebruch spectral sequence for KO – theory.

In 1988, I determined the structure of the KO – groups of the complex flag manifold of lengths 2 and 3 (Publicacious Matematique, vol 32 (1988), 159 – 164). With a determined effort to establish a general result for the KO-groups of complex flag manifolds, I established the relationship between the torsion subgroups of the KO-groups of projective bundles over flag manifolds within restricted range (abacus, vol 8, n.2 (1989), 208 – 209). This relationship allowed me to deduce the KO-groups of complex flag manifold of length 4.

Sensing that the above tremendous calculations might not yield good results in the general case, I revised the technique in 1992 during my visit to the University of Manchester, U.K and decided to compute the ring-structure instead of the ordinary group structure (Annal of Math. Analysis 1(1): 9 – 13, 1999). Sensing fresh problems with this new technique, I decided to start the computation of the KO-groups of complex projective bundles over complex projective spaces (Math theory 1(2): 1-4 (1998.)

**CONTRIBUTION TO BOOKS AT THE TERTIARY LEVEL**

I have contributed to the following books and monographs

1. **AJETUNMOBI, M.O.:** Date Analysis.

Recommendation and Conclusion in Research, Journal of Professional Adm; Jan – March. Vol.1, pp 28-29, 2002

2. **AJETUNMOBI, M. O. (1999):** Undergraduate Text in Group Theory. JAS Publishers, Lagos 181 pages

3. **AUDU, M.S. et al (2001):** Lecture notes series in Algebra. NMC, Abuja No 1.

4. **AJETUNMOBI, M. O. (2000):** Management Information Systems (MIS). LASUMBA lecture Notes series.

**MATHEMATICS DEPARTMENT:**

The faculty of science was established in 1984 at the inception of LASU and it had two departments: Department of Biological & Chemical Sciences (B & C) and the department of Physical and Mathematical Sciences (P & M). The department of Physical and mathematical sciences had 2 units namely the Physics unit and the Mathematics unit. P&M awarded honours degrees in both physics and mathematics. The mathematics unit offered a range of courses in pure applied and applicable mathematics. By 1990, it became that no mathematics graduate can do without the knowledge of computing. Abstract algebra had resurrected in computer science and computer Engineering, in the form of GATES. The abstract Truth table and the Boolean functions were utilized effectively in the simplification of electrical systems. Everybody loved the new technology and paid little or no attention to those who study the SAME theory in the abstract sense.

What exactly is the computer system?

The computer system consists of 3 parts:

- The hardware, which is the machine, the electrical gadgets which we can touch;
- The software, which are collection of algorithms written in particular computer languages and
- The manware, which are the people who work on the system.

The hardware utilizes anything that can exist in 2 states. Examples are:

- Conducting system
- Magnetizing system
- Punched Card phenomenon etc.

The two distinct states are denoted by O and 1 just for convenience, and instructions are obeyed using the Truth table. Let me give some examples. Denote, the AND connective by "**.**" the OR connective by "+" and the NOT connective by the complement notation. Let p and q be logic variables, then we have the truth table

| **P** | **q** | **p.q** | **p+q** | **$p^1$** |
|---|---|---|---|---|
| **1** | **1** | **1** | **1** | **0** |
| **1** | **0** | **0** | **1** | **0** |
| **0** | **1** | **0** | **1** | **1** |
| **0** | **0** | **0** | **0** | **1** |

The Nigerian Mathematics World felt cheated. People without any logical mind make good money, just by associating with the computer world. Mathematicians cannot afford to leave computing in the hands of these people; computer science is our making, it is resurrected abstract algebra and also we need the monetary reward *"Every labour is worthy of his wages" (Luke 10:7).*

In 1993, P&M introduced two programming courses;

MAT 232 – BASIC programming languages and

MAT 233 – FORTRAN programming language

These courses were started with the 486 desktop computer I brought back from the University of Manchester, U.K.

The aims of P&M were:

1. to sell these courses to the LASU community
2. to prepare the department for the eventual take off of computer science unit
3. to show and demonstrate the capability of the mathematics lecturers in the teaching of programming languages.

Without any external incentive, we forged ahead. The department of curriculum studies, Faculty of Education patronized the courses while other departments in LASU felt otherwise.

By 1998 P&M had shown its superiority in the teaching of these courses. P&M then applied to the LASU Senate for the establishment of computer science

unit. This move was strongly opposed by FETES and the report of the committee set up by the Deans of Science and FETES on the instruction of the Vice-Chancellor never surfaced. I was a member of that committee.

The desire of P&M to be relevant in computer science led to the establishment of a Part-time degree programme in computer science.

In 2002, P&M was split into the department of physics and the department of mathematics.

By 2004, the department of mathematics revisited the establishment of the computer science unit, and prepared document for Senate. Then came the new LASU in 2005. The first department created by the new Vice-Chancellor, Prof. Hussain is that of Computer Science.

Today, looking back at the Computer Science activities within the department, I feel very satisfied and happy. All the key actors at the LASU ICT are products of the department.

Twenty two years after the establishment of Mathematics programme in LASU, the department has just completed plans to start postgraduate programme in mathematics and statistics. This long delay is caused by the lack of suitable senior personnel. The department now has the resources.

**MANAGEMENT MATHEMATICS**

The advances in science and technology have led to the massive production of goods and the marketing of such goods and services. This led to the need for knowledgeable people to manage the manufacturing environment. These are the people who seek for the Masters in Business Administration (MBA).

Before now, we have had heuristic managers who did things without any scientific explanation and when such policies fail or are not adequate enough, it had always been difficult to explain why expected results were not achieved.

In recent times, there has been a high drive to formulate and execute Business policies using mathematical models. It is therefore not unexpected when many mathematicians joined in the teaching of management mathematics. Management mathematics has topics which include.

- Application of set theory;
- Application of matrix theory to the solution of linear systems and transition matrix in Brand switching problems in marketing;

- Application of series to simple and compound interest problems annuity and present value;
- Mathematics of Risk and portfolio management;
- Optimisation of manufacturing functions;
- Optimisation of scarcity problems;
- Inventory management and
- Queuing theory.

As the demand for Business managers increases, the demand for management mathematics teachers also increases. As expected with any society with little or no control, many unqualified teachers joined in the teaching. The situation becomes worse as the MBA gate is opened to all first degree graduates irrespective of the discipline at the undergraduate level.

The MBA program in LASU started in 1996 with Dr. S. O. Otokiti as the first Director.

With the large intake of students with varied backgrounds, the teaching of management mathematics presented many technical problems. One such problem is the fact that some of the mathematical models have structures different from the additive and multiplicative operations in the real number system.

**THE INVERSE OF AN ELEMENT**

One major problem encountered in the teaching of management mathematics is to explain what is meant by the inverse of an element in an algebraic structure. Many students have taken $a^{-1}$ to be 1/a. so when given a non-singular square matric A, it is difficult to explain that $A^{-1}$ is not 1/A. Infact 1/A does not exist. The problem is further compounded by a careless author who, for God knows what, writes

$AB = C$

$\Rightarrow$ **A = C/B**

where A,B,C are compatible matrices.

For an algebraic structure G with an identity element e, the inverse of an element a in G is another element b in G such that $b*a = a*b = e$

The element b is denoted by $a^{-1}$. So it is now clear that $a^{-1}$ is just a symbol for the inverse of the element a.

I now give some examples:

- In the real number system, R, under the additive operation with identity element O. The inverse of 2, is -2, So $2^{-1} = -2$.

- In the real number system, R, under the multiplicative operation, the inverse of 2, is ½. . So $2^{-1} = ½$.

This is what many people are used to.

- In the group of square non-singular matrices of order n, under the usual matrix multiplication the inverse of a matrix A is another matrix B such that AB = BA = I

where I is the identity matrix. One representation of $A^{-1}$ is given by

$$\mathbf{A^{-1}} = \frac{\textbf{Adjoint A}}{\textbf{det A}}$$

- In the group of compatible matrices for additive operation with identity element O, the inverse of A is –A. Thus

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

**FORECASTING BUSINESS ACTIVITIES**

It is true that everybody is in business in order to make profit, but today with the advancement in technology, knowledgeable people are in business in order to make MAXIMUM profit. Business environment is surrounded with risk and the minimization of these risks will lead to profit maximization. One such method of risk minimization is to have a "Good" further idea of the business activities. In business we can count our chickens before they are hatched. This procedure is called FORECASTING. Forecasting techniques are used to predict the future in business activities, using the past business data.

The three functional areas of business that make the most use of forecasting technique are marketing, production and finance. The major forecasting techniques include

- Regression Analysis for both the linear and multiple models
- Moving Averages in Time – series
- Exponential smoothing in Time series which improves on the Moving Average technique.
- Learning Curve and
- Transition matrix.

To have a reliable forecast, the past data must correlate "very well", and the forecast errors must be unbiased.

The introduction of fast computers has now introduced simulation as a forecasting technique. The success of computer simulation as a forecasting technique is now under investigation. This lecturer is now working on the use of exponential smoothing technique in which the value of the smoothing constant is time dependent following the works of Rudolph Kalman.

**SECURITY OF BUSINESS INFORMATION**

It is not enough to minimize business risks by forecasting the future, a greater problem is to secure the business data and information, some of the information needed to be secured are:

- Formulas;
- New products under development ;
- Quarterly earnings before they are released to the general public;
- Customer lists , and
- Employees phone numbers.

Advances in computer technology have created an acute need for people to monitor and secure the data and information needed for their business activities. Business information security covers both products and processes to prevent unauthorized access, modification, and deletion of information and data. It also involves the protection of resources by preventing them from being disrupted by situations or attacks that may be largely beyond the control of the person responsible for information security.

Business information security can be classified as

- Physical security
- Operational security and
- Management and Policies

A mathematician's concern is on the operational security.

Operational security deals with how the business environment does things. This includes the use of computers, telecommunication systems and management information. Operational issues include access control, authentication and security topologies. The major operational issue to a mathematician is the security of the telecommunication networks.

The goals of Business information security are:

- Prevention of security breaches
- Detection of security breaches and
- Response to develop strategies and techniques to deal with an attack or loss of data.

The network can be secured through:

- Access control which defines how users and systems communicate and in what manner. It has the following models:

  Mandatory Access control (MAC),

  Discretionary Access Control (DAC) and

  Role-Based Access Control (RBAC)

- Authentication, which proves that the user or system is actually who they say they are;
- This is carried out using the following;
- Something you know e.g password PIN or Challenge Handshake Authentication protocol (CHAP);
- Something you have e.g. a smart card, certificate, token or Kerberos;
- Something you are e.g. fingerprints or retinal pattern.

System also authenticate each other using similar methods.

Frequently system will pass private information between each other to establish identity. Once authentication has occurred two systems can communicate in the manner specified in the design.

**CRYPTOGRAPHIC SECURITY**

I have taught the MBA class for 10 years and I am very proud of the various managerial positions these "boys" and "girls" occupy in the society.

They have associated me with quantitative techniques. I mean with mathematics. My major concern, a mathematician concern is how to protect the business data/information of my business students during transmission. One way of securing telecommunicated data is CRYPTOGRAPHY.

Cryptography is the science of keeping oral and written forms of communication secret as well as providing a means of authentication of the communicating parties.

The surest way to preserve the secrecy of information is to hide it so effectively that those who seek to obtain it do not recognize its presence.

Cryptographic methods include:

- Steganography;
- Transposition cipher;
- Substitution cipher;

By combining a mixture of the above methods, cryptographers found that stronger concealment cipher, called a product cipher is produced. Even as product cipher became more complex, it can still be attacked using statistical methods.

Ideally, ciphertext should present itself as a random string of letters or bits. The cryptographer wants to eliminate any clues that might help the cryptanalyst to reclaim plaintext. This means eliminating statistical relationship between ciphertext and the underlying plantext.

Diffusion is defined as the dispersion or distribution of plaintext in a statistically random manner over the ciphertext. Each application of diffusion and confusion is known as a round. The repeated application of rounds is called iteration.

The Data Encryption standard (DES) is an example of an iterated product cipher. It was once the encryption standard of the United State of America (U.S.A) government and is a block cipher that uses 16 rounds of activity against a 64 – bit block of data. Other variants are:

- Triple DES (3 DES), which is an enhancement to DES, and it concatenates DES ciphertext with itself and uses up to three keys.
- Advanced Encryption standard (AES) which replaced DES as the new U.S. federal standard. AES is a cipher block algorithm that uses a 128 – bit, 192-bit or 256-bit block size and a key size of 128 bits.
- Cryptologists always assume that enemies (i.e attackers) know the encipherment and decipherment algorithms, so security resides entirely in the key or keys used by the cipher. With an iterated product cipher, statistical analysis of the ciphertext letters is no longer a practical option to crack the ciphertext message to yield the

true message. THEN the ecryptanalyst's best attack is to try every possible key – a brute force attack.

- Mr. Vice-Chancellor sir, this is not difficult, considering the recent advances in computer technology using high speed processors and distributed computing power.

**PUBLIC-KEY CRYPTOGRAPHY**

So far, I have discussed the transmission of business data, using a single key to encrypt and the same key, or a copy of it, to decrypt the data. These single – key, symmetric algorithms work fine as long as the key can somehow be shared between the parties that wish to use it. The problem now is that of key management.

I now discuss two methods of key management. The first was proposed by Whitefield Diffie and Martin Hellman. The Diffie – Hellman key agreement protocol uses two sets of mathematically related keys and a complex mathematical equation that takes advantage of this relationship. If each of two computers calculates its own set of related keys (neither set being related to the other) and shares one of the keys with the other computer, they each can independently calculate a third secret key that will be the same on each computer.

The second method for the exchange of session key is the use of Public-key Cryptography. This algorithm is asymmetric – it uses a set of related keys. If one key is used to encrypt the message, the other is used to decrypt it. In this circumstance, if each party holds one of the keys, a session key can be securely exchanged. In the typical arrangement, each party has their own set of these asymmetric keys. One of the key pairs is known as the private key and the other as the public key. Public keys are exchanged and private keys are kept secret. Even if a public key becomes, well, public, it does not compromise the system.

Public–Private key pairs can be used to exchange session keys. To do so, each party that needs to exchange keys generates a key pair. The public keys are either exchanged among the parties or are kept in a database. The private keys are kept secret. When it is necessary to exchange a key, one party can encrypt it using the public key of the other. The encrypted key is then transmitted to the other party. Since only the intended recipient holds the private key that is related to the public key used to encrypt the session key, only that party can decrypt the session key. The confidentiality of the session key is assured, and it can then be used to encrypt business data communication between the two parties.

## NON-REPUDIATION

A situation similar to the above is non-repudiation. Non-repudiation is the guarantee that something came from the source it claims. It also means that the sender cannot claim to have not sent the message. Digital signatures can be used to establish non-repudiation.

Digital signatures can be produced using public key cryptography. In this scenario, the private key of the sender is used to encrypt the message, and the sender's public key can be used to decrypt it. Since only the sender of the message can have the private key, if the message is decrypted with the corresponding public key, it must have come from that person.

## MATHEMATICS FOR SECURITY

It is clear from the above that the security of business data during transmission is strongly based on the relationship between the private and public keys. The mathematics of this relationship is the most active part of mathematics today and many professional mathematicians are employed in this area.

The search for these relationships forms the topic of this Inaugural lecture" Mathematics for Security, and World Peace". The security of mathematical cryptography rests on the fact that even given the public key, it is infeasible to determine the private key, and given the ciphertext, it is infeasible to determine the plaintext.

Crytographic algorithms span the mathematical world of number theory, complexity theory, elliptic curves, vector calculus, tensors and set theory.

Today, the use of the elliptic curve algorithm gives the most secure option. Cryptographic algorithms revolve around the following three mathematical problems:

1. **Integer Factorisation Problem (IFP)** RSA is the best known of a family of systems whose security relies on the difficulty of the IFP
2. **Discrete Logarithm Problem (DLP)** As with IFP, there are both special purpose and general purpose algorithms that are used to solve the DLP. The fastest general – purpose algorithms known for solving the DLP are based on a method called the index-calculus. The index-calculus method uses a database consisting of small prime numbers and their associated logarithms. This method may also be applied on a distributed computer network and run in parallel.

3. **Elliptic Curve Cryptosystem (ECC)** In ECC, DLP is utilized over the points on an elliptic curve $\mathbf{y^2 = x^3 + ax + b \pmod p}$ for two integers a,b and a prime P. An elliptic curve can also be defined over the finite field consisting of $2^m$ elements. Such a representation offers extra efficiency in the operation of the ECC.

The algorithms of these three cryptographic systems are based on the following modulus arithmetic:

1. Two integers a, b belong to the same residue class modulo an integer n, iff, n divides a-b written as $a \equiv b \pmod n$.
2. A theorem of Fermat and its generalisation by Euler.

**The Problem**

Given an integer n with a prime factorization

$$n = pq$$

Choose a random interger e,

**which satisfies $o < e < n$, with $(e, \varphi(n)) = 1$ and $e$ odd**

**Then compute $d$ such that $ed \equiv 1 \pmod{\varphi(n)}$**

**Where $\varphi(n)$ is the Euler phi number of $n$**

**The public key exponent is $(e,n)$ while the private key exponent is $(d,n)$**

**Application**

**Given the plaintext T, this is encrypted with the public $e$**

$C = T^e \bmod n$

**At the other end, the ciphertext $C$ is decoded by the private key $d$ as**

$C^d \pmod n$

**and this gives $T$ back.**

The security of the above three cryptosystems depends on the following:

1. It is widely believed that to break RSA in general, the IFP must be solved (i.e. prime factorization) for the integer n. The security of the

RSA algorithm can be increased greatly by ensuring that the integer n is a large number.

2. The problem in discrete logarithm system is the computation of $g^x \pmod p$where p is a prime and $o \leq g < p$ for some integer $x$.

3. Elliptic curve system uses a variant of DLP, but instead of direct integer algebra, elliptic curve system uses an algebraic formula to determine the relationship between public and private keys within the universe created by an elliptic curve. If $K(x,y)$ and $Q(x,y)$ are on the elliptic curve, then K + Q is on the curve. The elliptic curve discrete logarithm problem (ECDLP) for a prime p is to determine an integer x such that

$$Q = xK$$

where xK represents the point K added to itself x times

**CRYPTOGRAPHY TODAY**

One of the advantages of ECC is that ECDLP is believed to be harder than both IFP and DLP modulo p. This extra difficulty makes ECC one of the strongest public key cryptographic systems known today.

**WORLD PEACE**

Peace is a function of careful interrelationship between entities, a state of freedom from war or disturbance. Every war had always ended in a conference hall. Every disturbance had always being resolved through the provision of information. One can then deduce that peace can be achieved through the provision of adequate information.

It has been shown that data needs to be protected from adversaries. The data attacker is also very anxious when data is over secured. The dilemma of data security and data attack led to the study of mathematical cryptography and the existence of mathematical cryptanalyst. Mathematics and in particular number theory will continue to be enriched as long as the cryptosystems exist.

Cryptosystem can be seen as a state of mathematical warfare. Mathematics is used in data security and on the other hand, the same mathematics is used by cryptanalysts to decode the secured data.

Since there is no morality in warfare, a non-moral question is Who is a computer criminal?

Is a computer criminal, the organisation that secures its data in order to achieve a competitive advantage or the organisation that decodes the secured data of other organisations in order to achieve a competitive advantage also?

There cannot be world peace as long as the cryptosystem exists.

**RECOMMENDATIONS**

Mr. Vice-Chancellor Sir, based on the issues raised in the lecture, I propose the following recommendations:

1. Mathematicians should play more active role in the development of mathematical cryptographic systems
2. More Algebra courses for 300 and 400 levels computer science students
3. Effective collaboration between Nigerian Mathematicians and computer scientists should be introduced.
4. National Mathematical centre (NMC), Abuja should spearhead the collaboration between mathematics and computer science in the areas of data security during transmission
5. More workshops on number theory particularly on elliptic curves should be organized.
6. More collaboration between mathematicians and statisticians in the development of business oriented quantitative techniques
7. Mathematicians and statisticians should participate more in the teaching of business oriented quantitative techniques.

**CONCLUSION**

Mr. Vice Chancellor sir, I have in this lecture given some varied definitions of mathematics and an overview of my research on KO-theory of certain homogeneous spaces, in particular flag manifolds and flag bundles

I then discussed my involvement, experience and contribution to the teaching of quantitative techniques on the MBA programme in Lagos State University.

In the process of the lecture, I explained that my love for the security of the Business Executives data during transmission afforded me the opportunity to study the mathematics of cryoptographic systems and highlighted the role played by elliptic curve cryptography in the security of data during transmission

I then concluded by proffering ideas that could help improve teaching of quantitative techniques to MBA students and the study of data security during transmission.

**ACKNOWLEDGEMENTS**

First I thank the Almighty God, the creator of all things for making me an University Inaugural Lecturer. I wish to express my gratitude to the following three mathematics professors who shaped my life as an algebraic topologist:

1. Professor Moon, my undergraduate lecturer at the University of Ife, Ile-Ife in 1974;
2. Prof. B. O. Balogun, my M.Sc. project supervisor in 1977 at the University of Ife, Ile-Ife;
3. Prof. S. A. Ilori, my Ph.D. supervisor, at the University of Ibadan, Ibadan.

I also wish to thank all my lecturers at the following universities:

- University of Ife, Ile-Ife (now Obafemi Awolowo University)
- University of Ibadan, Ibadan
- University of Lagos (Department of Computer Science), Akoka
- University of Manchester, U.K.

I wish to express my appreciation to all my colleagues in the faculty of science, particularly members of staff in the departments of mathematics, physics and (presently) computer science.

To all the administrative staff in the department, I say thank you.

I wish to thank Dr. S. O. Otokiti, the first director of the MBA programme for inviting me to teach on the MBA programme

I wish to put on record, people and organizations that made mathematics research easy for me.

1. Prof. (Mrs.) Ebun Oni, Dept. of physics, University of Ibadan Mama, I love you. She included my name along with other colleagues in the department of physics to ICTP, Italy;
2. Prof. O. A. Kuku, Maths Dept. University of Ibadan;
3. International Mathematics Union (IMU) which sponsored me to the University of California, USA in 1986;

4. International Centre for Pure and Applied Mathematics (ICMPA) NICE, France;
5. International Centre for Theoretical Physics (ICTP), Trieste, Italy;
6. British Council;
7. PISA, Cortona, Italy
8. Centre de Roceta mathemate, Barcelona Spain;
9. Lagos State Government Scholarship Board;
10. Federal Government of Nigeria Scholarship Board;
11. Department of Mathematics, University of Lagos, Akoka;
12. On the Social front, I sincerely thank the First Club, Igbogbo, Ikorodu for giving me the opportunity to relax socially.

I wish to remember my late parents Chief B. O. Ajetunmobi and Madam Abegbe Serah Ajetunmobi (Nee Bamgbose) Mama, you tried your best for me. I also wish to thank my sisters and brothers.

Finally, I wish to thank my wife, Nike Ajetunmobi and my children, Tosin & Tope Ajetunmobi. You are the pillar of my strength.

Thank you all for listening.

**REFERENCES**

1. **ADU, D.I (2003):** Mathematics; An Exact Science: The Axion of Choice- A case in Point. University of Lagos Press. Inaugural lecture series.

2. **Bragg, R; Rhodes – Ousley, M; Strassberg, K (2004):** Network Security: The complete Reference. The McGraw-Hill/Osborne

3. **Ilori, S. A. (2003):** Mathematics for Recognition and Relevance. Inaugural lecture. University of Ibadan.

4. **Nicholas, R.K., Lekkas, P.C. (2002)**: Wireless Security. Models, Threats, and Solutions. McGraw Hill Telecom.

5. **Salimanu, Y. A. (2003):** Mathematics: An Essential Tool for Sustainable Technological Development in Nigeria 8th Inaugural lecture series. LASPOTECH inaugural lecture series No.8.