ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Developing a Secured Internal Memo Platform Using the SHA-1 Cryptography Technique for the University of Agriculture Makurdi-Nigeria

[I]D.D. Atsa'am, [II]E.I.Oko
[I,II]Dept. of Mathematics/Statistics/Computer Science, University of Agriculture, Makurdi, Nigeria

Abstract
This research was embarked upon with the aim of developing a secured internal memorandum platform using the SHA-1 cryptography technique for the University of Agriculture Makurdi-Nigeria. The current method in use at the university does not guarantee confidentiality and integrity of information. Memos are typed on computer systems and printed on papers, stapled with pins and delivered to recipients by dispatch riders. With this arrangement, an adversary could gain illegal access to a document that does not concern him, thus compromising confidentiality and integrity. With the memo platform developed in this research, messages from the first party (sender) to the second party are encrypted using the SHA-1 algorithm. The information is then decrypted by the second party by supplying the right key for the message, thereby securing the information from a third party (intruder) for which the message was unintended. Java programming language was used to develop the cryptographic system, MYSQL server for the database design and JBOSS tool as an application server. The new system is evaluated against the manual approach of sending and receiving memos within the University of Agriculture community.

Keywords
Encryption,Decryption, University of Agriculture Makurdi, Cryptography

I. Introduction

Cryptography is the study of information hiding and verification [1]. It includes the protocols, algorithm and strategies to securely and consistently prove or delay unauthorized access to sensitive information and enable verification of every component in a communication.

The University of Agriculture, Makurdi (UAM) was established on 1st January, 1988 as a specialized university in the area of Agriculture and allied sciences [3]. As it is the case with such organizations, the UAM community uses internal memorandum (internal memo) to communicate on official matters within the university. A memo could originate from a staff of one department to a staff of another department, or from within the same department. Memos within the UAM convey information such as staff promotions, disciplinary decisions, approvals, and any other form of management or departmental policies. Most of the information conveyed within memos deserves confidentiality because of their sensitive nature.By confidentiality, we mean that ideally, only the sender and receiver of such memos should be aware of the memo content.

Unfortunately, the method employed for sending and receiving internal memo within the University of Agriculture Makurdi does not guarantee confidentiality. Memos are typed with computer systems and printed on papers, stapled with pins and delivered to recipients by dispatch riders. With this arrangement, a third party, which can be the dispatch rider, a hijacker or a rival, can conveniently compromise the confidentiality of a memo when they gain illegal access to the document.

It is in order to guard against this that this research is embarked upon to develop a secured internal memo platform for UAM. In the design, we will use the SHA-1 encryption algorithm to encrypt an internal memo before it is sent to the recipient. Upon encryption, a decryption key will be generated; the sender will pass this key across to the receiver, through a mutually agreed medium and will be used to decrypt the contents of the memo.

A. Literature Review

Within the context of any application-to-application communication, there are some specific security requirements [1] including:*Authentication:* The process of proving one's identity.*Privacy/confidentiality:* Ensuring that no one can read the message except the intended receiver.*Integrity:* Assuring the receiver that the received message has not been altered in any way from the original.*Non-repudiation:* A mechanism to prove that the sender really sent this message.Cryptography then, not only protects data from theft or alteration, but can also be used for user authentication.[4].

There are three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions. In all cases, the initial unencrypted data is referred to as *plaintext*. It is encrypted into *cipher text*, which will in turn (usually) be decrypted into usable plaintext.

Reference [5] states that there are several ways of classifying cryptographic algorithms.For purposes of this research; they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms are: *Secret Key Cryptography (SKC):* Uses a single key for both encryption and decryption *Public Key Cryptography (PKC):* Uses one key for encryption and another for decryption. *Hash Functions:* Uses a mathematical transformation to irreversibly encrypt information.

B. Use of Internal Memorandum within the University of Agriculture, Makurdi (UAM)

Memorandum comes from the Latin noun memorandum and has the same root as memorare[2].Memorare translates as to recount, to mention or call to mind. So a memo can be considered as something that should be used to remind people of something.

Memo is used by UAM staff to communicate among each other usually meant for use only within the office and are sent through the internal mail system of the organization. Memos are often used to:

- Instruct: about private information, fire, health and safety procedures, new equipment and so on.
- Remind: when staff need to remember an important time or date, such as a monthly meeting.
- Highlight: informing others of changes in staff roles, such as promotion or dismissal.

As of today, the method of sending and receiving memos within UAM has defied all the objectives that cryptography seeks to achieve, namely: Authentication, Confidentiality, Integrity, and Non-repudiation. This is because a sender typesets the memo on the computer, prints it, at times staples it and then passes it to a dispatch rider for onward delivery to the recipient. A dispatch rider could tamper with the contents of the memo, or possibly read a memo not meant for him, thus compromising integrity and confidentiality. A sample of UAM internal memo is shown in Fig 1. Motivated by these shortcomings, this research is embarked upon to develop a messaging platform where cryptography will be implemented for use by the UAM community.

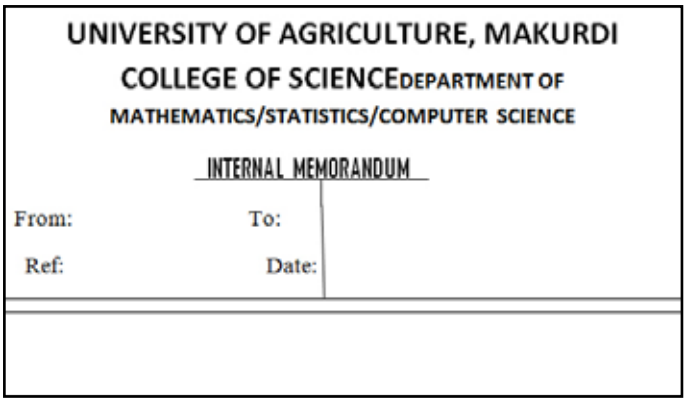
UNIVERSITY OF AGRICULTURE, MAKURDI
COLLEGE OF SCIENCEDEPARTMENT OF
MATHEMATICS/STATISTICS/COMPUTER SCIENCE
INTERNAL MEMORANDUM
From: To:
Ref: Date:

Fig.1: Sample Internal Memo for the College of Science, University of Agriculture, Makurdi

II. Methodology

In this section, we will use the Unified Modeling Language (UML) to design a memo platform such that when the sender types the memo and clicks send, the encryption algorithm is invoked and the message is automatically encrypted by the system and the encryption key is displayed on the screen. The key is a ten digit encryption key which is randomly generated using the SHA-1 Algorithm. The sender sends the key to the receiver so that the receiver will be able to decrypt the message. When the receiver logs in, a new message alert is displayed. When opening the message, he is expected to supply the encryption key to be able to read the message. This process is modeled with a UML sequence diagram in Fig 2.

The public key encryption is going to play a very vital role such as each staff UserID is automatically their public key; the unique identifier made up of the user's personal decryption key would serve as the private key.The text message when sent to the intended staff would be converted into a cipher text which will be the corresponding unintelligible alphabetic code of each individual character.

In order for this cipher text to be decrypted back into original form called the plain text, authorized staff will log into the secure interface, which we call *Mediator*, using his UserID and password. The staff must carefully input the key provided by the sender, and thenpress the *Descriptor* button which will automatically convert the cipher text into plaintext (readable text). The flowchart of the proposed system is shown in Fig 3.

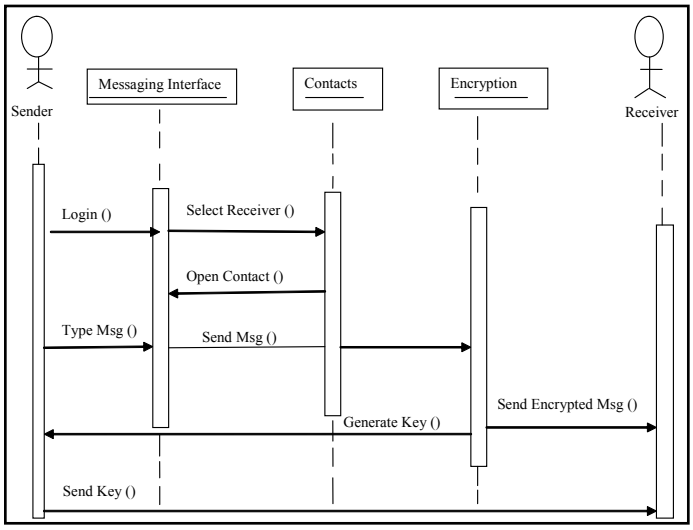

Fig. 2: Sequence Diagram for Sending Message

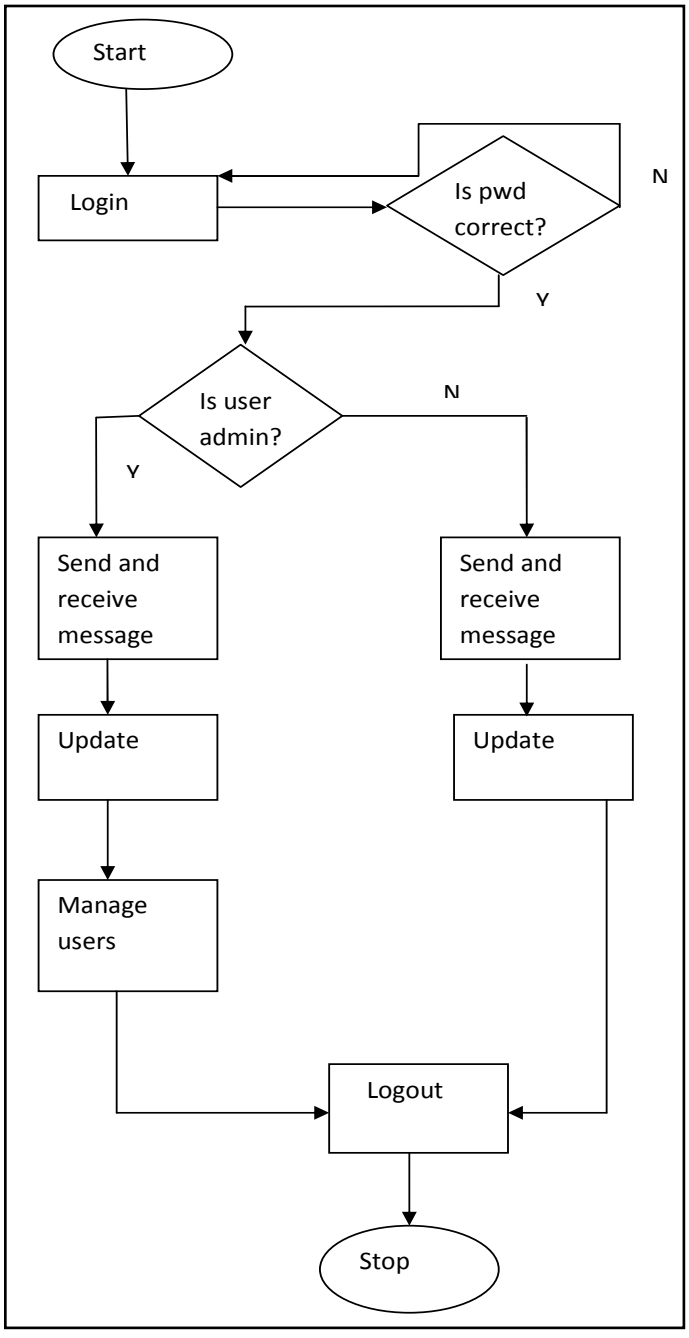

Fig 3: Flowchart of the System

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

The memo platform will consist of the *Login*, *Encrypt message, Decrypt message*, and *User management* classes as shown in Fig4.

Login: here provision for the UserID and password is made available; the password is verified from the database of the host system before been authorized to login.

Encrypt message: In this class the intended message is typed and the proposed receiver selected, when the *Send* button is clicked, the SHA-1 algorithm encrypts the memo and randomly generates a ten digit encryption key, and this encrypted message is delivered to the user in ciphertext.

Decrypt message: The user, to whom the message was sent, receives the message and enters the randomly generated key to view the message. Note that the key is not sent alongside the message but by a separate means.

User management: In this class, the administrator has the capacity to add, edit, and delete contacts and departments. He can also verify user details.

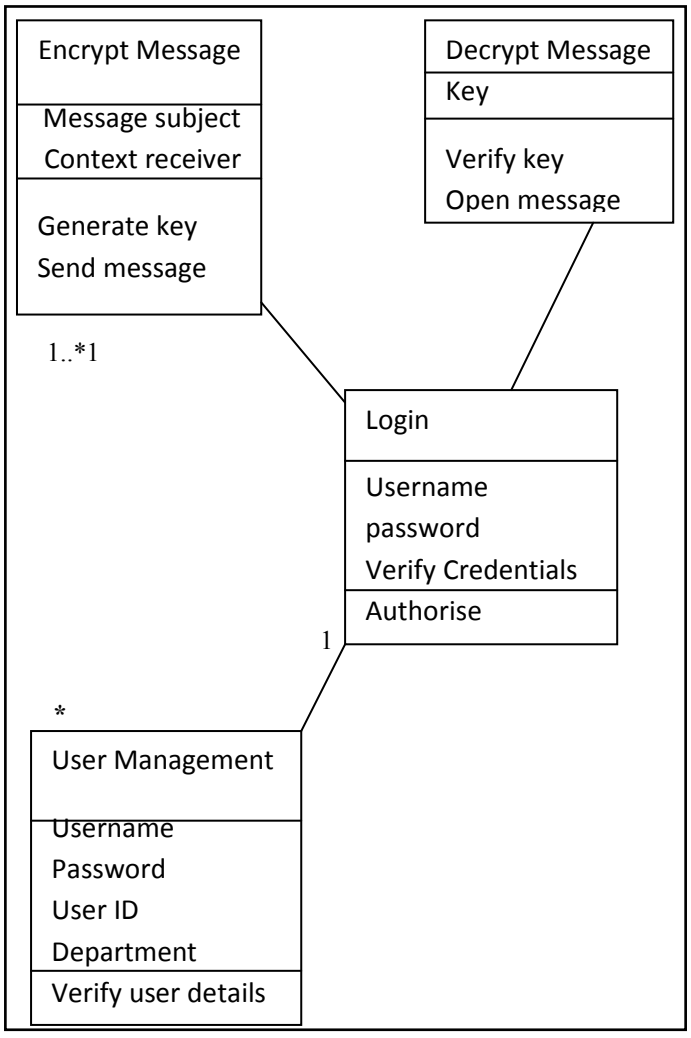

Fig 4: Class Diagram of the Proposed System

III. Results and Discussion

The memo platform and the SHA-1 algorithm were implemented using Java programming language.MYSQL Server database was used to store sent and received messages as well as staff details. The SHA-1 algorithm converts strings into binary, SHA-1 message digests in hexadecimal and in Base 64 binary to ASCII text encoding. Observe from the Received messages interface in Fig. 5 that all messages (memo) received appear in encrypted format. To decrypt a message, the staff will click the "*view message*" button beside the message and then supply the key to decrypt it. Fig6 shows a Decrypted message ready to be read.

To deploy this application for use, the following hardware and software are required: 800MHz Processor or higher, 20GB Hard Disk space or higher, 1GB RAM size or higher, Local Area Network installations within the University of Agriculture, Makurdi, Windows XP operating system or higher versions, MYSQL Server database, any Browser (Mozilla Firefox, Internet Explorer, Google Chrome, etc). These are minimum requirements; higher specifications will enhance better functionality.

In the course of the program implementation, the program was well tested and documented to ensure a robust application is put forward with minimal errors. We inserted test data, ran the program severally and fixed any errors found. Documentation was achieved right from the design stage with the use of UML tools and flow charts. Comments were inserted at the beginning of each procedure for clarity and future reference. A user manual was also designed to serve as a guide for first time users of the memo application.

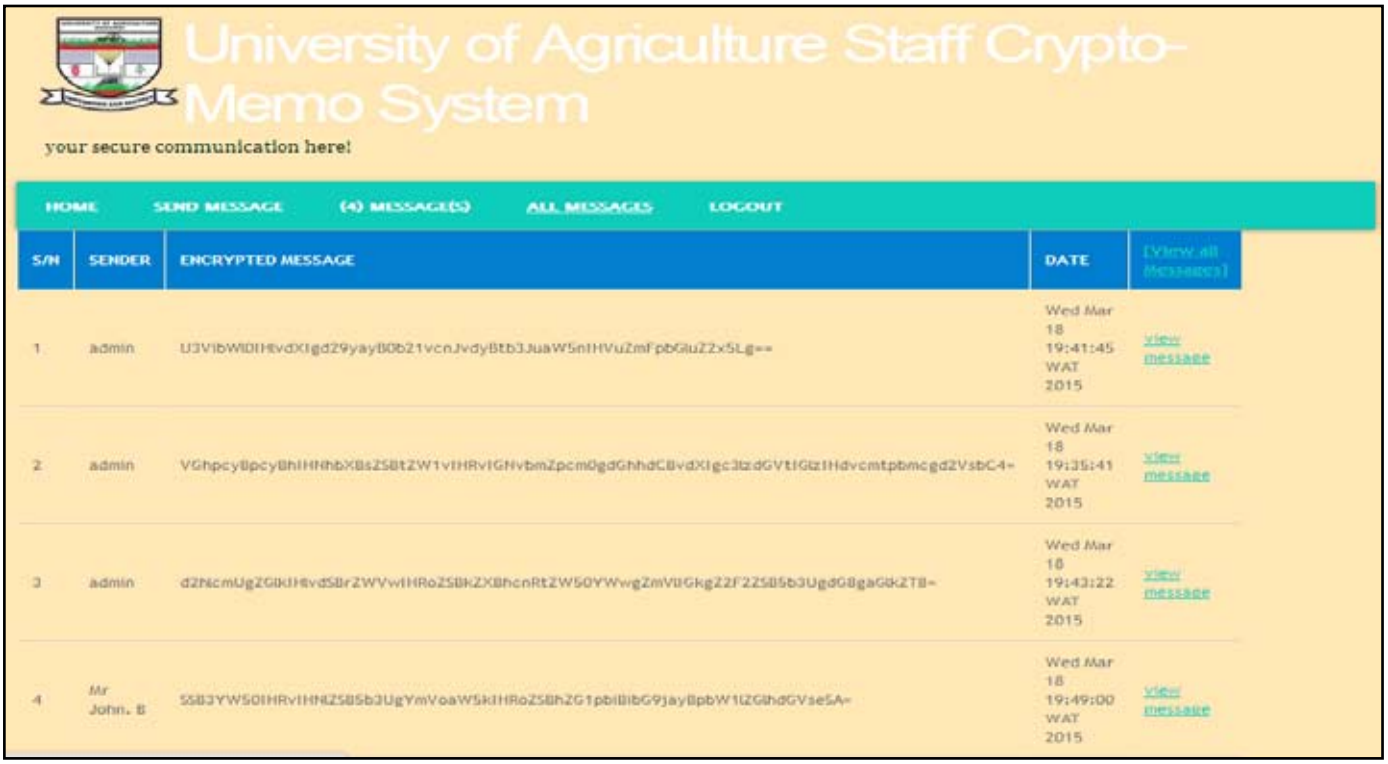

Fig. 5: Received messages Interface

Fig. 6: Decrypted Message Interface

IV. Conclusion

Having considered the manual system of sending memo between staff within the University of Agriculture Makurdi which is inefficient, insecure and unreliable, this research was embarked upon in order to implement a cryptographic system for a secured internal memo platform using the SHA-1 algorithm. This is to ensure that a secure communication between two parties even in the midst of malicious users (intruders) is guaranteed. It was developed using the Java Programming Language and MYSQL Server Database. The cryptographic system was tested and found to be efficient and quick in message transfer.

The manual approach to sending and receiving memos within the university no doubt poses a lot of problems, some of which are in-effective storage and management of information, late delivery of information and lack of confidentiality among others. Organizations that have implemented an effective cryptographic system no longer face these challenges, or if they do at all will be at a very minimal level. No doubt, an electronic memo system implemented with cryptography is far more effective, economical, and secured than the primitive manual method.

We recommend that further research should be conducted to identify a better way of transmitting the decryption key to the receiver. In this research, attention is not given to the issue of how the key will be transmitted.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

References

[1] *Barr, T.H. (2002). Invitation to Cryptology. Upper Saddle River, NJ: Prentice Hall. Retrieved from: <http:// www. en.Wikibook.org/Wiki/Cryptography/Introduction> on "15th of March 2015".*

[2] *Diana, N. (2004). Helping you Gain Control of your Career. McGraw-hills. U.S.A.*

[3] *Directorate of ICT, UAM Nigeria (2015). University'sHistory. Retrieved from: <http://uam.edu.ng/About- us/History> on "17th of March, 2015".*

[4] *Jordan, E. (2011). Secrets of the New Cryptology. New York: Macmillan.*

[5] *Gray, J.O. (2011). Cryptography and Number Theory for Digital Cash.Retrievedfrom: <http://www.swiss.ai.mit. edu/6.805/articles/money/cryptnum.htm> on "15th of February, 2015".*