Asian Journal of Scientific Research

ISSN 1992-1454

science alert
http://www.scialert.net

ANSInet
an open access publisher
http://ansinet.com

Asian Journal of Scientific Research 6 (4): 632-649, 2013
ISSN 1992-1454 / DOI: 10.3923/ajsr.2013.632.649

Securing m-Government Transmission Based on Symmetric and Asymmetric Algorithms: A Review

[1]M.A.Watari, [2,3,4]A.A.Zaidan and [2,3,4]B.B.Zaidan

[1]Department of Systems and Networking, College of Information Technology, University Tenaga Nasional (UNITEN), Selangor, Malaysia

[2]Network and Communication Security Research Group, ICT and Computational Science Research Cluster, University of Malaya, 50603 Kuala Lumpur, Malaysia

[3]Faculty of Engineering, Multimedia University, Jalan Multimedia, Cyberjaya, 63100 Selangor Darul Ehsan, Malaysia

[4]Predictive Intelligence Research Cluster, Office of Research and Higher Degrees, Sunway University, No 5, Jalan University, Bandar Sunway, 46150 Petaling Jaya, Selangor, Malaysia

Corresponding Author: M.A.Watari, Department of Systems and Networking, College of Information Technology, University Tenaga Nasional (UNITEN), Selangor, Malaysia

ABSTRACT

Several changes have taken place in the field of communication technologies (ICT) in recent years, specifically in the era of rapid technology development. Mobile technologies, especially smart phones, have replaced computers in various significant tasks. This development influenced the interactions between citizens and government agencies in m-Government. m-Government is an extension of e-Government, which provides services to citizens in general or to subscribers in particular. These services range from public to private bodies and the data transmitted sometimes require authentication and confidentiality. Thus, the need for data security is inevitable. This study will discuss the security of m-Government using security algorithms and report some literature work in this field to highlight its weaknesses.

Key words: M-Government, symmetric algorithm, asymmetric algorithm

INTRODUCTION

Establishing communication or becoming the "middle-medium' between different government agencies and citizens has become indispensable in this century. This situation can be observed in the last century before the invention of mobile and wireless networks. The rapid development of technology and communication infrastructure that forces human affairs and businesses to adopt and deal with the development as the core aspect of processes in terms of business, communication, information and technology (Hmood *et al*., 2010). The m-Government (Mobile Government) can be considered as an opportunity in the transformational government strategy. SMS (short message service) can act as one of the avenues through which m-Government transactions can be conducted. Dealing with such topic indicates the several dimensions involved, which is becoming more complicated due to the increasing number of important issues that should be considered, including privacy, authentication and confidentiality. Important demands of these services must be considered to meet the needs of clients or citizens. To achieve this, several security algorithms

have been implemented to satisfy these needs. Requirements are dictated in specific security systems. Some have been used as powerful tools for encryption and some have been broken or even anticipated to be broken soon.

MOBILE GOVERNMENT (M-GOVERNMENT)

To avoid the overlap between e-Government and m-government, it is important to show the distinction between the two. E-Government refers to the government's use of information technology to send and receive information and provide services to citizens. In other words, e-Government refers to the use of wired Internet technology in public organizations to provide better services efficiently (OECD-ITU, 2011). At present, mobile technology have enabled governments to improve their capacity to provide benefits and deliver outcomes to citizens and businesses, as well as to create a positive impact on the national economic growth. Developing countries will significantly benefit this development because they have been historically restricted by poor or non-existent communication infrastructure that, which in turn has stunted their economic development and social improvements. However, m-Government will also provide countries with more developed e-Governments and the opportunity to tackle a number of issues. These issues are related to the digital-divide, which remains a critical factor in the levels of services delivered by e-Government (OECD-ITU, 2011). M-Government can also be regarded as a strategy that employs wireless and mobile technologies, applications and devices towards enhancing the quality of service delivery to all e-Government key players including citizens, business organizations and a variety of government departments (Abramowicz *et al*., 2005).

The most prominent strength of m-Government services is ubiquity, a concept used to describe the provision of information and services at whichever place and time. This feature upholds the idea of personalization, ease of use, time and cost saving and services based on various locations. Several countries have become strong advocates of m-Government services, such as the USA, the UK, Singapore, Malaysia and Australia. In an e-Government transaction, the involved parties are securely authenticated and any transmitted information is treated with confidentiality and integrity. These security requirements have been emphasized and made more significant with the emergence of m-Government because the wireless interfaces have verified security deficiency if drawn in comparison with their wired counterparts. Additionally, the ever-increasing storage and processing capabilities of mobile devices have seized the attention of malevolent programmers and hackers all over the world (OECD-ITU, 2011).

In general, four major models of m-Government have emerged, namely, government-to-citizens (G2C), government-to-government (G2G), government-to-business (G2B) and government-to-employees (G2E). Mobile applications and services largely constitute government-to-citizens (G2C) services. Nonetheless, G2G, G2B and G2E m-government services are also established. This study concentrates on government-to-citizens (G2C) services as a core approach. Whether or not these services are interactive (e.g., alert messages), educational (e.g., grades, admissions, exam results), or transactional (e.g., bank account info), they must be secured against different types of attacks and breaching (OECD-ITU, 2011; Bellovin, 1989).

Ensuring the safety of information and data transfer between government mobile agents and users is important. Issues pertinent to this process consist of methods of first-degree security of the medium of transfer, the applicability of cryptosystem algorithms in protecting data transmission, issues with regards of speed, power and time duration that have persisted before the attackers have come up with ways to break the encryption of a particular algorithms. Mukherjee and Biswas (2005) developed a framework of implementation for government services to different parties,

namely, citizens, businesses and governments. This implementation framework embodies two guidelines. That is, the network architecture for m-Government and the implementation methodology for its services to a variety of parties, particularly the citizens. El Kiki and Lawrence (2006) initiated a tailored model for real-time, ever-present mobile government, modified from the phases of growth model and the five stages framework. The purpose of this model is to place emphasis on the fast-paced expansion and uptake of wireless technology. In (Brucher and Baumberger, 2003) explained the role of mobile technology in processes of democracy and outlined the legal constraints, technical and political requirements. In specific, they have also provided evidence of the fact that mobile devices can contribute to the deterioration of the flaw of the democratic process made available by non -mobile gadgets. Yun and Chen (2000) broached a new data into the mining capability of mobile commerce environment. To mirror the patterns of customer usage in the particular environment, they suggested a novel mining model, known as the mining mobile sequential patterns, which pays attention to both customer movement and purchase patterns. M-government services have its appeal to law enforcements, firefighting emergency medical services, education, sport, financial, health and transportation (Zalesak, 2003).

INFORMATION SECURITY

Before the advent of technology, information security was a primitive procedure for physical objects and other classified documents, as the primary threats were physical theft of devices and espionage on system products (Naji *et al*., 2011). Exploration of the history of information security reveals that several attempts have been made to secure messages. For example, ancient Mesopotamians wrote a private message in cuneiform script on a fresh clay tablet, which was exposed to the sun to dry. This tablet was then enclosed in a clay envelope on which the addressee's name was written (Kartalopoulos, 2009). Bellow, Fig. 1 gives idea on how simple authentication used to be carried out (German, 2012).

Fig. 1: Clay tablets enclosed in clay envelopes assures the secrecy and authenticity of the message (German, 2012)

A sound summarization of the foundation of computer security at the end of the 1960s (Ware, 1998). Information security is the procedure of protecting information and information systems from unauthorized access, disruption, disclosure, destruction or modification (Kissel, 2011). The origin of this term comes from the terms commonly used in computer security and information assurance. These terms are used interchangeably in the field of security, which indicates its interrelation. Moreover, these terms share the target of protecting the confidentiality, availability and integrity of information. However, subtle differences exist between them. Differences among those subjects can be seen in terms of the focus and strategies employed to protect data and information. Information security focuses on protecting and securing the content of the information using various tools and tactics. This process is also concerned with the security of application and infrastructure. Information assurance focuses on managing the risk and the processes of storage and transmission of data. Notably, information security and information assurance emerged from the concept of computer security as the foundation of security field. Computer security focuses on protecting the system infrastructure and ensuring the safety of the system with less concern about the processes or the data being stored (Feruza and Kim, 2007). Information security regulations is concerned with securing the target information from any illegal access, or providing concession for the system from unauthorized log-in (Stevens, 2010). The policy of data infringement comprises of subjects linked to situations of external, internal, handling and reports of information infringement (Harris, 1997).

CONFIDENTIALITY

The Merriam Webster dictionary defines confidential as "containing information whose unauthorized disclosure could be prejudicial to the national interest." The term also means keeping information away from disclosure and providing methods of protecting information and personal privacy in a secure manner. Confidentiality prohibits unauthorized access or disclosure of private information, either by a person or a system. Assessing, using, copying, or disclosing confidential information should only be conducted by an authorized guide and only when there is an actual need (Pappas, 2008; Zaidan *et al*., 2011).

Confidentiality is breached when information system or confidential information is accessed or might be accessed, copied, used, or disclosed by any unauthorized person for certain information (Pal, 2008). This is applicable when writing confidential information on a piece of paper and someone is looking. This situation qualifies as abuse of privacy if the person is not allowed to look, l*et al*one read the information. Another example of abuse of privacy is the disclosure of confidential data over the telephone when the caller is not authorized to obtain that information (Feruza and Kim, 2007).

AUTHENTICATION

The authentication service ensures that the communication is authentic. The primary aim of this process is to keep information genuine and original. Information is usually stored in the form of paper documents, videos, or digital CDs. The task of an authentication service is to ensure that documents are not faked or fabricated (Lhotska and Aubrecht, 2008). In information security, e-Business and computing, it is important to ensure the authentication of data communication, transaction or documents (physical or electronic). The term "authentication" also includes the authenticity of the sender, receiver, or all parties connected with the information communication processes (Feruza and Kim, 2007; Lhotska and Aubrecht, 2008). In common occurrences, the authentication process works well in validating the information source and running a check on its originality. This process is materialized by cryptographic checksums known as authentication code,

which is computed with a reference made to an endorsed cryptographic algorithm. The other name for authentication code is message authentication code. Alternatively, a message authentication code is a one-way hash function, wherein the calculation is derived from a message and a secret key. The strength of the code lies in the secret key. Forging this code is almost impossible if the secret key is not known or revealed (Kartalopoulos, 2009).

Recognizing the value of information and expected attacks from these unauthorized parties and then defining the correct procedures and guarding the requirements for the information are the most important parts of information security. Information security is classified at varying levels. Some information requires higher level of protection such as top secret information. This type of information needs highly secure software systems with different levels of security. In responding to guarding information, the authentication between different parties must be established and well-defined. Two specific authentication services are defined in X.800 (security recommendation):

- Peer entity authentication helps in the identity validation of a peer entity in an association. Two entities shall be perceived as peers if they enforce the same protocol in varying systems, e.g., two TCP modules in two communicating systems. Peer entity authentication would be applied on the phase where data will be transferred in a connection. This method assures that a mock-up entity or a prohibited replay of a connection made earlier does not exist
- Data origin authentication contributes to the justification of the data unit source. The method does not offer any protection against replicated or altered data units. This kind of service would be used compatibly in applications like electronic mail, where there are no previous interactions taking place between the communicating entities (Stallings, 1995)

CRYPTOGRAPHY

Cryptography is the science securing messages (Zaidan *et al.*, 2010d). The encryption system does not differentiate between authorized and unauthorized users if both parties provide the same decryption key (Zaidan *et al.*, 2010e; Salem *et al.*, 2011). Therefore, encryption on its own will not provide security. Encryption and decryption must be governed by a proper process (Nabi *et al.*, 2010). Accurate data on the cost of failures in the security of the information infrastructure are not available because the victims rarely publicize security compromises. This situation is attributed to fear of embarrassment and incurring punitive damages for inadequate protection of private information or loss of business (Pathan *et al.*, 2006; Zaidan *et al.*, 2010a, b). The bellow Fig. 2 explains about cryptography and its types.

A cryptosystem supplies the encryption and decryption and it can be created in hardware components or program codes available in an application. The cryptosystem manipulates an encryption algorithm, which ascertains the simplicity or complexity of a process. The majority of algorithms are naturally complex mathematical formulas, which take up a certain sequence to the plaintext. Most encryption methods are equipped with a secret value known as a key (usually a long string of bits), which works with the algorithm in text encryption and decryption (Patil and Shaligram, 2010). In light of the algorithms that have fulfilled the purpose of encryption, cryptography employs either one key for encryption and decryption or two keys for both purposes.

In this study, cryptography is mostly concerned with security algorithms and its built system in terms of encryption and decryption performance. A comparative study among different cryptographic algorithms (symmetric and asymmetric) must be conducted to choose the appropriate algorithms to secure the transfer medium in m-Government. Different algorithms provide different levels of security depending on its robustness. Different criteria are used to determine the risk of

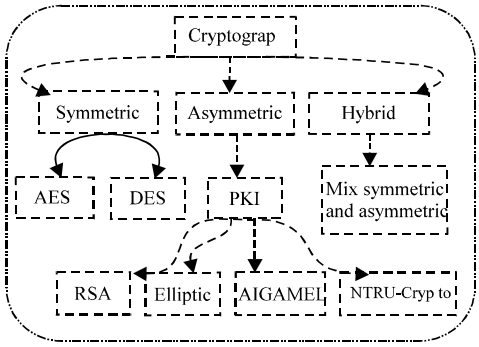

Fig. 2: Cryptography types and classification of security algorithms

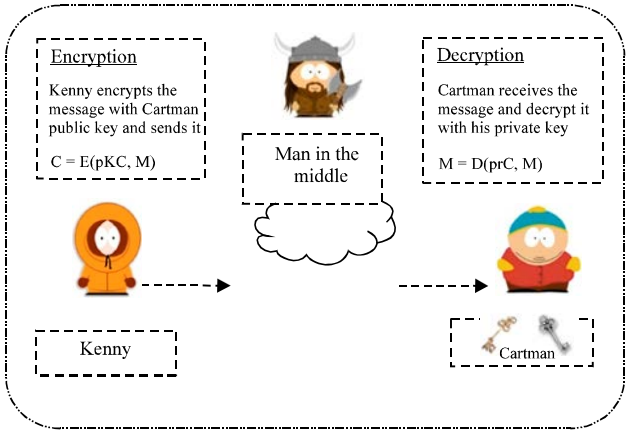

Fig. 3: Messages transmission (encryption and decryption)

breaking cryptographic algorithms. For example, if the time required to break an algorithm is longer than the time needed to keep the encrypted data secret, then the algorithm is seen to be secure. Figure 3 illustrate the mechanism of altering messages between the communicating parties.

SYMMETRIC CRYPTOGRAPHY ALGORITHMS

The secret key, which is a single key that is used to encrypt and decrypt texts, should be first defined before defining the symmetric cryptography algorithm (Abomhara *et al*., 2010a). This process is also known as secret-key cryptography. Symmetric algorithms, which can also be labeled as conventional algorithms, are algorithms, wherein the encryption key can be computed from the decryption key and works the opposite way. The encryption key and the decryption key in several symmetric algorithms do not show any difference. These algorithms, which are also called secret-key algorithms, single key algorithms, or one-key algorithms, are pre-conditioned that the sender and receiver would come to a mutual decision on a key before communication can safely take place. The protection offered by a symmetric algorithm is vested within the key. Exposing the key would imply that anyone can encrypt and decrypt countless number of messages. Provided that the communication should stay discreet, it is imperative that the key must also remain as such (Schneier, 1996).

To exemplify this further, if Dan intends to talk to Norm as an introduction, Dan has to find ways on how to provide Norm with the correct key. He is aware that sending the key in an e-mail

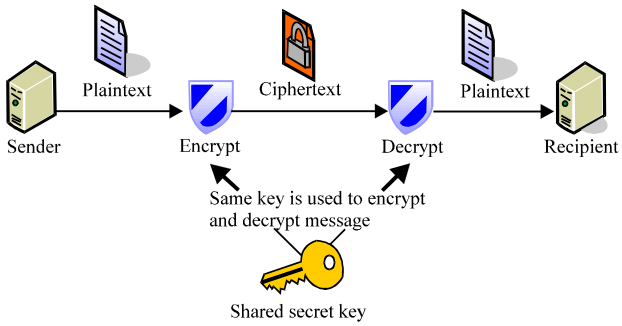

Fig. 4: Symmetric encryption and decryption (Microsoft Corporation, 2005)

message would be risky because the key is far from safe and it can be easily intervened and manipulated by roaming attackers. Dan realizes that he has to deliver the key to Norm through an external method. Dan thinks that he can save the key on a floppy disc and saunter off to Norm's desk, send it to him through the normal, slow mail, or have a dependable carrier send it to Norm. This method is inconvenient and vulnerable to danger as both users would make use of the same key to encrypt and decrypt. The mechanism of exchanging secret key is shown in Fig. 4 (Microsoft Corporation, 2005).

In this situation, the symmetric cryptography suffers from some drawbacks. For example, the process of exchanging the secret key requires high level of trust as the process of choosing, delivering and storing the secret key in a secure and dependent manner is not easy. Symmetric key encryption also lacks authentication service. In other words, the recipient can neither authenticate the sender nor verify that the decrypted message is the same as the original message (Yadav, 2010).

Several algorithms have been deployed for the purpose of securing wireless networks. In this section, the researcher compares the DES (Data Encryption Standard), 3DES (triple Data Encryption Standard) and AES (Advanced Encryption Standard). By drawing this comparison, the analysis of this comparative study will decide on the best algorithm among the three algorithms.

The level of security of an encryption algorithm is calculated by the key space size (Brucher and Baumberger, 2003). The larger the key space, the more time the attacker needs to search the key space extensively, which would lead to higher security level. The key in encryption denotes the piece of information (value that comprises a large sequence of random bits), which specifically outlines the specific transformation from the plaintext to ciphertext, or vice versa during decryption. Encryption key shows its dependency on the key space, which is the range of the values that can be manipulated to put a key together. The larger the key space, the more possible keys can be built (e.g., today it is commonplace to use key sizes of 128, 192 or 256 bit. Thus, key size of 256 would bring a 2256 key space) (Naji *et al*., 2009a).

Cryptosystem utilizes an encryption algorithm that discerns the level of simplicity or complexity of the encryption process, the indispensable software component and the key (normally a long string of bits), which collaborate with the algorithm towards encrypting and decrypting the data (Naji *et al*., 2009b).

Data encryption standard (DES): DES is a cipher, an approach adopted to encrypt information. This code was favored to be the official Federal Information Processing Standard (FIPS) for the

United States in 1976 and has been used in international domains. The algorithm started off with a spark of controversy, but equipped with some confidential elements of design, a short key length and the rising distrust over a National Security Agency (NSA) backdoor. In effect, the DES had been placed under extreme academic enquiry and it further boosted the modern understanding regarding block ciphers and their cryptanalysis. DES is currently considered unprotected for various applications, which is best explained by the 56-bit key size, which is too small, which allows DES keys to be breached in less than 24 h.

Some methodical results also provide proof of the theoretical flaw in the cipher, although they are simply not feasible to mount in practice. The algorithm is deemed practically safe in the form of Triple DES despite the theoretical attacks that have ensued. Several years earlier, the cipher was outmoded by the Advanced Encryption Standard (Naji *et al*., 2009c).

Since the adoption of DES, speculation has been rife that a certain backdoor was created into the cryptic S-boxes that would permit those who have the knowledge to crack DES successfully. Such speculation has been proven inoperative over time. Irrespective of any backdoors in the hash function, the rapid progress in the electronic circuitry speed in past two decades along with the natural parallelism upheld in the Feistel ciphers and the relatively small key of the DES have led to the algorithm becoming obsolete. In 1998, the Electronic Frontier Foundation constructed a DES Cracker (full specifications are available online) for less than $250,000. The cracker could decode DES messages within the period of not more than a week (Zaidan *et al*., 2009a; b).

Triple DES: Triple DES has undergone further developments to overcome some apparent shortcomings without having to create an entirely new cryptosystem. Triple DES works on the key size of DES by applying the algorithm three times in succession with three varying keys. The shared key size is 168-bits (3 times 56), which cannot be reached by brute-force techniques such as those used by the EFF DES Cracker. Triple DES has always been treated suspiciously, because the original algorithm was never intended to be employed as such, but no severe weaknesses have been revealed in its design. Today, it serves as a cryptosystem prevalent in several Internet protocols (Abomhara *et al*., 2010b).

Advanced encryption standard (AES)/Rijndael: Towards the end of the 1990s, the U.S. National Institute of Standards and Technology (NIST) organized a competition that aimed to develop a substitute for DES. The winner, which was announced in 2001, was called the Rijndael (pronounced "rhine-doll") algorithm, which gradually manifested itself as the new Advanced Encryption Standard. Rijndael integrates the Substitution-permutation Network (SPN) model by adopting the Galios field operations in each round. Rijndael shares a slight resemblance with the RSA modulo arithmetic operations. The Galios field operations have been demonstrated as rather nonsensical, but they can be inverted in a mathematical manner. By nature, the security of AES is not absolute, particularly in the area where it depicts a correlation between time and cost (Alam *et al*., 2010). Any questions raised on encryption security should be along the lines of how long and how costly it will be for an attacker to discover a key. It has been hypothesized that military intelligence services potentially have the technical and economic revenues to attack keys equivalent to about 90 bits, although any ordinary researcher with any kind of exposure would also possess such capability. The actual systems have demonstrated that today, within the limits of a commercial budget of about 1 million dollars, a system can administer key lengths of approximately 70 bits. A rough estimate on the rate of technological advancement is expressed within the

assumption that technologies will doubly increase the speed of computing devices annually at a static cost. If this is accurate, in theory, 128 bit keys would be in the range of a military budget in 30-40 years' time. To illustrate this, the current status for AES is shown here, where it is presumed that an attacker is capable of building or purchasing a system that computes keys at one billion keys per second. At the very least, this is 1000 times faster than the fastest personal computer ever sold in 2004. Under this unfounded premise, the attacker will require about 10 000 000 000 000 000 000 000 years to try all potential keys for the version with prominent weakness, which is AES-128. Thus, the key length should be selected after reaching a decision on how long the security is required and at what price it is to contain a secret key. In some military predispositions, security is seen to be endured in a matter of hours or days, as after a war or particular mission has ended, the information would be cast aside as uninteresting and valueless. Nonetheless, in other incidences, a lifetime may not be that time-consuming. To date, there is no evidence that AES has any limitations in terms of launching any sort of attack other than making the performance of a rather thorough search, i.e. brute force, probable. Even AES-128 has put forward a large number of possible keys that are regarded sufficient, altogether implying the impracticality of an exhaustive search. This is based on the proviso that no technological infiltration that could lead to a drastic increase in the availability of computational power and that theoretical studies do not resort to shorter procedures that remove the necessity of an exhaustive search. Relevant programmers need to be reminded of the variety of shortcomings, to steer clear of the time the encryption comes into practice and keys are produced (Zaidan *et al.*, 2010c). It is essential to ensure that every implementation is secure. However, this is a tough call because expertise would be needed to examine the implementation in detail and with great care. Any particular implementation should undergo an important aspect of assessment to ensure that such examination has been conducted, or can be carried out (Naji *et al.*, 2009c; Alanazi *et al.*, 2010c).

Comparison of symmetric encryption AES, 3DES AND DES: Advance Encryption Standard (AES) and Triple DES (TDES or 3DES) are the most common block ciphers used. The use of either AES or 3DES relies on the particular need of the user. This section will place focus on the differences of the two systems, particularly in terms of security and performance. As Triple DES works based on the DES algorithm, this section will first elaborate on the DES. The development of the DES in 1977 was carefully piloted to demonstrate better performance in hardware than it would be in the software. The DES performs considerable bit manipulation in substitution and permutation boxes in every one of the 16 rounds. For example, switching bit 30 with 16 is much easier in hardware than its software counterpart. DES encrypts data in 64 bit block size and effectively benefits from a 56 bit key. A 56-bit key space totals up to 72 quadrillion possibilities, in estimation. Although seemingly large, with contemporary computing power, this size is still insufficient and still susceptible to brute force attack. The DES could not keep abreast with the latest technological updates and is no longer considered suitable for security. As DES used to be wildly popular, an immediate way to solve this problem was to introduce Triple DES, which is sufficiently adaptable for most purposes today. The Triple DES is a built-up of the DES application three times in sequence. The system (Triple DES) with three varying keys (K1, K2 and K3) has effectual key length of 168-bits (the use of three distinct keys is advisable for 3DES). Another variation is labeled the two-key (K1 and K3 is same) 3DES, has a lower effective key size of 112 bits, which is not very secure. Two-key 3DES is widely used in the electronic payment industry. Moreover, Triple DES takes thrice as much CPU power than its antecedent counterpart, which has a more significant performance reputation. The AES also outperforms 3DES both in software and hardware (Arenas *et al.*, 2008; Barker and Roginsky, 2011).

Table 1: Comparison between AES, 3DES and DES (Alanazi *et al*., 2010d)

Factors	AES	3DES	DES
Key length	128, 192 or 256 bits	(k1, k2 and k3) 168 bits (k1 and k2 are same) 112 bits	56-bit
Cipher type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher
Block size	128, 192, or 256 bits	64 bits	64 bits
Developed	2000	1978	1977
Cryptanalysis resistance	Strong against differential, truncated differential, linear, interpolation and square attacks	Vulnerable to differential; Brute Force Attacker could analyze plain text using differential cryptanalysis	Vulnerable to differential and linear cryptanalysis; weak substitution tables
Security	Considered secure	One only weakness, which exists in DES	Proven inadequate
Possible keys	2^{128}, 2^{192}, or 2^{256}	2^{112} or 2^{168}	2^{56}
Possible ASCII printable character keys	95^{16}, 95^{24}, or 95^{32}	95^{14} or 95^{21}	95^{7}
Time required to check all possible keys at 50 billion keys per second**	For a 128-bit key: 5 x 10^{21} years	For a 112-bit key: 800 days	For a 56-bit key: 400 days

The Rijndael algorithm is chosen as the Advance Encryption Standard (AES) to take over the 3DES. Rijndael is the brainchild of Joan Daemen and Vincent Rijmen. With the combined qualities of security, performance, efficiency, implement ability and flexibility of the Rijndael, it is ideal for the AES. As to the aspect of design, the AES as software works more rapidly and in turn, works efficaciously in hardware. The AES also functions quickly even on not-very-large gadgets such as smart phones and smart cards. Moreover, the AES offers more security, as explained by its larger block size and longer keys as it AES adopts 128-bit fixed block size and it is compatible with 128-, 192- and 256- bit keys. In general, the Rijndael algorithm has flexibility that allows it to cooperate sufficiently with the key and block size of any multiple 32- bits with minimum of 128- bits and maximum of 256- bits. The AES is the substitute for 3DES and following the regulations of NIST, both ciphers will exist together until 2030, which indicate that both will be sanctioned to undergo gradual transition to become the AES. However, although the AES has better theoretical strength than the 3DES especially where speed and efficiency are concerned, in some hardware, 3DES reinforcement may be more fast-paced, particularly because the 3DES has more mature support (Alanazi *et al*., 2010a, c; Juels, 2006).

In Table 1, a comparison among these three algorithms is performed based on nine factors to recognize basic differences among them (Alanazi *et al*., 2010d).

The table shows a comparison of the DES, 3DES and AES, which is divided into nine factors, namely the key length, cipher type, block size, developed, cryptanalysis resistance, security, possibility key, possible ACSII printable character keys and time required to check all possible keys at 50 billion seconds. The comparison shows that the AES is better than the DES and 3DES (Alanazi *et al*., 2010d).

Asymmetric cryptography algorithms: Asymmetric cryptography is a type of cryptography also known as public-key cryptography, which is conducted using a pair of related keys, as shown in Fig. 5 (Microsoft Corporation, 2005). A message encrypted with a key can only be decrypted with the equivalent part of that key (Alanazi *et al*., 2010a). In public-key encryption, every participating party should have a pair of keys: a private one, which should be secured and known only to the

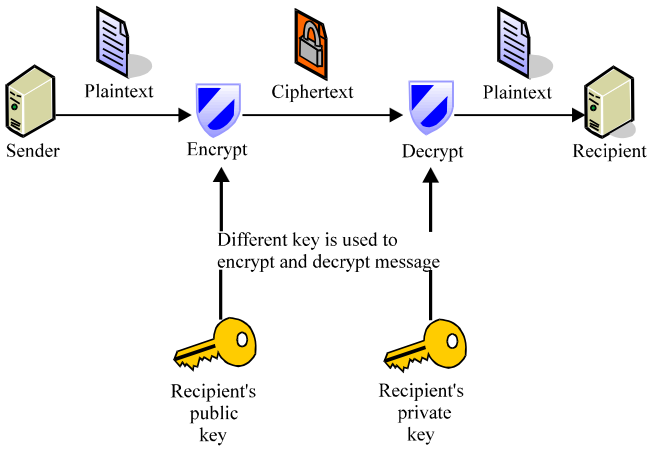

Fig. 5: Process of asymmetric encryption (Microsoft Corporation, 2005)

holder and a public one, which anyone can hold. If the encryption process is performed with a party's public key, the decryption should be completed with the counterpart private key (Al-Bakri *et al*, 2011; Medani *et al*., 2011). The inverse is also correct: if a message is encrypted with someone's private key, it should be decrypted with the user's public key (Menezes *et al*., 1996). In contrast to symmetric algorithms, asymmetric algorithms are more recent. Among the most well known asymmetric algorithms is the RSA. Rivest *et al*. (1978) introduced the RSA Cryptosystem, the first public-key system (Alanazi *et al*., 2010a).

Public key Cryptography does not require a secure initial exchange of one or more secret keys to both sender and receiver. Asymmetric key algorithms are used to generate a mathematically linked key pair, a private key and a public key. The use of these keys provides security in the authenticity of a message by producing a digital signature using the private key, which can be verified using the public key. It also provides protection in terms of confidentiality and reliability of a message. Public key cryptography is a crucial and widely used technology around the world. It is an approach that has been employed by numerous cryptographic algorithms and cryptosystems. Some examples of well-known asymmetric algorithms include the RSA, ECC and NTRU (Menezes *et al*., 1996; Yadav, 2010).

RSA (Ravest, Shamir, Adleman): The RSA is a widely established asymmetric encryption system pioneered by Rivest *et al*. (1978). As an adopted standard system that deals with public key encryption, the private key remains private, but the public key is given to everybody in the RSA. Since its creation, the RSA has been considered as one of the most protected cryptosystems (Al Hasib and Haque, 2008). The RSA has become commonplace in instances where secure communication channels are set up as well as for authentication of the service provider identity over vulnerable communication mediums. In the authentication scheme, the server enforces public key authentication with the client by having the client sign a unique message using the private key, bringing about what it known today as the digital signature. The signature is then returned to the client, who validates it using the server's well-established public key (Singh and Maini, 2011). The security of the RSA cryptosystem security also has certain imperfections. An attacker can exploit a number of approaches to harass the RSA algorithm. Some popular approaches include the Brute force, Mathematical attacks, Timing attacks and Chosen Ciphertext attacks (Al Hasib and Haque, 2008).

Ntru algorithm (nth degree truncated polynomial ring units): The NTRU algorithm was created in 1996 by three mathematicians, namely, Hoffstein *et al.* (1998). The NTRU Cryptosystem received endorsement to be systemized as a standard by the Institute of Electrical and Electronics Engineers (IEEE) (Hoffstein *et al.*, 1998). As one of the most widely known robust cryptosystem algorithms, NTRU has been transformed for presentation as a novel cryptography generation that contributes to the enhanced performance of encryption and decryption processes that reflect numerous cryptography-based problems. Despite still being in the process of development and requiring further research to ensure perfection, the NTRU algorithm serves as a good alternative as a more solidified foundation for upcoming wireless communications because of several plus points, including a more assured security great speed and reduced computational complications (Alanazi *et al.*, 2010b; Jha and Saini, 2011).

The NTRU is a ring-based public key cryptosystem that relies on the dual ring operations of addition and multiplication. Bearing this in mind, it is noticeably dissimilar to most widespread cryptosystems, which are group-based and use only group operations to serve the parameters. The well-off arithmetical arrangement of the underlying ring is one advantage of the NTRU cryptosystem. Conversely, the ring structures in cryptography are not as thoroughly explored as the group theory and therefore, it more convenient to administer security evidence within groups (Anonymous, 2002).

In principle, lattice-based systems and NTRU offer great speed and are anticipated to endure the advancement of fairly sized quantum computers successfully because their root problems do not recognize any quantum algorithm, particularly general cases. It is also difficult to suggest any secure instances, even when reference is made to a classical computing model. Moreover, complications that have surrounded the classical lattice reduction algorithm are still not very well understood (Yadav, 2010). To date, no established quantum algorithms can unravel the lattice problems with more credible complexity than classical algorithms. Therefore, lattice-based schemes might show off their sense of survival in the quantum computation age (Anonymous, 2002).

Comparison of RSA and NTRU: The construction of secure instances and excellent performance for security algorithms remains an area of active focus in research. Recent works appear to suggest that a fast, yet efficient, NTRU-based system is feasible. In this section, comparative analysis is presented to show the strongest features between the RSA and NTRU. Criteria used to evaluate security algorithms include, key size, data types, encryption/decryption speed, power consumption and several other features like estimated breaking times and compatibility.

Key size: The expression of public and private key sizes in the form of bits has been considered as appealing. The key size formula is interpreted as the number of bits needed to maintain the storage of each term and the coefficient of each polynomial in the key, multiplied by the number of terms in the polynomial. Therefore, as an instance, the public key size for N = 167 and q = 128 is 167*log 2128 = 1169 bits. The private key would normally involve keeping tab of both f and Fp and thus is twice as large as the public key. Nevertheless, the speedier key generation variation of NTRU does not require storage and thus, the sizes of the private and public keys are similar. The RSA leans on modular arithmetic with extremely lengthy operands, thus, RSA performance has been noted to lag on constrained environments, one of which is poor memory and processor power.

Table 2: Estimated breaking times for NTRU and RSA (Karu and Loikkanen, 2001)

Cryptosystem	Security level	Estimated breaking time
RSA	512 bits	105 MIPS-years
NTRUEncrypt	N =167	106 MIPS-years
RSA	1024 bits	1012 MIPS-years
NTRUEncrypt	N =263	1014 MIPS-years
RSA	2048 bits	1021MIPS-years
NTRUEncrypt	N =503	1035 MIPS-years
RSA	4096 bits	1033 MIPS-years

Some advances noted on the issue of factorization have led to key sizes that are thought to be well protected today to be relatively long. The normal key size used for the RSA is 1024-bits (Karu and Loikkanen, 2001). As relationship between the key size and performance for a given cryptosystem is quite marked, it is rather imminent that the RSA would no longer be considered practical anymore, particularly because other systems proposed will boast of simultaneously better quality and protection. The reality is that the current implementation on high security RSA on embedded system is a tough call for technological experts. Variations are used even for short key and soon the RSA can no longer be deemed to be a lightweight cryptosystem (Anonymous, 2002).

Encryption and decryption: The good point about decryption time for the NTRU over the RSA demonstrates the advantage of the use of small integer values by the NTRU over the large integer values of the RSA. Another tangible aspect is that as the key size increases, the performance of the NTRU gradually increases. The fastest variations of both algorithms were adopted and towards providing a fair comparison, the encryption time for RSA is remarkably faster than the NTRU as explained by the small modulo exponentiation operations required when using F4 as the public exponent (e). A similar outcome can be anticipated should (e) be fixed to 3. Some of the NTRU versus RSA criteria assessments in literature have mentioned (e) as a random large number, following the order of the modulus size. However, this option appears to be non-existent in the Cryptic RSA implementation and as the result was eliminated for encryption and it should be supposed that the NTRU would have speed roughly twice that noted in the decryption (D'Souza, 2001). In Table 2 estimated time of breaking for both algorithms (NTRU and RSA) is provided based on key size (Karu and Loikkanen, 2001).

Referring to the previous comparison between the RSA and NTRU algorithms (Table 2), it can be concluded that NTRU has more advantages over the RSA, particularly in terms of encryption performance and compatibility. The analysis graphs above indicate the superiority of NTRU in terms of encryption and decryption processes. Table 3 provides some literature work done in the m-Government area to explore most significant contribution in the field.

CONCLUSION

A theoretical study of information security and m-Government was explored and two significant requirements for secure systems and applications were discussed. The significant aim of the study is to show the remarkability of applying security in any information system implemented. The study

Table 3: Literature survey on some contributions in the m-government field

Author, year	Paper	Contribution	Strengths	Weaknesses
Ostberg (2003)	Swedish view on mobile government	Registered driver can log in and out of a parking space using a mobile phone, Fee is automatically charged to the driver's account and receipt is sent via SMS	Adoption of mobility	No security in data transmission
Kim *et al.* (2004)	Architecture for implementing , mobile government services in Korea	PDA-based interactive services m-police and m-tax management	SMS was the killer application for mG2c and mG2G	Services were based on platforms of private service providers
Abanumy and Mayhew (2005)	M-government Implications for E-government, In developing countries: The case of Saudi Arabia	Saudi government has started to liberate the telecommunication sector through privatization and competition	Mobile technology usage increased	Increased both Internet and mobile penetration
Griffin *et al.* (2006)	Using SMS, texting to Encourage Democratic participation by youth citizens: a case study of a project in an English local authority	Adopting M-voting to be used in elections	Mobile phone as a technology is ubiquitous among young citizens	Lack of security and privacy
Cao and Luee (2007)	Application of M-government system in Beijing municipal government	M-commerce applications have been adopted in China	Balanced the gap between requirements and capacity	No security consideration in transmission medium
Ntaliani *et al.* (2008)	Mobile government: A challenge for agriculture	Implementation of m-Government in agriculture	Cost-effective	No security consideration
Hypponen (2009)	Open mobile identity secure identity management and mobile payments using hand-held devices MNO and naturally,	Estonia follows an approach similar to the Finnish one. The mobile e-ID solution called Mobiil-ID began in 2007 and ports functionality originally provided by e-ID smart cards to SIM cards. This way, mobile phones can be used to authenticate web portals and create electronic signatures	Provides compatibility with almost any GSM mobile phone and needed infrastructure	Authentication cannot be done without the participation of the availability of all operators charge both customers and service providers for authentication using MNO services for every transaction increase latency

also provides an assessment of m-Government and presents some well-known algorithms applied in security particularly applied to embedded systems such as mobiles. A comparison among these algorithms was conducted and a literature survey that points to the strongest algorithm in securing the transfer medium in the m-Government (G2C) was provided. Upon the completion of this work, the objective of choosing a powerful technique in securing m-Government services in general and messaging services in particular should be clear. The study further aims to deliver a sound theoretical background in the field of study and make references to the needs and requirements for m-Government services to make them more vigilant on the malicious breaches by attackers and increase awareness to ensure better privacy.

REFERENCES

Abanumy, A.N. and P.J. Mayhew, 2005. M-government implications for e-government in developing countries: The case of Saudi Arabia. Proceedings of the 1st European Mobile Government Conference, July 10-12, 2005, University of Sussex, pp: 1-6.

Abomhara, M., O. Zakaria, O.O. Khalifa, A.A. Zaidan and B.B. Zaidan, 2010a. Enhancing selective encryption for H.264/AVC using advance encryption standard. Int. J. Comput. Electr. Eng., 2: 1793-8201.

Abomhara, M., O.O. Khalifa, O. Zakaria, A.A. Zaidan, B.B. Zaidan and H.O. Alanazi, 2010b. Suitability of using symmetric key to secure multimedia data: An overview. J. Applied Sci., 10: 1656-1661.

Abramowicz, W., L. Karsenty, P.M. Olmstead, G. Peinel, D. Tilsner and M. Wisniewski, 2005. USE-ME. GOV (Usability-driven open platform for Mobile-government). http://www.m4life.org/proceedings/2005/PDF/2_R361OP.pdf

Al Hasib, A. and A.A.M.M. Haque, 2008. A comparative study of the performance and security issues of AES and RSA cryptography. Proceedings of the 3rd International Conference on Convergence and Hybrid Information Technology, November 11-13, 2008, Busan, pp: 505-510.

Al-Bakri, S.A., M.L.M. Kiah, A.A. Zaidan, B.B. Zaidan and G.M. Alam, 2011. Securing peer-to-peer mobile communications using public key cryptography. Int. J. Phys. Sci., 6: 930-938.

Alam, G.M., M.L.M. Kiah, B.B. Zaidan, A.A. Zaidan and H.O. Alanazi, 2010. Using the features of mosaic image and AES cryptosystem to implement an extremely high rate and high secure data hidden: Analytical study. Sci. Res. Essays, 5: 3254-3260.

Alanazi, H.O., A.H. Jalab, A.A. Zaidan and B.B. Zaidan, 2010a. New frame work of hidden data with in non multimedia file. Int. J. Comput. Network Security, 2: 46-54.

Alanazi, H.O., B.B Zaidan, A.A. Zaidan, A.H. Jalab, M. Shabbir and Y. Al-Nabhani, 2010b. New comparative study between DES, 3DES and AES within nine factors. J. Comput., 2: 152-157.

Alanazi, H.O., H.A. Jalab, G.M. Alam, B.B. Zaidan and A.A. Zaidan, 2010c. Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance. J. Med. Plants Res., 4: 2059-2074.

Alanazi, H.O., M.L.M. Kiah, A.A. Zaidan, B.B. Zaidan and G.M. Alam, 2010d. Secure topology for electronic medical record transmissions. Int. J. Pharmacol., 6: 954-958.

Anonymous, 2002. IST-2002-507932 ECRYPT: European network of excellence in cryptology. D.AZTEC.2 Alternatives to RSA, Network of Excellence, Information Society Technologies, pp: 1-138.

Arenas, A., J.P. Banatre and T. Priol, 2008. Developing secure chemical programs with aspects. CoreGRID Technical Report, Number TR-0166, August 31st, 2008.

Barker, E. and A. Roginsky, 2011. Transitions: Recommendation for transitioning the use of cryptographic algorithms and key lengths. NIST Special Publication, SP 800-131A, January 2011.

Bellovin, S.M., 1989. Security problems in the TCP/IP protocol suite. Comput. Commun. Rev., 19: 32-48.

Brucher, H. and P. Baumberger, 2003. Using mobile technology to support eDemocracy. Proceedings of the 36th Hawaii International Conference on System Sciences, January 6-9, 2003, IEEE Computer Society Washington, DC, USA., pp: 1-8.

Cao, J.T. and T.J. Luee, 2007. Application of m-government system in Beijing municipal government. Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, October 7-10, 2007, Montreal, Canada, pp: 3220-3224.

D'Souza, R., 2001. The NTRU cryptosystem: Implementation and comparative analysis. Semester Project. http://teal.gmu.edu/courses/ECE543/project/reports_2001/dsouza.pdf

El Kiki, T. and E. Lawrence, 2006. Government as a mobile enterprise: Real-time, ubiquitous government. Proceedings of the 3rd International Conference on Information Technology: New Generations, April 10-12, 2006, Las Vegas, Nevada, pp: 320-327.

Feruza, Y.S. and T.H. Kim, 2007. IT security review: Privacy, protection, access control, assurance and system security. Int. J. Multimedia Ubiquitous Eng., 2: 17-32.

German, S., 2012. Sumerian art. Khan Academy. http://smarthistory.khanacademy.org/sumerian-art.html.

Griffin, D., P. Trevorrow and E. Halpin, 2006. Using SMS texting to encourage democratic participation by youth citizens: A case study of a project in an english local authority. Electronic J. e-Government, 4: 63-70.

Harris, R.E., 1997. The need to know versus the right to know: Privacy of patient medical data in an information-based society. Suffolk Univ. Law Rev., 30: 1183-1218.

Hmood, A.K., Z.M. Kasirun, H.A. Jalab, G.M. Alam, A.A. Zaidan and B.B. Zaidan, 2010. On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates. Int. J. Phys. Sci., 5: 1054-1062.

Hoffstein, J., J. Pipher and J.H. Silverman, 1998. NTRU: A ring-based public key cryptosystem. Proceedings of the 3rd International Symposium on Algorithmic Number Theory, June 21-25, 1998, Portland, Orgeon, USA.

Hypponen, K., 2009. Open mobile identity - secure identity management and mobile payments using hand-held devices. M.A. Thesis, University of Kuopio, Finland.

Jha, R. and A.K. Saini, 2011. A comparative analysis and enhancement of NTRU algorithm for network security and performance improvement. Proceedings of the International Conference on Communication Systems and Network Technologies, June 3-5, 2011, Katra, Jammu, pp: 80-84.

Juels, A., 2006. RFID Security and privacy: A research survey. IEEE J. Select. Areas Commun., 24: 381-394.

Kartalopoulos, S.V., 2009. Security of Information and Communication Networks. Vol. 15. Wiley-IEEE Press, Washington, DC, USA., ISBN-13: ISBN: 978-0-470-29025-5, Pages: 344.

Karu, P. and J. Loikkanen, 2001. Practical comparison of fast public-key cryptosystems. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.96.5694&rep=rep1&type=pdf

Kim, Y., J. Yoon, S. Park and J. Han, 2004. Architecture for implementing the mobile government services in Korea. Conceptual Modeling Adv. Appli. Domains, 3289: 601-612.

Kissel, R., 2011. Glossary of Key Information Security Terms. DIANE Publishing, New York, USA., ISBN-13: 9781437980097, Pages: 207.

Lhotska, L. and P. Aubrecht, 2008. Deliverable D09 security of the multi agent system. Agent System, Project of K4CARE. http://www.k4care.net/fileadmin/k4care/public_website/downloads/MAS_Security_D09.pdf

Medani, A, A. Gani, O. Zakaria, A.A. Zaidan and B.B. Zaidan, 2011. Review of mobile SMS security issues and techniques towards the solution. Sci. Res. Essays, 6: 1147-1165.

Menezes, A.J., P.C. Van Oorschot and S.A. Vanstone, 1996. Handbook of Applied Cryptography. CRC Press, Boca Raton, FL, USA.

Microsoft Corporation, 2005. Web Service Security: Scenarios, Patterns and Implementation Guidance for Web Services Enhancements (WSE) 3.0. O'Reilly Media Inc., Cambridge, MA, USA.

Mukherjee, A. and A. Biswas, 2005. Simple implementation framework for m-government services. Proceedings of the International Conference on Mobile Business, July 11-13, 2005, IEEE Computer Society Washington, DC, USA., pp: 288-293.

Nabi, M.S.A., M.L.M. Kiah, B.B. Zaidan, A.A. Zaidan and G.M. Alam, 2010. Suitability of using SOAP protocol to secure electronic medical record database transmission. Int. J. Pharmacol., 6: 959-964.

Naji, A., A. Zaidan, B. Zaidan and I.A.S. Muhamadi, 2009a. Novel approach for cover file of hidden data in the unused area two within EXE file using distortion techniques and advance encryption standard. Proceedings of the International Conference on Computer, Electrical and Systems Science and Engineering, May 4-6, 2009, Ottawa, Canada, pp: 26-28.

Naji, A.W., A.A. Zaidan, B.B.A. Shihab and O.O. Khalifa, 2009b. Novel approach of hidden data in the (Unused area 2 within EXE file) using computation between cryptography and steganography. Int. J. Comput. Sci. Network Secur., 9: 294-300.

Naji, A.W., A.S. Housain, B.B. Zaidan, A.A. Zaidan and S.A. Hameed, 2011. Security improvement of credit card online purchasing system. Scient. Res. Essays, 6: 3357-3370.

Naji, A.W., H.A. Shihab, B.B. Zaidan, F. Al-Khateeb Wajdi, O.O. Khalifa, A.A. Zaidan and S.T. Gunawan, 2009c. Novel framework for hidden data in the image page within executable file using computation between advance encryption standared and distortion techniques. Int. J. Comput. Sci. Inform. Security, 3: 73-78.

Ntaliani, M., C. Costopoulou and S. Karetsos, 2008. Mobile government: A challenge for agriculture. Government Inform. Q., 25: 699-716.

OECD-ITU, 2011. M-Government: Mobile Technologies for Responsive Governments and Connected Societies. OECD Publishing, Geneva, Switzerland, ISBN-13: 9789264118690, Pages: 152.

Ostberg, O., 2003. A Swedish view on mobile government. Proceedings of the International Symposium on E- and M-Government, December 18, 2003, Seoul, Korea.

Pal, R.K., 2008. Design and implementation of secure file system. Master's Thesis, Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, India.

Pappas, J.A., 2008. A revitalized information assurance training approach and information assurance best practice rule set. Master's Thesis, Naval Postgraduate School, Monterey, CA., USA.

Pathan, A.S.K., H.W. Lee and C.S. Hong, 2006. Security in wireless sensor networks: Issues and challenges. Proceedings of the 8th International Conference Advanced Communication Technology, Volume 2, February 20-22, 2006, Phoenix Park, Dublin, Ireland, pp: 1043-1048.

Patil, J.E. and A. Shaligram, 2010. FPGA implementation for real time encryption engine for real time video. Proceedings of the 14th WSEAS International Conference on Circuits, July 22-25, 2010, Corfu Island, Greece, pp: 62-69.

Rivest, R.L., A. Shamir and L. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM., 21: 120-126.

Salem, Y., M. Abomhara, O.O. Khalifa, A.A. Zaidan and B.B. Zaidan, 2011. A review on multimedia communications cryptography. Res. J. Inform. Technol., 3: 146-152.

Schneier, B., 1996. Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley and Sons Inc., New York, USA.

Singh, S.P. and R. Maini, 2011. Comparison of data encryption algorithms. Int. J. Comput. Sci. Commun., 2: 125-127.

Stallings, W., 1995. Network and Internetwork Security: Principles and Practice. 2nd Edn., Prentice Hall, New York, USA., ISBN-13: 9780024154835, Pages: 462.

Stevens, G., 2010. Federal information security and data breach notification laws. Congressional Research Service (CRS) Report for Congress. http://www.fas.org/sgp/crs/secrecy/RL34120.pdf.

Ware, W.H., 1998. The Cyber-Posture of the National Information Infrastructure. RAND Corporation, USA., ISBN-13: 9780833026217, Pages: 37.

Yadav, S.K., 2010. Some problems in symmetric and asymmetric cryptography. Ph.D. Thesis, Department of Mathematics, Agra University, India.

Yun, C.H. and M.S. Chen, 2000. Mining web transaction patterns in an electronic commerce environment. Proceedings of the 4th Pacific-Asia Conference on Knowledge Discovery and Data Mining: Current Issues and New Applications, April 18-20, 2000, Kyoto, Japan, pp: 216-219.

Zaidan, A.A., A.W. Naji, S.A. Hameed, F. Othman and B.B. Zaidan, 2009a. Approved undetectable-antivirus steganography for multimedia information in PE-file. Proceedings of the International Association of Computer Science and Information Technology-Spring Conference, April 17-20, 2009, Singapore, pp: 425-429.

Zaidan, A.A., B.B. Zaidan, M.M. Abdulrazzaq, R.Z. Raji and S.M. Mohammed, 2009b. Implementation stage for high securing cover-file of hidden data using computation between cryptography and steganography. Int. Assoc. Comput. Sci. Inform. Technol., 20: 482-489.

Zaidan, A.A., B.B. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010a. An overview: Theoretical and mathematical perspectives for advance encryption standard/rijndael. J. Applied Sci., 10: 2161-2167.

Zaidan, A.A., B.B. Zaidan, A.Y. Taqa, H.A. Jalab, K.M. Sami and G.M. Alam, 2010b. Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem. Int. J. Phys. Sci., 5: 1776-1786.

Zaidan, A.A., B.B. Zaidan, H.O. Alanazi, A. Gani, O. Zakaria and G.M. Alam, 2010c. Novel approach for high (Secure and rate) data hidden within triplex space for non multimedia file. Sci. Res. Essays, 5: 1965-1977.

Zaidan, B.B., A.A. Zaidan, A. Taqa, G.M. Alam, M.L.M. Kiah and H.A. Jalab, 2010d. StegoMos: A secure novel approach of high rate data hidden using mosaic image and ANN-BMP cryptosystem. Int. J. Phys. Sci., 5: 1796-1806.

Zaidan, B.B., A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010e. On the differences between hiding information and cryptography techniques: An overview. J. Applied Sci., 10: 1650-1655.

Zaidan, B.B., A.A. Zaidan and M.L.M. Kiah, 2011. Impact of data privacy and confidentiality on developing telemedicine applications: A review participates opinion and expert concerns. Int. J. Pharmacol., 7: 382-387.

Zalesak, M., 2003. M-government: More than a mobilized government. Web Projects Ltd.