A Review of RSA Cryptosystems and Cryptographic Protocols

[1]Prince Oghenekaro Asagba, [1]Enoch O. Nwachukwu

[1]Department of Computer Science, University of Port Harcour, PMB 5323, Port Harcourt,
Rivers State, Nigeria (pasagba@yahoo.com),

ABSTRACT

The use of cryptography in information security over insecure open network in both the convectional, symmetric encryption and the public-key cryptography has witnessed tremendous developments over the years. No doubt, the public-key cryptography is an established technology in terms of modern approach in information security despite the seemingly challenges it has. This paper gives an overview of the public-key cryptography with emphasis on the RSA algorithm. We examined public-key cryptography, reviewed RSA cryptosystems and cryptographic scheme, and discusses some security issues and challenges of RSA. The objective of this work is to present holistic appraisal of the RSA cryptosystems.

Keywords

Cryptography, Public-key Cryptosystems, RSA algorithm, Encryption, Decryption, Cryptographic Scheme.

1.0 Introduction

Nowadays, the use of computer has gone beyond their early intentions. They now found use in the e-initiative (e-banking, e–commerce, e–shopping) etc. These phenomenal changes have brought about the need for tight security to data and information as they are transported across network to network [1]. E-banking, e-commerce, e-shop- ping, etc., transactions over the un-trusted communications channels are now possible because of the application of data encryption mechanisms. The inability to secure data or information where unauthorized access is probable and where other security techniques are inadequate may have necessitated the concept of cryptography.

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin [17]. Cryptography is one of the technological means to provide security to data being transmitted on information and communications systems. Cryptography is especially useful in the cases of financial and personal data. Hence, information security is a precondition of e-application systems when communicating over un-trusted medium like the Internet [3]. Cryptographic techniques have been providing secrecy of message content for thousands of years [7]. A cryptographic primitive is a basic mathematical operation on which cryptographic schemes can be built [16]. Cryptography is about communication in the presence of adversaries. Cryptographic goals include: privacy/confidentiality, data integrity, authentication, and non-repudiation.

A fundamental goal of cryptography is to adequately address these four areas_in both theory and practice. Cryptography is all about the prevention and detection of cheating and other malicious activities [17]. Cryptography can be applied to safeguard communication channels and physical databases. Cryptography has two techniques: symmetric algorithms (or private key cryptosystems) and asymmetric algorithms (or public key cryptosystems). In the symmetric scheme, the same cryptographic key is used for both enciphering and deciphering processes. Symmetric key do not guarantee security if the sender key is known. In asymmetric cryptographic algorithms, two keys are used: one key, called the public key is used to encrypt the plaintext or message; while the second key, called the private key is used to decrypt the plaintext or message. These two techniques are inherently different from each other.

In the symmetric cryptosystem where the sender and the receiver use the same key, which is kept secret from every one else, the biggest problem is the shared key management. If communications were to take place between you and several people - you need to have different secret keys for each person otherwise each person can read messages meant for one another. The concept of the public key infrastructure conceived by Diffie and Hellman, proffer a solution to get around the problem of key management by using the asymmetric cryptosystem or public-key cryptography. This paper is a review of the public-key cryptography with emphasis on the RSA cryptosystems and cryptographic schemes.

The development of public-key cryptography is the greatest and perhaps the only true revolution in the entire history of cryptography. From its earliest beginnings to modern times, virtually all cryptographic systems have been based on the elementary tools of substitution and permutation [23].

2.0 Public-Key Cryptography

Public-key cryptography is based on the use of a key for encryption and another but related key for decryption. The characteristics of Public-key cryptography are summarized as follows:

- It is computationally difficult to ascertain the decryption key with the knowledge of the encryption key and cryptographic algorithm.
- In some cryptosystems, like RSA, either of the two related keys, e or d, could be used to compute encryption and decryption respectively.

2.0.1 The Essential Steps of Public-Key Cryptography

The essential steps of Public-key cryptography in [23] are:

- Each end system in a network generates a pair of keys to be used for encryption and decryption of messages that it will receive.
- Each system publishes its encryption key by placing it in a public register or file. This is the public key. The companion key is kept private.
- If A wishes to send a message to B, it encrypts the message using B's public key.
- When B receives the message, B decrypts it using B's private key. No other recipient can decrypt the message because only B knows B's private key.

2.0.2 Applications of Public-key Cryptography

The use of public-key cryptosystems can be applied to three classes:

- Encryption / decryption: A encrypts a message with B's public-key.
- Digital signature: A "signs" a message with its private key, while for the verification of the signature, only the knowledge of the corresponding public key is necessary.
- Key exchange: This involves two parties agreeing in exchanging a session key. A number of techniques for achieving this abound - with regard knowledge of the private key(s) of one or both parties.

Some algorithms are suitable for all three applications, whereas others can be used only for one or two of these applications [23].

2.0.3 Requirements for Public-Key Cryptography

The cryptosystem in Table 1 rely on the use of two related keys for its cryptographic protocols. Table 1 shows applications for public-key cryptosystems.

Table 6: Applications for Public-key Cryptosystems [23]

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No

2.0.4 Public-key Cryptanalysis

An attacker tries to decrypt encrypted messages using any of the available methods at his/her disposal, such as, brute force – attempts to guess decryption keys; attacks on algorithms and protocol weaknesses, etc.

As with conventional encryption, a public-key encryption scheme is vulnerable to a brute-force attack. The countermeasure is the same: Use large keys. However, there is a trade-off to be considered. Public-key systems depend on the use of some sort of invertible mathematical function. The complexity of calculating these functions may not scale linearly with the number of bits in the key but grow rapidly than that. Thus, the key size must be large enough to make brute-force attack impractical but small enough for practical encryption and decryption. Another form of attack is to find some way to compute the private key given the public key [23].

3.0 Brief History of Asymmetric Cryptosystems And Rsa

The first invention of asymmetric cryptosystems was by James H Ellis, Malcolm Williamson, and Clifford Cocks in the early 1970s. 1976 marked a major breakthrough in the history of asymmetric cryptography. In that year, an asymmetric cryptosystem was published by Diffie Whitfield and Hellman Martin, which came to be known as Diffie-Hellman key exchange, was the first practical method for establishing a shared secret key over an insecure communications channel without bothering on the use of previous shared secret. Cooks method was later reinvented by RSA in 1977 and their work was made published in 1978, and the algorithm came to be known as RSA [28]. The introduction of public-key cryptography by Diffie and Hellman in 1976 was an important watershed in the history of cryptography. The work sparked off interest in the cryptographic research community and soon several public-key schemes were proposed and implemented. The RSA, being the first realisation of this abstract model, is the most widely used public-key scheme today [2]**.** The security of RSA is based on the difficulty of factoring n.

The RSA cryptosystem, named after its inventors R. Rivest, A. Shamir, and L Adleman, is the most widely used public-key cryptosystem. It may be used to provide both secrecy and digital signatures and its security is based on the intractability of the integer factorization problem [18]. The concept of a digital signature was introduced by Diffie and Hellman. The first practical realization of a digital scheme appeared in the paper in [20].

3.0.1 Review of Cryptographic Scheme

A number of works on the application of cryptographic scheme to secure data from untrusted communications channels based on different computer services and applications have been developed by academic scholars and researchers over the years. [12] worked on a secure directory service based on exclusive encryption. Their design uses encryption for protecting data privacy and Byzantine replication for protecting data integrity. The context of their work is a secure scalable file system that logically functions as a centralized file service but physically distributed among a network of untrusted desktop workstations.

If across the board services encryption is needed for services like FTP or Telnet, encryption devices are employed. Theses devices examine every network packet before it leaves the private network, and if a packet is destined for outside networks specified by a security administrator, the data portion of the packet is encrypted. Anyone capturing that data packet as it travel over an outside network connection is unable to read it [6]. The blooming e-commerce is demanding better method to protect online user's privacy, especially the credit card information that is widely used in online shopping. Holding all these data in a central database of the web sites would attract hackers' impose unnecessary liability on the merchant web sites, and raises the customers' privacy concerns [11]. The use of encryption techniques is not limited to data and information alone, its use extends to areas where absolute security are needed, such as operating systems, Web applications, GSM, and so on.

Asymmetric encryption algorithm can be used to exchange the key of the symmetric encryption algorithm because it is t more slowly than symmetric encryption algorithm, so asymmetric encryption algorithm is usually used to secure encryption key of the symmetric encryption algorithm in the practice, but symmetric encryption of message algorithm is usually used to secure the communication [31]. Tamper detection is also accomplished with cryptography technologies [6]. Kerberos is a security protocol developed by MIT. Windows 2000/Active Directory networks use Kerberos to authenticate users logging on to the network. Because Kerberos relies on the asymmetric scheme when exchanging data with the clients and servers involved in the authentication process, all passwords and other sensitive information are always transmitted in encrypted form, and never in cleartext. This ensures that even if an unauthorized individual were to capture the packets exchanged during the authentication procedure, no security compromise would result. Kerberos authentication is based on the exchange of tickets that contain an encrypted password that verifies a user's identity [29]. Cryptographic applications will continue to increase as long as the demand for Internet services continues. All the services provided by the Internet require one form of encryption or another.

The objective of GSM system is to make the system as secure as the public switched network. Radio transmission is the media of transmission for GSM system and this poses a number of threats from eavesdropping. Authentication is used to identify the user to the network operator. It uses a technique that can be described as "Challenge and response", based on encryption. A random challenge is issued to the mobile; the mobile encrypts the challenge using the authentication algorithm (A3) and the key assigned to the mobile, and sends a response back. The operator can check that, given the key of the mobile, response to the challenge is correct [19]. In the GSM System, encryption takes place over the air path.

In the digital world it is easy to impersonate others. Only strong cryptography can protect against these attacks [21]. The last threat we must guard against is people. People are always the weakest security link. Whether it is a guard being bribed to leave a door open or an unsuspecting employee opening an attachment that turns to be a virus. People are the most difficult security problem. They will forever bypass security they find intrusive, subvert security they find bothersome, and attack the very systems they are supposed to be guarding. On computer networks, inside attacks are much more dangerous that outside hackers. User mistakes are much more damaging than malicious code. It is a problem as old as civilization, and it's not one that computers can magically solve [26].

3.0.2 Review of RSA Cryptosystems

A number of works on the review/modification of RSA cryptosystem have been proposed (or embarked upon) by academic scholars and researchers over the years.

A resemblance of the RSA cryptosystem which uses special kinds of elliptic curves over Z_n, where n is a composite integer, was proposed by Koyama et al. Also, Demytko, presented a resemblance of the RSA cryptosystem where there is very little restriction on the types of elliptic curves that can be used. A new cryptosystem based on elliptic curves over Z_n in which the message is held in the exponent instead of the group element was proposed by Vanstone and Zuccherato. The security of all these schemes is based on the difficulty of factoring n [18].

Rabin encryption scheme is a modification of the RSA cryptosystem where cryptograms are generated using the fixed public key k = 2, and $C = M^2$ (Mod N), where N is the modulus. A legal recipient, who knows the proper factorizing of N, can decrypt by computing two congruences, in Z_p and in Z_q, respectively, using the Chinese Remainder Theorem. Rabin's cryptosystem has the disadvantage that its encryption process is not one-to-one for all messages. There is 4:1 ambiguity in the decrypted message [22]. Williams presented a public-key encryption scheme similar to Rabin's but using composite integer n = pq with primes p ≡ 3 (mod 8) and q ≡ 7(mod 8). Williams' scheme also has the property that breaking it is equivalent to factoring n, but has the advantage over Rabin's scheme that there is an easy procedure for identifying the intended message from the four roots of a quadratic polynomial. However, a further work by Williams later removed the restrictions on the forms of the primes p and q [18].

Williams showed how to redefine Rabin's scheme to overcome most of the drawbacks. He has proved that the decryption process can be simplified for all messages M whose Jacobi symbol is: $\left(\frac{M}{N}\right)=1$

Where, primes are selected in such a way that:

P = -1(mod 4) and q = -1(mod 4), then the deciphering process is expressed by the following congruence:

$$C^k = \pm\ M(\text{mod } N)$$

Where, the secret key k = 1/2[1/4(p – 1)(q – 1) + 1]. In Williams' scheme, the receiver selects N using p = -1(mod 4) and q = -1 (mod 4) and a small integer S such that $\left[\frac{S}{N}\right]=-1.$ and publish N and S but keeps secret the key k [22]. William's further considered the cryptosystem where cryptograms are generated using the fixed public key k = 3, and $C = M^3$ (Mod N), where N is the modulus. He was able to show and proved that it is as difficult to break as it is to factor N.

Another modification of the basic RSA system for k ≡ 3 (modulus 18) have been presented by Khoo, Bird and Seberry. However, they recommended that their modification should be used for k, whose binary representation has several zeros. Their work is defined in the ring $Z(\omega)$ where ω is a primitive cube root. They also proved that it is as difficult to break as it is to factor N.

In RSA scheme, p and q should be almost the same bit lengths. Shamir proposed a variant of the RSA encryption scheme called unbalanced RSA, which makes it possible to enhance security by increasing the modulus size (e.g. from 500 bits to 5000 bits) without any deterioration in performance. In this variant, the public modulus n is the product of two primes p and q, where one prime (say q) is significantly larger in size than the other; plaintext messages m are in the interval (0, p-1) [18]. The computational equivalence of computing the secret key d, and factoring n was shown by Rivest, Shamir and Adleman, based on earlier work by Miller [18].

A system is computationally secure if the task of inverting the plaintext is computationally infeasible or traceable [22]. A trapdoor in the RSA cryptosystem was proposed by Anderson, whereby a hardware device generates the RSA modulus n = pq in such a way that the hardware manufacturer can easily factor n, but factoring n remains difficult for all other parties. However, Kaliski subsequently showed how to efficiently detect such trapdoors and, in some cases, to actually factor the modulus [18]. A number of works has been put forward by eminent scholars in the area of email security. The scope of their researches covers the same territory but with some differences in approach and technology.

An example of the use of cryptography in this regard is the PGP – Pretty Good Privacy scheme proposed for adding privacy to Internet mail applications. PGP was invented by Phil Zimmermann to provide all four aspects of security (Privacy, integrity, authentication and nonrepudation) in the sending of email [13]. PGP encrypts data by using a block cipher called IDEA (International Data Encryption Algorithm). It takes plaintext as input and produces signed cipher-text in base64 as output. The sender starts by invoking the PGP program on his/her computer. PGP first hashes the message using MD5, and then encrypts the resulting hash using his/her private RSA key. When the receiver gets the message, he/she can decrypt the hash with the public key of the sender and verify that the hash is correct. Even if someone else could acquire the hash at this stage and decrypt it with the sender's known public key, the strength of MD5 (Message Digest) algorithm guarantees that it would be computationally infeasible to produce another message with the same MD5 hash [24].

Like PEM, PGP generates and manages secret keys on behalf of a user and uses asymmetric encryption only to transmit secret keys to the intended communication partner. PEM uses both public and secret-key encryption - mail users obtain a public/private key pair from a local PEM program and publish the public key with their mail address. Each user relies on a local PEM program that maintains a small database of their keys. The PEM is available as an application program called RIPEM that uses a public-key encryption library called RSAREF produced by RSA Data Security Inc, under license from PKP (public key partners), a firm that owns a patent covering the RSA public key encryption method [8]. In [1] any cryptosystems, two fundamental assumptions are made as follows:

(i) The cryptanalyst (the intruder) knows the encryption algorithm;

(ii) The medium of transmission is insecure.

3.0.3 Cipher

A cipher is a character-for-character or bit-for-bit manipulation irrespective of the language structure of the message/data. In other words, a cipher is an algorithm for executing encryption and decryption. The following are some major ciphers: substitution, transposition, block and stream.

Substitution Cipher

Substitution cipher is when a letter or a collection of letters is replaced by another letter or collection of letters with the aim of scrambling it, usually in a preserved order of the plaintext.

Transposition Cipher

Transposition cipher maintains the characters of the plaintext but reorders its position to create the ciphertext. The text is structured into a matrix form whose columns are interchanged using a key. The substitution and transposition cipher are traditional ciphers.

Block cipher

Modern ciphers employ the use of block and stream ciphers. In block cipher, the unit of encryption/decryption is based on a block of bits.

A block cipher is an encryption scheme which breaks up the plaintext messages to be transmitted into strings (called blocks) of a fixed length t over an alphabet A, and encrypts one at a time [18].

-
- **Stream Ciphers**

Stream ciphers can be viewed as a block cipher with a block length equal to one. For any encryption transformation there must be change for each symbol of plaintext. Stream ciphers are useful where transmission errors are highly required because they do not propel errors. Stream ciphers are useful when plaintext must be encrypted one symbol at a time.

3.0.4 Encryption and Decryption

Encryption and decryption are the algorithms used for manipulating cryptographic schemes.

- **Encryption**

Encryption or enciphering is the scrambling of data/messages in some way to make it unreadable.

- **Decryption**

Decryption or deciphering is the unscrambling of data/messages in some way to make it readable. Decryption or deciphering is possible with keys that are related. A message read/sent across a network or communication channel is referred to as the plaintext whereas the encrypted message is the ciphertext.

Although, the transformation of encryption and decryption is the inverse, the private key system handles the data as a bit, but the public key system handles the data as a number that perform function operation and the mathematical function is one-way. It is to say, it can easily come true from one side, but very difficult to another side, so simple steps unable to decrypt the cipher text [27].

3.0.5 Components of Cryptography

Cryptography has three major components: cryptosystems, protocols and key management.

Cryptosystems

Cryptosystems is considered to be the collection of encryption and decryption systems, the key generator, as well as the protocols for key transmission [22]. The term cryptosystems is used to describe cryptographic algorithms and their characteristics.

Cryptographic Protocols

The term cryptographic Protocols, is used to describe the composition and application of cryptographic algorithms with regards to securing of a communications channel or information in a database.

A protocol is a series of steps taken to accomplish a task. In fact that is also the definition of an algorithm but we use algorithm to refer to the attainment of internal, mathematical results like encrypting a block, and protocol to refer to the attainment of user-visible results such as secret communication and digital signatures [25]. A Protocol is a set of rules and conventions that defines the communication framework between two or more agents. These agents, known as principals, can be end-users, processes or computing systems. Security related and cryptographic protocols are used to establish secure communication over insecure open network and distributed system. These protocols use cryptographic techniques to achieve a specific security objective. Unfortunately, open networks and distributed systems are vulnerable to hostile intruders who may try to subvert the protocol design goals [14].

- **Key Management**

The term key management is used to refer to the fundamental problems of creating, distributing, and storing keys.

4.0 Cryptographic Algorithms

A cryptographic algorithm is defined to be the mathematical description of the enciphering and deciphering processes together with the interrelation between their keys. Cryptographic algorithm is more software oriented [22].

4.0.1 Asymmetric Cryptosystems

Asymmetric cryptosystems involves two keys – a private key and a public key that are mathematically related. A message encrypted with one key can be decrypted only with the other. It is extremely difficulty to determine the value of one key by examining the other. In an asymmetric cryptosystem, the encryption key is different from the decryption key. The public key is often called the encryption key. Figure 1 shows an asymmetric cryptosystem. Typically, each participant in public key cryptosystem creates his own key pair. Then one member of the pair, called the private key, is kept secret never revealed to anyone else, whereas the other member of the key part, called the public key is distributed freely. Either key may be used for encryption or for decryption, but the most important point is that the private key never be revealed.

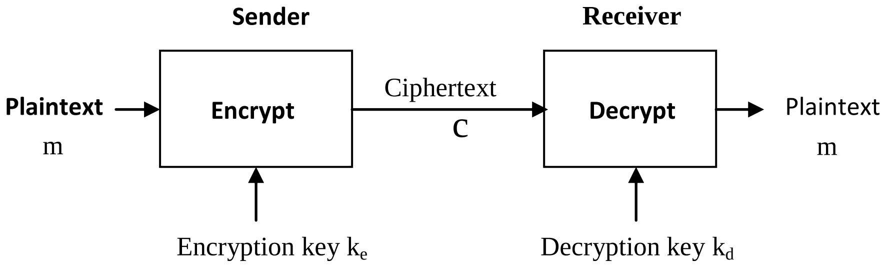


Fig. 1: Asymmetric cryptosystem

4.0.2 Functions of Asymmetric Cryptography

Asymmetric cryptography provides the following functions: privacy, authentication, integrity, and nonrepudiation A fundamental goal of cryptography is to adequately address these four functions in both theory and practice.

Privacy

Privacy is a secret message whose contents are known only by the sender and receiver. The recipient public key is used to encrypt the message and with the secret key in his possession, he can decrypt the message.

Authentication

Authentication arises when the receiver knows who sent the message and its genuineness and the sender knows that the message shall get to the intended recipient.

The recipient has the ability to authenticate the sender of the message by simply verifying a digital signature.

Integrity

Integrity arises when the receiver knows that the message was not corrupted or modified either deliberately or accidentally while in transit. Digital signature message offers message integrity. The encryption of the message is done with the sender's private key.

Nonrepudiation

The sender of the message cannot reject that the message did not originate from him/her. In asymmetric cryptography, the provision of nonrepudiation is possible using digital signatures.

An attack may have an adverse effect on one, or a combination of all these functions [15].

5.0 THE RSA ALGORITHM

The RSA scheme is a block cipher in which the plaintext and the ciphertext are integers between 0 and n-1 for some n [23].

1.0 THE RSA ALGORITHM

Algorithm for RSA Asymmetric Encryption

Y encrypts a plaintext m meant for X, and X decrypts it. Y follows the procedure in (a) and Y follows the procedure in (b):

(a) Encryption:

1. Get X's public key, (n, e).

Prepare the plaintext for computation in the interval, [0, n-1].

3. Compute c = m^e mod n.
4. Send encrypted text or cipher text c to X.

(b) Decryption:

X uses the private key, d, to compute:

m = c^d mod n (to recover message m).

The RSA scheme is a block cipher in which the plaintext and the ciphertext are integers between 0 and n-1 for some n [23].

1. RSA Algorithms for Secret
2. Communication

RSA algorithms for privacy for the existing system include: algorithm for key generation and algorithm for asymmetric encryption.

Algorithm for Key Generation

If communication must exist between two entities, X and Y, each entity must be capable of creating an RSA public key and a related private key. X follows the procedure as follows:

(a) Generate any two large prime numbers, p and q having approximately the same size.

(b) Compute n = pq and z = (p-1) (q-1).

(c) Compute public key, e, by choosing any number that is relatively, prime with z such that e has no common factors with z.

(d) Compute private key, d, by solving the equation: e x d = 1 (mod z).

(e) X's public key is (n, e) and X's private key is d. e, d are the encryption and decryption exponents, n is the modulus.

Where:

m is the original Message/Plaintext.
c is the Cipher text/ encrypted text.
e is the Encryption key.
d is the Decryption key.
n is the RSA modulus.

3. RSA Algorithm for Digital Signatures

RSA algorithms for digital signatures for the old system include: key generation, signature generation and verification. Algorithm for Key Generation is the same as in RSA algorithms for Secret Communication.

Algorithm for RSA Signature Generation and Verification

In a Digital Signature scheme, X can sign a plaintext $m \in M$. Y is capable of verifying X's signature and recover the plaintext m from the signature.

(a) **Signature Generations:**

To sign a message X follows the procedure as follows:

1. Compute $m = D(m)$.
2. Compute $s = m^d \bmod n$. **1.**
3. X's signature for the message, m is **2.** s.

(b) **Verification:**

Y can verify X's signature s and recovers the message m as follows: •

1. Get X's public key (n, e). •
2. Calculate $m = s^e \bmod n$.
3. Verify if $m \in M_D$ otherwise rejects Signature.
4. Compute $m = D^{-1}(m)$ to recover the message.

D is the redundancy function $D:M \quad Z_n$, $(D(m) = m$ for all $m \in M)$, s is the signature, M is the result of the redundancy function.

5.0.1 Secret Communication and Digital Signatures

Secret communication and digital signatures are cryptographic protocols. Protocols use cryptographic schemes to achieve a specific security objective. Protocols play a major role in cryptography and are essential in meeting cryptographic goals. Encryption schemes and digital signatures are some examples of protocols.

Secret Communication

Secret communication is a situation whereby a message is made secrete and only the sender and intended recipient knows the contents of the message.

Asymmetric Encryption

Asymmetric encryption is a secrete communication where a message is encrypted using the recipient's public key and only the intended recipient has the rightful private key to decrypt the message – it is known as privacy. Figure 2 shows an illustration of secure communication service for asymmetric cryptosystem.

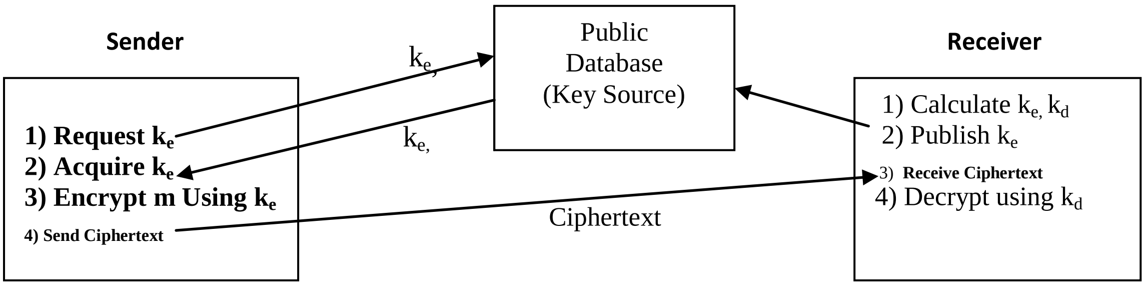
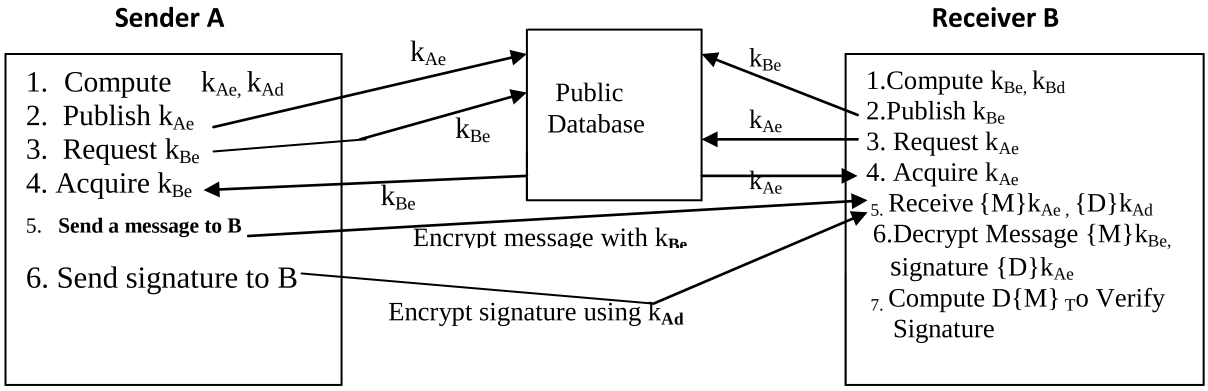


Fig. 2: Illustration of secure communication service for asymmetric cryptosystem

3. Digital Signatures

The concept of digital signature is not a new phenomenon. Digital signature was introduced by Diffie W. and Hellman M, over three decades ago in [10]. In asymmetric cryptosystems, we can achieve the following basic form of security: authentication, integrity, and nonrepudiation by using what is called digital signature.

A digital signature scheme is a public key algorithm that allows one to authenticate a message by means of a piece of information called the signature. The generation of the signature requires the knowledge of the signer’s private key, while for the verification of the signature, only the knowledge of the corresponding public key is necessary. If the public key is publicly accessible, then everybody can verify the signature, while only the signer, who known the private key, is able to sign. The purpose of a digital signature is to provide a means for an entity to bind its identity to a piece of information. Figure 3 shows an illustration of digital signature using asymmetric cryptosystems.



Sender A
Receiver B
1. Compute $k_{Ae,}$ k_{Ad}
2. Publish k_{Ae}
3. Request k_{Be}
4. Acquire k_{Be}
5. Send a message to B
6. Send signature to B
k_{Ae}
k_{Be}
k_{Be}
Public Database
Encrypt message with k_{Be}
Encrypt signature using k_{Ad}
k_{Be}
k_{Ae}
k_{Ae}
1.Compute $k_{Be,}$ k_{Bd}
2.Publish k_{Be}
3. Request k_{Ae}
4. Acquire k_{Ae}
5. Receive $\{M\}k_{Ae}$, $\{D\}k_{Ad}$
6.Decrypt Message $\{M\}k_{Be,}$ signature $\{D\}k_{Ae}$
7. Compute D{M} To Verify Signature

Fig. 3: Illustration of digital signature using asymmetric cryptosystems

6.0 The Security of RSA and Challenges

The security of RSA according to [23], has three possible approaches to attacking the RSA algorithm, these are stated as follows:

Brute-force: This involves trying all possible private keys

Mathematical attack: There are several approaches, all equivalent in effect to factoring the product of two primes.

Timing attacks

These depend on the running time of the decryption algorithm. The system structure of RSA algorithm is based on the number theory of the ruler. It is the most security system in the key systems. The safe of RSA algorithm bases on difficulty in the factorization of the larger numbers [30]. As a matter of fact, implementing high-security RSA on embedded systems is nowadays a difficult technological challenge, despite the steady hardware developments of the last years. Indeed, an important requirement for a practical cryptosystem is its speed. Whereas for specific applications a highly secure, yet slow cryptosystems can be used, for a general deployment a system must make reasonable use of the available resources such as memory, speed, bandwidth [5]. If any of the two prime factors of a participant’s public RSA-modulus can be found, then the private key of that participant can be found, and the system is considered to be broken. If the primes are properly chosen (that is large enough), then finding them given only their product (the RSA-modulus) is believed to be a computationally infeasible task. To make the system secure the primes must therefore be chosen sufficiently large. On the other hand, large primes imply a large RSA-modulus, which leads to substantial computational overhead when using the RSA system. Thus, in RSA there is a trade-off between security and efficiency: on the one hand moduli must be large for security; on the other hand small moduli are preferred for efficiency. How large they have to be, depends on the speed of socalled factorization algorithm [9].

7.0 Conclusion

In this study, we did a comprehensive review of public-key cryptosystems in general and RSA algorithm in particular. We found out that on the whole, the RSA algorithm is a good algorithm but its implementation has some challenges. One of such is the low speed of encryption and decryption compared with the symmetric cryptographic algorithm. The RSA cryptosystems relies on the difficulty of factoring very large numbers and if there is an algorithm that can decompose a large number fast, the RSA algorithm's security would be threatened.

The defence against the brute-force approach is the same for RSA as for other cryptosystems – namely, use a large key space. Thus, the larger the number of bits in e and d the better. However, because the calculation involved, both in key generation and in encryption/decryption, are complex, the larger the size of the key, the slower the system will run [23]. The RSA system has been shown to provide less security than initially believed. Still, RSA has remained unchallenged among the public key cryptosystems in terms of dissemination. [5]. Virtually all the major types of cryptography in use today rely on the use of one-way functions, mathematical functions that are easy to compute but impractical to invert, or reverse. For example, it is easy to multiply together two large prime numbers, but it is computationally impractical to reverse that by factoring the resulting product. That is the basis of RSA cryptography. Similarly, it is easy to compute $a = x^n$ given x and n, but hard to compute the discrete logarithm n given a and x.

The "discrete logarithm problem" is the basis for a number of cryptosystems, such as the Diffie-Hellman protocol and elliptic curve cryptography [4]."In the 21st century, even the most secure isolated systems have been penetrated [32].With the year-on-year increase of the amount of data and the continuous improvement of people's needs, RSA faces various challenges, application security, data security and privacy, cloud security, denial of service attacks, Advanced Persistent Threats (APTs), mobile security and so on. There are the prospects of the development in the few years [33].

References

[1] Adewumi, S. E., Garba, E. J. D., (2002), Data Security: A Cryptosystems Algorithm Using Data Compression and Systems of Non-Linear Equations, COMPUTER Association of Nigeria Conference Series, Volume 13, 200-221.

[2] Alese, B. K., Philemon, E. D., Falaki, S. O. (2012), Comparative Analysis of Public-Key Encryption Schemes, International Journal of Engineering and Technology Vol. 2, No. 9, Sept., pp. 1552 – 1568.

[3] Almarini, A. and Alsahdi, U. (2012), Developing a Cryptosystem for XML Documents,
International Journal of Information Science, Vol. 2. No. 5, pp. 65 – 69.

[4] Anthes, G. (2014), French Team Invents Faster Code-Breaking Algorithm, Communications of the ACM, Vol. 57 No. 1, Pages 21-23, **http://cacm.acm.org/magazines/2014/1/170850-french-team-invents-faster-code-breaking-algori, accessed Feb. 2014.**

[5] Avanzi, R., Ockle, G. B., Braeken, A., Cid, C., Geissler, K., Granger, R., Lange, T., Lenstra, A. K., Nguyen, P. Q., Preneel, B., Sendrier, N., Smart, N. P., Stam, M., Stern, J., Wolf, C. (2005), Alternatives to RSA (Lightweight Asymmetric Cryptography and Alternatives to RSA), The IST program under Contract IST-2002-507932,

[6] Avolio, M. F., (1994), Network Security: Building Internetwork Firewalls, Business Communications Review January (http://www.avolio.com)

[7] Chaum, D. (1981), Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Communications of the ACM Feb. 1981 volume 24, No. 2, 1-9, (http://world.std.com/crypto./chaum-acm-1981.html)

[8] Coulouris, G., Dollimore J., and Kindberg T. (1994), Distributed systems, Concepts and Design, Addison-Wesley Publishing Company, USA., Second Edition, 490 - 492.

[9] De, S. Haldar, A., and Biswas, S. (2013), A Review on Recent Trends in Cryptography, International Journal of Latest Research in Engineering and Computer (IJLREC), Vol.1, Issue 1.Sept- Oct., pp. 50-55.

[10] Diffie, W, and Hellman, M., (1976), New Directions in Cryptography, IEEE Trans, Info. Theory, 644-654.

[11] Donghua, X., Chenghnuai, L., and Andre, D. S., (2002), Protecting Web Usages of Credit Cards using One-Time Pad Cookie Encryption, IEEE computer society, proceeding the 18th Annual Computer Security Applications Conference (ACSAC'02).

[12] Douceur, R. J., Adya, A., Benaloh, J., Bolosky, J. W., and Yuval, G., (2002), A secure Directory Service based on Exclusive Encryption, IEEE Computer Society, Proceeding of the 18th Annual Computer Security Application Conference (ACSAC'02).

[13] Forouzan, A. B. and Fegan, S. C., (2004), Data Communication and Networks, Tata McGraw-Hill Publishing Coy Limited, New Delhi, Third Edition, 848 - 849.

[14] Gritzalis S., Spinellis D., Georgiadis P., (1999): Security Protocols Over Open Networks and Distributed Systems: Formal Methods for their Analysis, Design, and Verification, Computer Communications 22 (8); May, 695-707.

[15] Haggerty, J., Shi Q., Merabti M., (2002), **B**eyond the Perimeter: The Need for Early Detection of Denial of Service Attacks, IEEE Computer Society, Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC'02).

[16] Huang, Y., Rine, D., and Wang, X., (2001), A JCA-based Implementation Framework for Threshold Cryptography, IEEE Computer Society, Proceedings of the 17th Annual Computer Security Conference (ACSAC'01).

[17] Menezes, A., Oorschot, P. V., and Vanstone S., (1996), Handbook of Applied cryptography, CRC Press Inc, (Http//:www. cacr.math.uwaterloo.ca/hac

[18] Menezes, A, Oorschot, P. V. and Vanstone S., (1997), Handbook of Applied Cryptography, CRC Press Series on Discrete Mathematics and its Applications, CRC press.

[19] Oyeyinka, I. and Obianyo-Agu N., (2002), Security and Encryption Techniques in the GSM NETWORKS, COMPUTER Association of Nigeria Conference Series, Volume 13, 136-142.

[20] Rivest, R. L., Shamir, A., and Adleman, L., (1978), A Method for Obtaining Digital Signature and Public-key Cryptosystems, Communications of the ACM, Feb., 21:120-126.

[21] Schneier, B., (1997), Why Cryptography is Hard that it looks, Counterpane Internet Security Inc., 1- 4, (http://www.schneier.com/essay-037.html.).

[22] Seberry, J. and Pieprzyk, J., (1998), Cryptography: An Introduction to Computer Security, Prentice Hall of Australia Pty Ltd.

[23] Stalling, W. (1999), Cryptography and Network Security: Principles and Practice, 2nd (Ed.), Printice-Hall Inc., New Jersey, USA, Pp. 163-182.

[24] Tanenbaum A. S., (2005): Computer Networks, Prentice-Hall of India Private Limited, New Delhi, Fourth Edition, 799-804.

[25] Treese G. W., and Stewart C. L., (1998), Designing Systems for Internet Commerce, Addison Wesley Coy.

[26] Walsh, M. L. (2003), Moving Beyond, Information Security, Sept., 1-96.

[27] Wang, H. and Song, R. (2011). The length of the key influences the degree of security of the RSA system. Comput. Knowledge Technol., 10: 7104-7105.

[28] Wikipedia, Public-key Cryptography, the free encylclopedia, http://en.wikipedia.org/wiki/secure computing, accessed May, 2012.

[29] Zacker, C. (2001): Networking: The Complete Reference, Osborne/McGraw-Hill, USA.

[30] Zhang, Y. and Cao, T. (2011). Application of encryption based on RSA algorithm. Sci. Technol. Advisory (Technol. Admin.), 25: 79-80.

[31] Chen, C. and Zhu, Z. (2006). Application of RSA algorithm and implementation details.
Comput. Eng. Sci., 9: 13-14.

[32] Kerner, S. M. (2013), RSA 2013: Is Cryptography Still Necessary? **http://www.esecurityplanet.com/network-security/rsa-2013-is-cryptography-still-necessary.html**, accessed Feb. 2014.

[33] Na**a**Qi, Wei Wei, Jing Zhang, Wei Wang, Jinwei Zhao, Junhuai Li, Peiyi Shen, Xiaoyan Yin, Xiangrong Xiao and Jie Hu, (2013). Analysis and Research of the RSA Algorithm. *Information Technology Journal, 12: 1818-1824,* **DOI:** 10.3923/itj.2013.1818.1824, **http://scialert.net/abstract/?doi=itj.2013.1818.1824,** accessed Feb. 2014.