Journal of the Nigerian Association of Mathematical Physics
Volume34,(*March, 2016*), pp 213 – 218

The Strength of an Encryption Security System is Determined by the Complexity of the Key

[1]Ihama E.I, [2]Egbon C.C and [2]Aduhor G.E.

[1]Department of Computer Science and Information Technology, School of Applied Sciences, Edo State Institute of Technology and Management, Usen, Benin City,
[2]Department of Computer Science, Delta State College of Physical Education, Mosogar,Nigeria.

Abstract

The internet is a fast growing area of ICT and its usage is massively increasing every day. Electronic data, and e-commerce, due to their open nature has made individuals and organizations prone to malicious attack, making organizations to lose revenue, data integrity and customer trust, due to improvement in the nature of attacks on information systems. In this research work, we show that the complexity of an encryption system determines how strong the system will be, using a complex Key(N-key) in computer security techniques, with special reference to cryptography, using hashing techniques and using acomplex key(N key) encryption and decryption system. Software design was implemented using Visual BASIC programming language.

Key words: Encryption, Decryption, Cryptography, Cyphertext, Plaintext

1.0 Introduction

Cryptography is the science of writing in secret code and using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

People have been working on computer security for the past 37 years. During this time there have been many intellectual successes. Notable among them are the access control list [1], public key cryptography [2], and cryptographic protocols [3]. In spite of these successes, it seems fair to say that in an absolute sense, the security of the hundreds of millions of deployed computer systems is terrible.

A determined and competent attacker could destroy most of the information on almost any of these systems, or steal it from any system that is connected to a network. Even worse, the attacker could do this to millions of systems at once. The underlying working principles and the design of a computer security software using cryptography techniques is what this research provides.

Cryptography found its way into the commercial arena when, on December, 1980, the same algorithm, DES, was adopted by the American National Standards Institute (ANSI). According to levy [4], following this milestone, Data Encryption Standards, another new concept,was proposed to develop Public Key Cryptography (PKC). It is still undergoing research development today [4].

Bohli et al [5] conducted a study that examined popular proof models for group key establishment and the tools offered for analyzing group key establishment protocols in the presence of malicious participants. With respect to wireless security a means of improving security of the code division multiple access (CDMA), one of the most widely used wireless air link interfaces in 3G wireless communication, was proposed by Tafaroji and Falahati [6]. This was done by applying an encryption algorithm over the spreading codes. The authors carefully studied the cross-correlation between outputs of encryption algorithm causing multi-user interference due to the fact that multi-user detection is the inherent characteristic of CDMA. A combination of encrypted and unencrypted M-sequence is used as the spreading code to mitigate system performance. Thus the authors proposed a new method named “hidden direct sequence” to enhance the security of CDMA systems through the application of the cryptographic algorithm in the channelization code. This secure spectrum-spreading

Corresponding author: Ihama E.I., E-mail:eyoski@yahoo.com, Tel.: +2347039404855

method prevents eavesdroppers from hearing an intercepted message, and further prevents them from attempting to decipher the communication using the most powerful means.

With respect to chosen ciphertext attacks (CCA), Boneh et al [7], proposed a CCA-secure public-key encryption scheme based on identity-based encryption (IBE). These schemes provide for a new paradigm for achieving CCA-security, which avoids "proofs of well-formedness" that was the basis for previous constructions. Furthermore, by instantiating their constructions using known IBE constructions, Boneh et al [7] was able to obtain CCA-secure public-key encryption schemes whose performance was competitive with other CCA-secure schemes already in existence.

In a study carried out by Walters [8], he proposed a draft in information security(IS), security curriculum that should be incorporated into the core body of knowledge of the business curriculum, and proposes that additional practical guidance to Accounting Information Security (AIS) educators who would like to incorporate IS security into their existing curriculum needs to be undertaken.

Zanin et al [9], in their study presented a new distributed signature protocol based on the RSA cryptographic algorithm, which is suitable for large-scale ad-hoc networks. This signature protocol is shown to be distributed, adaptive, and robust while remaining subject to tight security and architectural constraints. The study further reveals that the robustness of this protocol scheme can be enhanced by involving only a fraction of the nodes on the network. The authors demonstrated that their protocol scheme is correct, because it allows a chosen number of nodes to produce a valid cryptographic signature; it is secure, because an attacker who compromises fewer than the given number of nodes is unable to disrupt the service or produce a bogus signature; and it is efficient, because of the low overhead in comparison to the number of features provided.

Recent work by Albertini et al. [10] show how to choose constants for a modi_ed version of SHA-1enabling a saboteur to help an attacker later and collisions of a certain form.

Hogue et al [11] discussed means of strengthening data encryption and authentication in cryptosystems on corporate networks. Also discussed and presented in the study is the feasibility of generating biometric key encryption. Experimental analysis of this study revealed encouraging prospects for its use in modern cryptosystems.

Bellare, Paterson, and Rogaway [12] explore SETUP attacks for case of symmetric encryption, and rebrand SETUP attacks as algorithmic substitution attacks (ASAs). They give SETUP attacks against symmetric encryption, but also seek countermeasures, in particular arguing that a symmetric encryption scheme is secure against sabotage if no attacker, even given a secret trapdoor, can distinguish between ciphertexts generated by the trusted reference algorithm versus ones generated by a backdoored version of it. They argue that deterministic, stateful schemes can be shown to meet this latter notion. However, it is important to note that this result is only meaningful if the algorithm underlying the reference implementation is assumed to be free of backdoors, More generally, the SETUP and ASA frameworks do not capture all relevant aspects of a cryptographic weakness, nor potential routes for a saboteur to achieve one.

In a study carried out by Schneier et al [13], the researchers concluded that the argument that secrecy is good for security is a myth and worthy of rebuttal. They further demonstrated that secrecy is especially not good for security with respect to vulnerability and reliability of information. They also show that security that relies totally on secrecy is extremely fragile, and once it is lost, there is no way to regain it. Schneier et al [13], goes on to make a case that cryptography, since it is based on secret keys that are short, easy to transfer, and easy to change, must rely on one of its basic principles that the cryptographic algorithm be made public if it is to remain strong and offer good security. This research work provides computer security techniques with special reference to cryptography, using the hashing techniques and using an N key encryption and decryption system, the software design was implemented using Visual BASIC programming language. The major advantage of this system is its ability to hide the information being transmitted from unauthorized user, by preventing the unauthorized user from gaining access to the information that is transmitted through insecure network (like the internet) or while in storage, except the intended recipient.

2.0 The Encryption Process

The diagram below shows the basic cryptographic process. Plaintext P is encrypted with an encryption algorithm and an encryption key K. The resulting ciphertext, C, is transmitted over the network. The receiver decrypts the ciphertext with a decryption algorithm and a decryption key H. The encryption and decryption algorithms are public information. However, at least one of the keys (K and H) are private information. The keys consist of a relatively short string of bytes (e.g., 128 bits). The longer the key, the more difficult to break the cipher, b.

Fig. 1: The Encryption Process.

Most existing cryptography softwares are Internet-based systems. That is they are applicable or useful in the protection of Internet files or systems within a network. This is not too appropriate because intruders do not only attacked or intrude into system within a network or Internet files but also attacked standalone systems and files in this standalone system.
In this paper, we carryout an analysis of existing cryptography softwares with a view to bringing out their weaknesses and benefits and we developed a cryptography system that will help to improve on the features of existing cryptography software while in storage and when transmitted across an unsecured network like the internet.

3.0 The Design Approach of the Cryptographic System

The system uses an N-Key (complex key) cryptography encryption systems, by protecting systems information, using hashing techniques, by preventing intruders from using the system by interchanging its multi-keys and it becomes more complex and more difficult to hack, thereby preventing an unauthorized users or intruders from gaining access to information systems,and will also provide protective facilities for standalone systems, or while being transmitted across an unsecured network like the internet.
Hash functions, also called message digests and one-way encryption, are algorithms that, in some sense, use no key, Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents, often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file.
The key in public-key encryption is based on a hash value. This is a value that is computed from a base input number using a hashing algorithm. Essentially, the hash value is a summary of the original value. The important thing about a hash value is that it is nearly impossible to derive the original input number without knowing the data used to create the hash value.

Table 1: Hashing Process

Input number	**Hashing algorithm**	**Hash value**
10,667	**Input # x 143**	**1,525,381**

From Table 1, one can see how hard it would be to determine that the value 1,525,381 came from the multiplication of 10,667 and 143 from table 1 above. But if you knew that the multiplier was 143, then it would be very easy to calculate the value 10,667. Public-key encryption is actually much more complex than this example, but that's the basic idea.
The important thing about a hash value is that it is nearly impossible to derive the original input number without knowing the data used to create the hash value. In order to ensure that encrypted information are not easily decrypted by cryptanalyst, the proposed system will use a complex key system, which will also show how difficult it is to determine the key,which makes the system quite unique.
The system will be user friendly. It will be designed with features, which provides users with input screen such that a user can enter his/her access code to login to the system. The system generally will provide the following facilities:

i.) Provide facilities for storing user information;
ii.) Provide facilities for encrypting user information using N key system of 64-bits each.
iii.) Provide facilities for keeping store of information being encrypted within the system for future reference.
iv.) Provide facilities for protecting information from unauthorized or accidental discloser while the information is in transit (either electronically or physically) and while information is in storage.

The system architecture is given below in Fig2

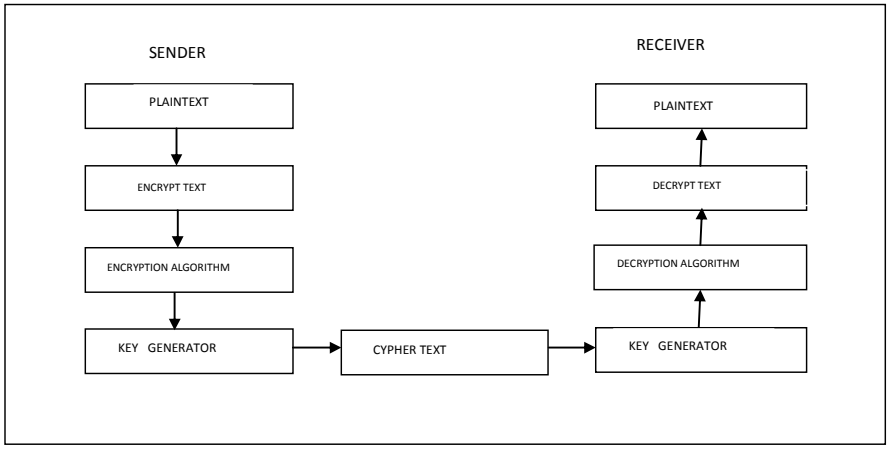

Fig. 2: The N-Key Based Cryptography System Architecture

The architecture in Fig2 ensures that a sender uses an encryption system to encrypt his or her message. This is done by supplying a (complex) N key/s, each key with a maximum of eleven characters, of 128bits, but if the encryption system is just a single key, an intruder or a hacker, can easily guess and get the key, after a number of triers. The single key can easily be hacked, since the key is just a single stream of key, but if the encryption system is a complex key process it becomes very difficult for an authorize user, as the intruder cannot easily guess and obtain this complex key. The message has been rendered into an unreadable form known as cipher text. The receiver at the other end might not get this cipher text if the encryption key is not an N-key (complex key), in the case of a single key. But when the receiver send his or her keys to the decryption system so that the cipher text can be transformed back to an understandable format. The screen shots of how the encryption and decryption are achieved through cryptographic process are shown inFig3, Fig4 and Fig5.

4.0 Conclusion

This research work shows that the more complex an encryption security system is, the more difficult it will be to di-cypher the encryption key compared to a single key system, it also show how strong the system will be for hackers or intruders to gain access to the system. The major advantage of this system is its ability to hide the information being transmitted from unauthorized user, by preventing the unauthorized user from gaining access to the information that is transmitted through insecure network (like the internet) or while in storage, except the intended recipient. This system will ensure that intruders into computers systems files and computer users involve in carrying out malicious acts on the system being used are prevented from further use of the system. Once used according to specification with the authentication checks in place, the system will no doubt provide security facilities for system users. The issue of being scared of loosing ones important files or information will be a thing of the past and also the problem of such threats from users will be drastically reduced since any attempts made by them will always be prevented.

5.0 Software Application

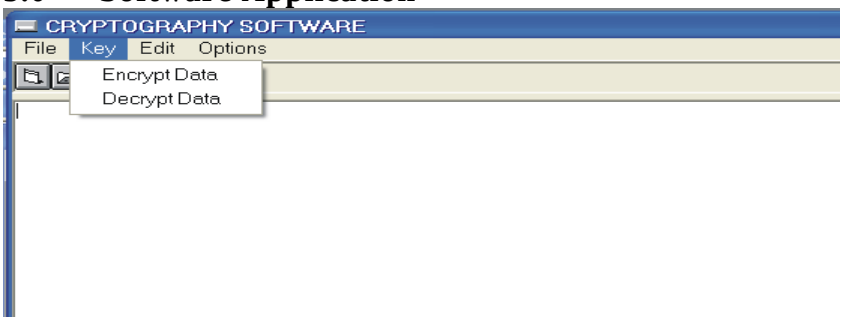

Fig.3: Sample Screen Design Showing The Multi-Decryption Keys To Decrypt The Encrypted Data

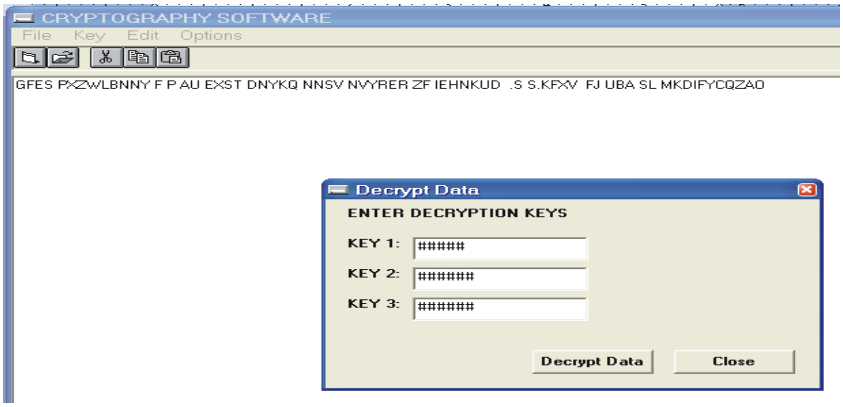

Fig.4: Sample Output Data Of The Encrypted Data

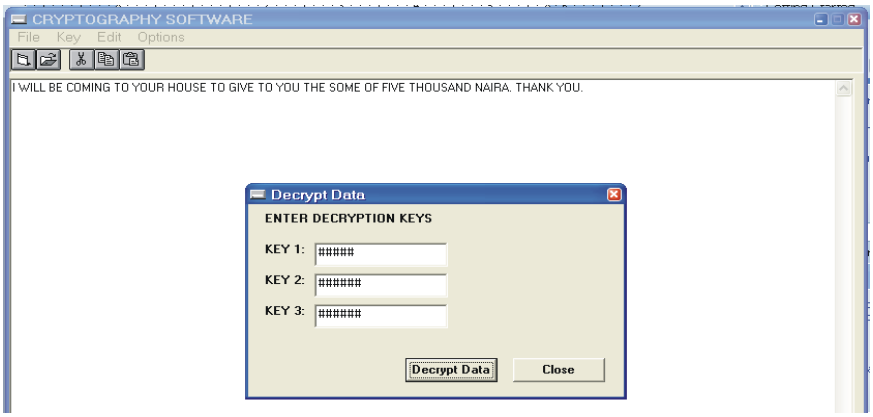

Fig. 5: Sample Output Data of the Decrypted Data

6.0 References

[1.] Saltzer, N. (1974). Overview of Computer Security Access Control List. ACM Trans. Computer Security Systems, 8(3): 324-353.

[2.] Rivest, H. (1978). Introduction to Public Key Cryptography, In Proceedings of the ACMSIGMOD Conference on Computer Security Management, 160-172.

[3.] Abadi, H. (1996). Cryptography Protocols, In Proceedings of the Conference on Computer Security Basis, 493-504.

[4.] Levy, S. (2008). Crypto: How the Code Rebels Beat the Government - Saving Privacy in the Digital Age. New York: Viking Penguin Publishing.

[5.] Bohli, J., González Vasco, M., and Steinwandt, R. (2007). Secure Group Key Establishment Revisited. *International Journal of Information Security*, 6(4), 243-254.

[6.] Tafaroji, M., and Falahati, A. (2007). Improving Code Division Multiple Access Security by Applying Encryption Methods Over the Spreading Codes. *IET Communications*, 1(3), 398-404.

[7.] Boneh, D., Canetti, R., Halevi, S., and Katz, J. (2006). Chosen-Ciphertext Security from Identity-Based Encryption. *SIAM Journal on Computing*, 36(5), 1301-1328.

[8.] Walters, L. (2007). A Draft of an Information Systems Security and Control Course. *Journal of Information Systems*, 21(1), 123-148.

[9.] Zanin, G., Di Pietro, R., and Mancini, L. (2007). Robust RSA distributed signatures for large-scale long-lived ad hoc networks. *Journal of Computer Security*, 15(1), 171-196.

[10.] A. Albertini, J. P. Aumasson, M. Eichlseder, F. Mendel, and M. Schl a_er. Malicious Hashing: EvesVariant of SHA-1. In Selected Areas in Cryptography(SAC, 2014).

[11.] Hoque, S., Fairhurst, M., Howells, G., and Deravi, F. (2005). Feasibility of generating Biometric Encryption Keys. Electronics Letters, 41(6), 1-2.

[12.] Mihir Bellare, Kenneth G Paterson, and Phillip Rogaway. Security of symmetric encryption againstmass surveillance. In Advances in Cryptology(CRYPTO, pages 1)19. Springer, 2014.

[13.] Schneier, B. (2004). The Non-security of Secrecy. Communications of the ACM, 47(10), 120-120.