THE IMPACT OF MATHEMATICS ON SECURITY AND TRUST IN E-COMMERCE, E-BUSINESS AND E-GOVERNMENT IN AFRICA.

Kondwani Thangalimodzi
(Msc Student): thangalimodzi@yahoo.com or thangalimodzi@gmail.com

Mzuzu University

Abstract

It has been observed that Africa is lagging behind on Information and Communication Technology as compared to other Continents. This could be caused by lack of trust from stakeholders on security. If the underlying mathematics on information security is well understood and applied in the development of online systems in Africa, there would be more trust on the use of online systems. Therefore in this article we describe the relationship between Mathematics and Security in Information and Communication Technology (ICT). Mainly, we discuss how mathematics in cryptology can address trust issues essential for online communication systems such as e-commerce, e-business and e-government in Africa.

1. INTRODUCTION

For users to fully adopt the electronic communication technologies of e-commerce, e-business and e-government, users need to be confident that security risks in conducting financial transactions are minimized and their privacy is protected. According to Hana newsagency, Africa must use ICTs to improve public services, overcome poverty, and enable regional integration - World Bank(2007).

The World Bank announced late this year (2007) that it is expected to double its commitment to Information and Communication Technologies (ICTs) in Africa to US$2 billion by 2012. According to a statement issued at the 'Connect Africa Summit' in Kigali, this year the funds will be channeled through the World Bank's three financing arms. These include the World Bank, the International Finance Corporation (IFC), and the Multilateral Investment Guarantee Agency (MIGA). The financing will continue to promote private sector participation, while supporting public private partnerships to address market gaps, with an emphasis on affordable high speed Internet. Robert B. Zoellick, World Bank Group President in a televised address to the Connect Africa Summit said that, "this access gap must be addressed before Africa can be connected to the globalized economy and use ICT to improve public services, overcome poverty, and enable regional integration."

What is e-commerce? E-commerce is a term for electronic commerce which refers to buying and Selling online, with or through a website, or by means of email. Ecommerce or electronic commerce is usually subdivided into B2B (business to business: wholesale), B2C (business to customer: retail) and C2C (customer to customer: auctions and information portals). Ecommerce comes in forms that are continually evolving.

What is e-business? E-business , or Electronic Business, is the administration of conducting business via the Internet. This would include the buying and selling of goods and services, along with providing technical or customer support through the Internet. e-Business is a term often used in conjunction with e-commerce, but includes services in addition to the sale of goods. It is where information technology is applied to all aspects of company's operations. In e-business are to be found systems for CRM (customer resource management), ERP (enterprise resource planning), SFM (sales force management), SCM (supply chain management) and EP (electronic procurement).

What is e-Government? E-Government(from electronic government, also known as e-gov, digital government, online government or in a certain context transformational government) is a generic term that refers to any government functions or processes that are carried out in digital form over the Internet.

Local, state and federal governments essentially set up central Web sites from which the public (both private citizens and businesses) can find public information, download government forms and contact government representatives. For example, a government can offer on-line filing of income taxes , which reduces the amount of paperwork, streamlines the process and speeds the amount of time that taxes are filed. E-government also refers to the standard processes that different government agencies use in order to communicate with each other and streamline processes. e-Government refers to governments use of information technology to exchange information and services with citizens, businesses, and other arms of government. e-Government may be applied by the legislature, judiciary, or administration, in order to improve internal efficiency, the delivery of public services, or processes of democratic governance. The primary delivery models are Government-to-Citizen or Government-to-Customer (G2C), Government-to-Business (G2B) and Government-to-Government (G2G) & Government-to-Employees (G2E). The most important anticipated benefits of e-government include improved efficiency, convenience, and better accessibility of public services.

The World Bank says it's financing of Africa will support partnerships between Governments and businesses in order to help fill gaps not being addressed by the market, especially for connectivity of rural areas and small towns.

According to Hana news IFCa financing will continue to support private sector African companies in telecoms and IT, as well as major infrastructure projects such as the Eastern African Submarine Cable Systems (EASSy) - together with partners including the African Development Bank. IFC will also encourage investments in new applications such as mobile banking.

Such innovative use of technology has tremendous opportunity to deliver social and financial services, especially in rural areas. Late this year (2007).Cisco Systems announced that it is to invest $10 million to develop its network infrastructure on the African continent. According to the report, five African countries who stand to benefit from the initiative are Nigeria, Cameroon, Ethiopia, Rwanda and Kenya. Announcing the investment, Cisco's area academy manager for West and Central Africa, Mr. Julius Ayuk Tabe, the opportunity would afford the organisation to expand its zeal in empowering Africans and especially the youth by deploying Information and Communication Technologies (ICT) for development via the networking academies.

The Plenipotentiary Conference of ITU, which took place in Antalya, Turkey in November 2006, recognized the need to make Internet content available in non-Latin based scripts. Internet users are more comfortable reading or browsing through texts in their own language and a multilingual Internet is essential to make it more widely accessible. The WSIS outcomes also focused on the commitment to work towards multilingualization of the Internet as part of a multilateral, transparent and democratic process involving governments and all stakeholders. All these stories tell us the need to start development of security systems in Africa. Localizing systems by the use of local languages in systems development has provoked the need of developing security systems locally but these need mathematics.

Despite the adverse publicity of electronic communication (online) in Africa, and the spectacular failures, ecommerce is here to stay and we can run a way from developing security systems, failure which may result in exposing our continent's systems to attack. Therefore there is a need to address security, trust and confidentiality issue.By confidentiality we mean the protection of transmitted data from passive attacks or protection of data from unauthorised disclosure. Lack of assurance in the security schemes that are implemented bring lack of trust on the systems. This becomes a barrier on the adoption of technologies in electronic communication.This problem of trust on security can be solved through the use of cryptography. There are many cryptosystems that are robust which are in use today, nevertheless trust pertaining to security of the electronic communication technologies using these robust cryptosystems is still an issue to be addressed. When you upload information to a server, when you transact online, buy and sell things online, bank and check balances online normally you are sure that your personal information is secure, that is, it can not be read or accessed by any unauthorised third party.This is all possible because of mathematics. The Connect Africa Summit, which took place this year (2007) under the patronage of Rwandan President Paul Kagame, aims to secure concrete commitments from private sector, Governments and development financial institutions to ensure all African capitals and major cities are connected to high speed Internet by 2012.

2. MATHEMATICS AND SECURITY

According to Merriam webster online dictionary. Mathematics is defined as the s cience of numbers and their operations, interrelations, combinations, generalizations, and abstructions and of space configurations and their structure, measurement transformations, and generalizations. Mathematics has many important applications in science and technology. It is at the heart of modern commercial and industrial activities. In the past years, mathematics has undergone tremendous development.New theories have been introduced and new applications have been developed. Among these are X-ray tomography, mathematical finance, digital information compression, Internet search engine, nuclear waste disposa.,security for e-commerce, e-government and e-business.

Mathematics is doing its best to try to address these questions with the goal of making on-line transactions totally secure. The mathematical tools which are making all this possible are ones that people in the past thought were inapplicable.New mathematical techniques are being discovered for those who try to create a secure Internet environment and those who want to steal money online from banks. In mathematics specifically in abstract algebra and its applications. The problem of computing discrete logarithms and the problem of integer factorization forms the basis of numerous cryptographic protocols. The difficulty of these problems has been used to construct various cryptographic systems.

For example given a finite group G, and g,e $\in$ G, to find m (if it exists) such that

$$g^m = e. \tag{1}$$

This problem is known as the Discrete Log Problem.

Say we are given

$$G = Z_n^* \tag{2}$$

under *, find an m such that

$$g^m = e(modn) \tag{3}$$

.

In this article we show the role mathematics play on security systems. There are many cryptosystems that are in use in information security. In this paper we examine the computational and cryptanalytical implications of ELGamal Cryptosystem. The ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key agreement. Diffie-Hellman (D-H) key exchange is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.

ELGamal cryptosystem is based on the Discrete Logarithm Problem.

ELGamal cryptosystem in Z_p^*.

Let p be a prime such that the Discrete Logarithm Problem in (Z_p^*) is infeasible, and let $\alpha\in$ (Z_p^*) be a primitive element. Let

$$\mathbf{P} = Z_p^* \tag{4}$$

$$C = Z_p^* * Z_p^* \tag{5}$$

and define

$$\mathbf{K} = (p, \alpha, a, \beta) : \beta = \alpha^a(modp). \tag{6}$$

The values p,α,and β are the public key, and 'a' is the private key. For

$$K = (p, \alpha, a, \beta), \tag{7}$$

and for a (secret) random number k∈Zp-1, define

$${}^{e}K(x, k) = (y_1, y_2), \tag{8}$$

where

$$y_1 = \alpha^k modp \tag{9}$$

and

$$y_2 = x\beta^k modp \tag{10}$$

For y_1, y_2∈Z_p^*

$${}^{d}K(y_1, y_2) = (y_2(y_1^a)^- 1modp, \tag{11}$$

Briefly that's how El Gamal cryptosystem works. The plaintext x is embeded in y_2 and y_2 is a product of the plaintext x and $\beta^k modp$. But y_1 which is a^k mod p is also transmitted together with the ciphertext. Bob who knows the private key ,a, can compute β^k from a^k. Now he can easily get x by dividing y_2 by β^k.

3. ENCRYPTION AND DECRYPTION CONCEPT.

By encryption, we mean a process of converting information to a disguised form in order to send it across a potentially unsafe channel. The reverse process is called decryption. Using strong encryption techniques, sensitive, valuable information can be protected against organized criminals, malicious hackers, or spies from a foreign millitary power. Cryptography used to be almost exclusively a tool for the millitary. But today it is a tool for security in e-commerce, e-business and e-government. The electronic communication setting is that when one is trying to communicate with someone. Say Alice would like to send a message to Bob. There is a possiblity that the message can be intercepted by someone say Eave while in the communication channel .

Alice and Bob want to communicate with each other. However, in general communication channels are not secure. Eave is eavesdropping on the channel. Any message m that Alice sends to Bob is also received by Eve. To prevent Eve from understanding the conversation that Alice and Bob are having, they use encryption. Alice and Bob first agree on a secret key K_e.

They have to do this via some communication channel that Eve can not eavesdrop on. When Alice wants to send the message m,, she first encrypts it using an encryption function. The encryption function is E(K_e,m) and then call the result the cipher text c . Instead of sending m, Alice sends the cipher text c:=E(K_e,m). When Bob receives c He can decrypt it using the decryption function D(K_e,c) to get the original plaintext m that Alice wanted to send to him. Eve does not know the key K_e,so when she recives the cipher text c she cannot decrypt it.

4. SECURITY SERVICES, MECHANISMS, AND ATTACKS

To manage security. There is a need to find a systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements.

Three aspects of information security

William Stallings(2003) points out the three aspects of information security as

I.Security attack: Any action that comprises the security of information owned by an organization.

II.Security mechanism: A mechanism that is designed to detect, prevent, or recover from a security attack

III..Security service: A service that enhances the security of the data processing systems and information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service

I.ATTACKS

An attack can be defined as an assault on security system that derives from an intelligent threat; that is, an intelligent act that is deliberate attempt to evade security services and violet the security policy of a system. While a threat is just a potential for a violation of security which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. In cryptography there is a distinction between attacking a system and attacking somebody personally. Any work is fair game. If somebody develops a system, it is an automatic invitation to attack it. One way to learn how to design secure cryptosystems is to look for weaknesses in any system. An attack on your system is not an attack on you. We always criticize the system not the designer. If you criticize the designer you will get the negative response.

The spirit fo finding weak points in a system creates misunderstandings in many people. Others think we are attacking somebody or an organisation when we attack their system and then complain about our manners. Generally in our society an attack on an idea is taken to be an attack on the Author . In cryptography the attitude is different. We don't take crticisms of our ideas as personal attack.

As G.J. Simmons points out, information security is about how to prevent attacks or, failing that, to detect attacks on information based systems wherein the information itself has no meaningful physical existence and then to recover from the attacks [SIMM92]. A good example of a security could be to gain unauthorised access to information.

Three dimensional axes of attack

I.Newly discovered cryptanalytic algorithms

II.Ever more powerful computers including computational hardware and memory.

III.New and better architectures for performing computational tasks.

II. MECHANISMS

There are many machanisms designed to detect, prevent, or recover from a security attack. How ever, there is one particular element that underlies many of the security systems in use: cryptographic techniques. Encryption of information is the most common mechanism for providing security.

III. SECURITY SERVICE

Electronic information takes on many of the roles performed by paper documents. Accordingly, the types of functions associated with paper documents are performed on documents that exist in electronic form. Documents typically have signatures and dates; they may need to be protected from disclosure, tampering, or distruction; they may be notarized ; may be recorded or licenced and so on. The impact of being able to access any information from anywhere in the world is revolutionary and creates many opportunities for mankind. Unfortunately, it has also opened up opportunities for criminal and unethical individuals and groups. It lets people from countries with unregulated cyberlaws attack businesses and intrude on other peoples privacy Early attacks on government and bank data were rather limited geographically or through the use of controlled channels,such as leased lines. They were also less visible and, once detected, easy to counteract. Today, attacks on any prominent Internet service can easily impact your needs, making them more noticeable. An even bigger problem is related to privacy. While using these technologies others are able to track your behavior, movement, and habits if the technology has no strong security. The implications are numerous. Other companies realize that this is valuable information that they can use in carrying out their businesses, to track what you buy and browse, from where you connect to the Internet, and so on. The world of wireless communication with all kinds of gadgets has open up even more opportunities for attacks. All of this creates many challenges for security and privacy experts today. Some are technical, such as scalability, more efficient cryptographic techniques, safe languages, and better secret key distribution. Social and legal aspects pose more challenges. Everything we are used to thinking about in the physical world is reversed in the electronic world. You win by creating boundaries and increasing reproduction, or at least access, coststhat is what develops a sense of security. When I log into a machine, I want to know that my information is not being inadvertently shared with others. When I send an e-mail, I want to know that it is not being stolen, copied, or intercepted during transmission. When I trade stock online, I need to know that when I say something that is what happens and not some other transaction. All the innovations thesedays are based on some kind of cryptographic- like function. Only by recreating brickwall secrets are we going to be able to produce these necessary adjuncts to what otherwise is a seamless sphere of information.

5. CRYPTO-OBSOLESCENCE

If a cryptosystem has just been developed, it is robust and immune to most existing current powerful cryptoanalysis. Many users appreciate its functionality. Now as time goes it starts to age, but experts continue with cryptanalysis. Cryptanalysis becomes stronger , more refined , and increasingly dangerous to the aging crypto system.

As algorithms are getting older they offer less protection . This is because they remain fixed and are surrounded by the new cryptanalytic techniques.

6. THE IMPACT OF CRYPTOGRAPHY IN REAL WORLD SYSTEMS

On themselves mathematics are not very useful and it's the same with cryptography. For cryptography to be useful it has to be incorporated in another system. Cryptography can be compared to a lock in the physical world. The lock itself is useless. It becomes important when it has been incorporated in a another system. It can be a door on a building, a chain, a safe or something. The lock is just a small part of a much larger security system. Though small, but it is a very critical part. Cryptography is like a part of security that allows others to access the systems while others are not allowed. Most parts of the security system are like walls, they are designed to keep everybody out. Cryptography takes the role of the lock. It has to distinguish between good access a bad access. This is a much more difficult than just keeping everybody out. Therefore, cryptography forms a point of attack for any security system

Cryptography is useful if the rest of the system is also secure. An attacker who breaks a cryptosystem has low chances of being detected. There will be no traces of the attack, since the attackers' access will look just like a "good " access. Many modes of attack leave traces, or disturb the system in some way. An attack on the cryptography can be fleeting and invisible, allowing the attacker to come back again and again.

7. WHY DO WE NEED CRYPTOGRAPHY IN E-COMMERCE, E-BUSINESS AND E-GOVERNMENT

E-Commerce and E-Business is done openly on e-markets , e-contracts and others. Cyptography may not be the solution of our problem. It might be part of the solution, or it might be part of the problem. If you want to prevent unauthorised use of your computer, you can do it by avoiding entry of people to your room. This might be by locking the door of your office. But with cryptography it's different you just encrypt the information you want to be secure and keep the key. The encrypted file is no longer secret. And you don't have to get worried about the file you have encrypted provided you keep the key secure. But where can you store the key? because a good key is too long to remeber.

Some cryptographic methods rely on the secrecy of the encryption algorithms, such algorithms are historical and are not adquate for todays world of technology.

Cryptography is a crucial part of many security systems. It provides a feeling of security, but no actual security. This is what most customers want . They want to feel secure while using the systems but they don't want the hassle of actual security. Cryptography is a solution in itself. Mathematics is what is used in encryption and decryption algorithm designs. Therefore, it also has a great impact on security and trust to open systems that are used in technology today. some of these are e-commerce, e-business and e-government.

Cryptography is difficult. In most cases, breaking a cryptographic algorithm boils down to solving mathematical problems such as to find a solution to an equation or to invert a function. These mathematical problems are considered "hard" or "intractable". More over the adversarial setting conspire to make life for a cryptographer very hard. Sometimes when you have little knowldge about cryptography you think it is easy. But sometimes people pay for and build systems designed by novices. And because bad cryptography looks just like good cryptography, until it is seriously attacked, some customers are fooled and buy the product. Later on they loose trust on the security of the systems in use.

Not withstanding the fact that cryptography is difficult, it is still an easy part of a security system. It is because there are people who know how to do a reasonably good job by the use of mathematics in cryptography

8. CONCLUSION

Mathematis is a very important tool of security. With mathematics we can build the confidence of Africans in using e-commerce, e-business and e-government in Africa.

9. REFERENCES

1. Jonathan Katz, Steven Myers, and Rafail Ostrovsky.Cryptographic Counters and Applications to Electronic Voting. Advances in Cryptology - EUROCRYPT 2001

2. CRYPTOGRAPHY DEMYSTIFIED by JOHN E. HERSHEY-(McGraw-Hill TELECOM)(2003)

3. PRACTICAL CRYPTOGRAPHY by Niels Ferguson and Bruce Schneier(2003)

4.http://www.mathaware.org

5.Cryptography and network Security Principles and Practices, 6.William Stallings (2003).

7. Hana newsagency

8. Internet search engines

9. Cryptography Theory and Practice. Douglas R. Stinson)(2002) (CHAPMAN AND HALL)