Journal of Modern Technology and Engineering
Vol.7, No.3, 2022, pp.233-241

Jomard Publishing

HYBRID APPROACHES IN CRYPTOGRAPHY

Nargiz Khankishiyeva Hati*

Ege University, Faculty of Science, Department of Mathematics, Izmir, Turkiye

Abstract. Different encryption methods that emerged with the development of cryptology have different advantages and disadvantages in terms of speed and security level. The importance of cryptography in this position is to reveal the advantages of encryption techniques by using them at the right time. In other words, the time of use and their management are as important as the strength of encryption algorithms. In this part hybrid encryption schemes come into play. Hybrid encryption schemes provide safer and faster data transmission by using the advantages of different encryption schemes on appropriate time. In this study, the reasons for the emergence of hybrid encryption schemes will be examined and the new hybrid encryption scheme will be mentioned. The new hybrid architecture consists of the implementation of the new encryption scheme and RSA, which is one of the asymmetric encryption schemes.

Keywords: Cryptology, RSA, Nuriyev Number System, Hybrid Encryption Scheme.
***Corresponding author:** Nargiz Khankishiyeva Hati, Ege University, Faculty of Science, Department of Mathematics, Izmir, Turkiye, e-mail: *nargizkhankishiyeva@gmail.com*
Received: 12 July 2022; Revised: 15 September 2022; Accepted: 23 October 2022;
Published: 29 December 2022.

1 Introduction

Cryptology is the science that learns methods to exchange data between two institutions in a way that only the targeted institutions can understand (Katz & Lindell, 2014). The importance of cryptology is increasing in terms of the secure transfer, storage of increasing data of governments, institutions or individuals with the development of technology (Stallings, 2011). Encryption methods which started from ancient times, have taken different forms until today (Schneier, 1996). The first encryptions started by assigning numerical values to letters and encrypting them (Hoffstein et al., 2008). Each encryption method has been replaced by more advanced encryption systems when its weaknesses emerged. Developing encryption systems provide more secure data transfer of communication technologies with the effect of number theory (Koblitz, 1994). These encryption systems are divided into two types as symmetric and asymmetric (Cormen et al., 2001). In this article, the advantages and disadvantages of both encryption systems will be revealed and hybrid encryption systems that only use their advantages, and finally the new hybrid encryption system included in this list, will be mentioned.

2 Encryption Algorithms

- Symmetric Encryption Algorithms
  - ◇ Hash Algorithms
- Asymmetric Encryption Algorithms
- Hybrid Algorithms

Symmetric encryption algorithms use the same key for encryption and decryption. The key is sent before communication is established between the sender and receiver. The problem of sending the key is considered a disadvantage of these algorithms and this makes the algorithms less resistant to attacks. The advantage of these algorithms is being fast. In addition, such encryption systems use simple translation, displacement and XOR operations to perform the encryptions process. AES (Advanced Encryption Standard), DES (Data Encryption Standard), Blowfish are symmetric encryption algorithms (Katz & Lindell, 2014).

Asymmetric encryption algorithms use two different keys for encryption and decryption. The key used for encryption is public and the other key used for decryption is known only to the receiver. Such encryption systems do not have a problem with sending keys, key generation algorithms are slow algorithms, because they rely on mathematical operations that take a long time to solve. RSA, El Gamal, ECC (Elliptic Curve Cryptography) are among the asymmetric encryption algorithms (Katz & Lindell, 2014).

A hash function takes text of any length as the input and produces a fixed length value as a result. This value is called the message digest (Schneier, 1996).

Since we will use the RSA algorithm in the following sections, let's give detailed information about the RSA encryption algorithm.

2.1 RSA Key Generation

RSA key generation is done with the following algorithms:

1. Two large prime numbers p and q are produced, with the same size. The reason why it is chosen large is that prime numbers are hundreds of digits. Therefore, factoring $p * q$ will be very difficult. This creates the security of the encryption scheme.

2. $n = p * q$ and $\varphi = (p-1) * (q-1)$ multiplications are calculated.

3. Random number e is chosen from the interval $1 < e < \varphi$ such that gcd (e,f)=1.

4. Number d is calculated from the interval $1 < d < \varphi$ such that $ed \equiv 1\ (mod\ \varphi)$.

5. Public key is (n, e), private key is d.

RSA Public Key Generation: The encryption and decryption operations are done according to algorithms below.

Encryption:

1. The public key (n, e) of the message receiver is obtained.

2. The message which will be decrypted has to be converted to a number m from the interval $[0,\ n-1]$.

3. $c = m^e\ mod\ n$ is computed.

4. The generated encryption message c is sent to the receiver.

Decryption:

1. The private key d is calculated by $m = c^d\ mod\ n$ and the original message is obtained.

The RSA algorithm is a very useful and important encryption method, but there is a disadvantage that this encryption system includes both public and private key encryption methods. While large data are encrypted RSA slows down because of these reasons (Nabiyev, (2016).

3 Hybrid Encryption Architecture

Hybrid encryption systems are encryption techniques formed by eliminating the shortcomings of symmetric and asymmetric algorithms and combining their superior features. These encryption systems are encryption techniques that combine two types together.

Key security, which is the disadvantage of symmetric algorithms, is the strongest feature of asymmetric algorithms. However, this feature gives slow performance to asymmetric algorithms which becomes the biggest disadvantage for them, but it makes symmetric algorithms fast on the contrary. The encryption process of symmetric algorithms is based on simple mathematical operations, while the encryption process of asymmetric algorithms is based on mathematical problems that are difficult to solve. For example, in the RSA encryption scheme numbers must be prime factored. The biggest reason for the security in the RSA encryption system is that it requires a long and difficult process to factor large composite number being the product of two large prime numbers (Arjen, 2000).

Public key encryption schemes usually have restricted message spaces, meaning that each ciphertext can hide only a limited amount of plaintext bits. This greatly limits their application since in practice one typically wants to efficiently encrypt large amounts of data. One way of solving this problem is by using a hybrid encryption scheme consisting of a public key part to encrypt the actual data (Herranz et al., 2006).

Hybrid encryption systems have emerged to eliminate the disadvantages of these two types of algorithms and combine their strengths. The hybrid encryption scheme provides key security by using asymmetric algorithms to encrypt keys, thus eliminating the key security disadvantage of symmetric encryption systems. Hybrid schemes are very secure, because asymmetric algorithms are very secure. The slowness of asymmetric encryption schemes does not affect hybrid schemes. Because the length of the keys is not long. On the other hand, symmetric algorithms are very fast at encrypting large data, so hybrid schemes are also fast.

Let's take a look at some of the hybrid encryption schemes below.

3.1 KEM/DEM

In this hybrid scheme mechanism managing encryption key is called KEM/ Key Encapsulation Mechanism, mechanism that encrypts data is called DEM/ Data Encapsulation Mechanism. In this hybrid mechanism security is ensured by encrypting the data encryption key using KEM, which data encrypted by this encryption key using DEM. For the first part one uses KEM to produce a random symmetric key K together with a ciphertext. For the second part this symmetric key K is then used to encrypt the data using a highly efficient DEM. This popular approach is often referred to as the "KEM/DEM paradigm" and was first formalized by Cramer and Shoup (Herranz et al., 2006).

A KEM consists of three algorithms:

1. A probabilistic, polynomial-time key generation algorithm, *Gen*, which takes as input a security parameter 1^k and outputs a public/private key pair (*pk; sk*).

2. A probabilistic, polynomial-time encapsulation algorithm, *Encap*, which takes as input a public key *pk*, and outputs a key K and an encapsulation of that key C. We denote this as *(C; K) = Encap(pk)*.

3. A deterministic, polynomial-time decapsulation algorithm, *Decap*, which takes as inputs the private key *sk* and an encapsulation C, and outputs a symmetric key K or the error symbol $\perp$. We denote this as $K = Decap(sk; C)$.

A DEM is a pair of algorithms consisting of:

1. A deterministic, polynomial-time encryption algorithm, Enc, which takes as input a message $m \in \{0,\ 1\}^*$ of any length and a symmetric key K of some pre-determined length. It outputs an encryption $C\ =\ EncK(m)$.

2. A deterministic, polynomial-time decryption algorithm, Dec, which takes as input an encryption $C \in \{0,\ 1\}^*$ and a symmetric key K of some predetermined length, and outputs either a message $m \in \{0,\ 1\}^*$ or the error symbol $\perp$. Let's denote this as $m = Dec_K(C)$.

3.2 Tag-KEM/DEM

In this mechanism, the tag needs to be created before the DEM key is selected, and it needs to identify the encrypter. The encryption function takes the tag as an input and output for the key of the DEM. In this model, the encryption function is divided into two functions: The first one selects a random key and the second one encrypts the key along with a given tag (Abe et al., 2005).

A Tag-KEM consists of three algorithms:

1. A probabilistic algorithm that generates public-key pk and private-key sk. The public-key defines all relative spaces, i.e., spaces for tags and encapsulated keys denoted by T and K_K. Let's denote this like $TKEM.\ Gen\,(1^n) = (pk,\ sk)$.

2. A probabilistic algorithm that outputs one-time key $dk \in K_D$ and internal state information ω. K_D is the key-space of DEM. Let's denote this like $TKEM.\ Key(pk) = (\omega, dk)$.

3. A probabilistic algorithm that encrypts dk (embedded in ω) into ψ along with τ, where τ is called a tag.

4. A decryption algorithm that recovers dk from ψ and τ. For soundness, $TKEM.\ Decsk\,(\psi,\ \tau) = dk$ must hold for any sk, dk, ψ, and τ, associated by the above three functions. The algorithm can also output special symbol $\perp \in K_D$ to present abnormal termination.

3.3 Fujisaki-Okamoto Hybrid Scheme

This system was made with the aim of eliminating the weak aspects of KEM/DEM. The Fujisaki-Okamoto scheme works by applying the Fujisaki-Okamoto transform using hash functions (Lippert, 2014).

3.4 Scrabbled KEM/DEM, Cascaded KEM/DEM and Combined KEM/DEM algorithms

In a study conducted by Kerim Yıldırım and H. Engin Demiray, new algorithms were introduced by eliminating the shortcomings of KEM/DEM. In this study, scrabbled KEM/DEM, cascaded KEM/DEM and combined KEM/DEM algorithms were proposed (Yıldırım & Demiray, 2008).

3.5 PGP (Pretty Good Privacy)

PGP is a technique that combines the advantages of symmetric and asymmetric systems. This method transmits and stores data by compressing them. After compression, session key part works. This key is a part random number and consists of random mouse movements and keys pressed by the user. Session key encrypts plaintext with very secure and fast symmetric key algorithm. After this encryption, it is also encrypted using a public key. The decryption of encrypted data also works in reverse. First, the session key is decrypted with the private key. Then the encrypted data is decrypted. This algorithm runs 1000 times faster than the public key algorithm. It provides solutions to key sharing and data transmission problem and can be applied safely (Yıldırım, 2006).

3.6 S/MIME (Secure/ Multipurpose Internet Mail Extensions)

S/MIME is the protocol used by e-mail applications to transmit digitally signed and encrypted e-mail (Levi, 2003).

3.7 SSL (Secure Socket Layer)

SSL is the infrastructure used by internet browsers. It is mostly used by e-commerce sites, especially banks. It provides a secure communication environment in the transfer of information between the server and the client with 128-bit encryption (Gençoğlu, 2017).

3.8 RSA/AES

In the paper named "The hybrid encryption algorithm of lightweight data in cloud storage", firstly, the RSA algorithm was improved in the cloud environment by increasing the length of the RSA key to an extent that it can quickly generate big primes. Then, AES and RSA algorithms were merged on the basis of the improved RSA algorithm. This is called a hybrid encryption algorithm which is suitable for security of the lightweight data in cloud storage environment in order to further enhance the confidentiality of data in the cloud (Chengliang, 2016).

3.9 Kurosawa-Desmedt Hybrid Encryption

PPPS (Password-Protected Secret Sharing) is a secret sharing scheme that ensures only the owner of the secret who knows correct password to get the original secret by applying password authentication to partial information. In this paper, a new PPPS model was proposed which use Kurosawa-Desmedt hybrid encryption, that is proven to be CCA secure in the standard model. Proposed PPPS is constructed by combining public key part of Kurosawa-Desmedt hybrid encryption with password authentication (Arai & Obana, 2016).

3.10 AES/ECC

In the paper named "A Novel Idea on Multimedia Encryption using Hybrid Crypto Approach", a new hybrid encryption scheme was proposed which is intended to provide security to a variety of multimedia data ranging from images, video, audio etc. This hybrid encryption model makes use of two algorithms, AES (Advanced Encryption Standard) and ECC (Elliptic Curve Cryptography). Firstly, multimedia is converted into a base64 encoded version in text format, the same is then subjected to an initial encryption using AES keys. For the second part of security, the AES keys are encrypted using ECC public key, the keys which are generated from the input base64 encoded text file. Such a hybrid model of encryption provides a much better level of security as compared to a single model applied individually (Iyer et al., 2016).

3.11 "Hybrid data compression and optical cryptography with orthogonal matching pursuit"

In this work, compressive sensing (CS) is achieved with the orthogonal matching pursuit (OMP) algorithm. Then, the CS-OMP algorithm is combined with the double random phase encryption (DRPE) method to achieve both compression and encryption of data. In order to achieve high security, the keys used in CS and DRPE are transmitted to the receiver by an asymmetric cryptography method. Thus, the overall cryptographic system is a hybrid optical system (both symmetric and asymmetric) since DRPE is a symmetric optical encryption method (Atar et al., 2017).

3.12 "Implementing a hybrid crypto-coding algorithm for an image on FPGA"

In this work, an idea for the operation of hybrid model on FPGA was proposed. This hybrid architecture consists of encryption scheme and error correction encoding scheme (Srividya & Akhila, 2018).

3.13 Nuriyev Number System

In the number system are symbolized by N^k, $k = 1,\ 2,\ 3,\ \ldots$ describes bases of this system. This number system is non-positional and there is not a zero in this number system (Nuriyev et al. 2016). The set of digits are $0, 1$. The general formula for the number system is as follows:

$$\left(\underbrace{\underbrace{0...0}_{k}\underbrace{0...0}_{k}...\underbrace{a_{k-1}...a_0}_{k}}_{m}\right)_N^k = \left(\left(\frac{m}{k}-1\right)\cdot\left(2^k-1\right)+...\left(a_{k-1}\cdot 2^{k-1}+...a_1\cdot 2^1+a_0\right)\right)$$

If $k = 1$, numbers in the number system N^1 is:

$$1_N^1 = 1$$

$$0_N^1 = 1+$$

$$(01)_N^1 = 1+1 = 2$$

$$(001)_N^1 = 1+1+1 = 3, ...$$

If $k = 2$, numbers in the base N^2 is:

$$(01)_N^2 = 1$$

$$(10)_N^2 = 2$$

$$(11)_N^2 = 3$$

$$(00)_N^2 = 3+$$

$$(0001)_N^2 = 3+1 = 4$$

$$(0010)_N^2 = 3+2 = 5$$

$$(0011)_N^2 = 3+3 = 6$$

$$(0000)_N^2 = 3+3+ = 6+...$$

4 A New Hybrid Encryption Scheme

This hybrid scheme is designed for encryption of binary images. The mechanism of this hybrid scheme consists of encoding the sequence numbers of repeating symbols in binary data by over and over writing corresponding equivalents of those numbers in different bases of the number system N^k ($k = 1,\ 2,\ 3,\ \ldots$) . The bases used in the encryption operation form the private key of this encryption scheme. For example, if the data is encoded in bases $N^4,\ N^3,\ N^5$ respectively, the encryption key is 435 (Nuriyeva & Karatay, 2017).

Let's encrypt the data expressed in binary bits below with the proposed encryption scheme:

11111000011100000001000011011111111

Here, let's first write consecutive numbers of 0 and 1 in the data:

$$\underbrace{11111}_{5}\underbrace{0000}_{4}\underbrace{111}_{3}\underbrace{0000000}_{7}\underbrace{1}_{1}\underbrace{0000}_{4}\underbrace{11}_{2}\underbrace{0}_{1}\underbrace{111111111}_{9}$$

Consecutive numbers:

$$543714219$$

Let's write the equivalents of these consecutive numbers in bases $N^3,\ N^4,\ N^5$ respectively.

The equivalent of these numbers in base N^3 is as follows:

$$5_N^3 = 101,\ 4_N^3 = 100,\ 3_N^3 = 011,\ 7_N^3 = 111,\ 1_N^3 = 001,\ 2_N^3 = 010,\ 9_N^3 = 000010.$$

If the consecutive numbers are replaced with their equivalents in the base N^3, the new form of the data will be as follows:

$$101100011111001100010001000010$$

Consecutive numbers of the symbols in new data are written again:

$$\underbrace{1}_{1}\underbrace{0}_{1}\underbrace{11}_{2}\underbrace{000}_{3}\underbrace{11111}_{5}\underbrace{00}_{2}\underbrace{11}_{2}\underbrace{000}_{3}\underbrace{1}_{1}\underbrace{000}_{3}\underbrace{1}_{1}\underbrace{0000}_{4}\underbrace{1}_{1}\underbrace{0}_{1}$$

$$11235223131411$$

The equivalent of these numbers in base N^4 is as follows:

$$1_N^4 = 0001,\ 2_N^4 = 0010,\ 3_N^4 = 0011,\ 4_N^4 = 0100,\ 5_N^4 = 0101.$$

If the consecutive numbers are replaced with their equivalents in the base N^4, the new form of the data will be as follows:

$$0001000100100011010100100010001100010011000101000001000 1$$

Consecutive numbers of the symbols in new data are written again:

$$\underbrace{000}_{3}\underbrace{1}_{1}\underbrace{000}_{3}\underbrace{1}_{1}\underbrace{00}_{2}\underbrace{1}_{1}\underbrace{000}_{3}\underbrace{11}_{2}\underbrace{0}_{1}\underbrace{1}_{1}\underbrace{0}_{1}\underbrace{1}_{1}\underbrace{00}_{2}\underbrace{1}_{1}\underbrace{000}_{3}\underbrace{1}_{1}\underbrace{000}_{3}\underbrace{11}_{2}\underbrace{000}_{3}\underbrace{1}_{1}\underbrace{00}_{2}\underbrace{11}_{2}\underbrace{000}_{3}\underbrace{1}_{1}\underbrace{0}_{1}\underbrace{1}_{1}\underbrace{00000}_{5}\underbrace{1}_{1}\underbrace{000}_{3}\underbrace{1}_{1}$$

$$3131213211112131323122311151 31$$

The equivalent of these numbers in base N^5 is as follows:

$$1_N^5 = 00001,\ 2_N^5 = 00010,\ 3_N^5 = 00011,\ 5_N^5 = 00101$$

If the consecutive numbers are replaced with their equivalents in the base N^5, the new form of the data will be as follows:

$$0001100001000110000100010000010001100010000010000100001000010001000100000100011$$
$$0000100011000100001100001000100001000011000010000100001001010000100011000 01$$

The encryption key of this example is 345 and this encryption key is sent to the receiver by asymmetric encryption scheme RSA. The decryption key is designed by reading the encryption key in reversed order. In this example, the given encryption key 345 is converted to 543 decryption key for the receiver. Then, the data is decrypted by decoding input first in N^5, then in N^4 and finally in N^3 in order to get original data. Because of the way encryption and decryption key created, this scheme is called symmetric encryption scheme. Since both symmetric and asymmetric algorithms are used here, the new encryption scheme is a hybrid encryption scheme. Since the RSA algorithm is a very secure algorithm, this encryption scheme is also a secure hybrid scheme.

5 Conclusion

In this paper, the advantages and disadvantages of both symmetric and asymmetric algorithms are revealed and it has mentioned that hybrid encryption schemes created by combining symmetric and asymmetric algorithms, can provide more safety data transfer by implementing those advantages of symmetric and asymmetric algorithms on the appropriate time. The importance of this study is to show the advantages of hybrid encryption schemes and that there can be created more powerful algorithms combining most powerful algorithms. Later, many of the hybrid encryption techniques were analyzed and finally the new hybrid encryption scheme combined the new encryption scheme and the asymmetric RSA algorithm, was mentioned. The new encryption technique we use in the new hybrid encryption scheme is a very fast algorithm since it is symmetrical and RSA ensures that the key of this symmetric scheme reaches the recipient securely. That means the new hybrid encryption scheme is a hybrid architecture that is efficient in terms of speed and security.

References

Abe, M., Gennaro, R., Kurosawa, K., & Shoup, V. (2005, May). Tag-KEM/DEM: A new framework for hybrid encryption and a new analysis of Kurosawa-Desmedt KEM. In *Annual international conference on the theory and applications of cryptographic techniques* (pp. 128-146). Springer, Berlin, Heidelberg.

Atar, E., Ersoy, O.K., & Özyilmaz, L. (2017). Mobile Compatible Multi-Language Supported Hybrid Encryption Algorithm. *Journal of the Faculty of Engineering and Architecture of Gazi University*, *32*(1), 139-147.

Arai, T., Obana, S. (2016, November). A password-protected secret sharing based on kurosawa-desmedt hybrid encryption. In *2016 Fourth International Symposium on Computing and Networking* (CANDAR) (pp. 597-603). IEEE.

Arjen, K.L. (2000). *Integer Factoring, Designs, Codes and Cryptography.* Kluwer, Academic Publishers, 19, 101–128.

Chengliang, L., Ning, Y., Malekian, R., & Ruchuan, W. (2016). The Hybrid Encryption Algorithm of Lightweight Data in Cloud Storage, *2nd International Symposium on Agent, Multi-Agent Systems and Robotics (ISAMSR) Agent, Multi-Agent Systems And Robotics (ISAMSR), 2016 2nd International Symposium*, August, pp 160-166.

Cormen, T.H., Leiserson, C.E., Rivest, R.L. & Stein, C. (2001). *Introduction to Algorithms.* The MIT Press, Cambridge, 1180 p.

Gençoğlu H. (2017). Hybrit Encryption. PhD Thesis, Trakya University Institute of Natural Sciences, 103 s.

Herranz, J., Hofheinz, D., & Kiltz, E. (2006). KEM/DEM: Necessary and Sufficient Conditions for Secure Hybrid Encryption. IACR EPrint Archive, August 8, 31 p.

Hoffstein, J., Pipher, J., & Silverman, J.H. (2008). *An Introduction to Mathematical Cryptography.* Springer Science + Business Media, LLC, 538 p.

Iyer, S.C., Sedamkar, R.R., & Gupta, S. (2016). A Novel Idea on Multimedia Encryption Using Hybrid Crypto Approach, *7th International Conference on Communication, Computing and Virtualization 2016, Procedia Computer Science 79,* pp.293-298.

Katz, J., Lindell, Y. (2014). *Introduction to Modern Cryptography.* Chapman and Hall/CRC, 498 p.

Koblitz, N. (1994). *A Course in Number Theory and Cryptography.* Springer-Verlag, New York, 238 p.

Levi, A. (2003). What Kind of E-Mail Security?. Bilisim Security, March/April, pp.38-40.

Lippert J. (2014). Fujisaki-Okamoto Transformation. Bachelor's Thesis, Paderborn University, November 22, 53 p.

Nabiyev, V.V. (2016). *Algorithms. From Theory to Practice.* Seçkin Publishing, Ankara, 871 p.

Nuriyeva, F., Karatay, M. (2017). On the analysis of an encryption scheme. *Theoretical and Applied Aspects of Program Systems Development*, 04-08 December, Kiev, Ukraine, pp.34-39.

Nuriyev, U., Nuriyeva, F., Sadık, T. (2016). On a New Number System. *Proceeding of the International Conference on Computer Science and Engineering*, UBMK 2016), Kemal University, Tekirdag, Turkey, October 20-23, pp 825-827.

Srividya, B.V., Akhila, S. (2018). Implementing A Hybrid Crypto-Coding Algorithm for An Image on FPGA. *Information and Communication Technology for Intelligent Systems, ICTIS 2017. (Smart Innovation, Systems and Technologies,* 84, pp.72-84.

Stallings, W. (2011). *Cryptography and Network Security: Principles and Practice.* Upper Saddle River: Pearson, 765 p.

Schneier, B. (1996). *Applied Cryptography.* Second Edition: Protocols, Algorithms, and Source Code in C, 2nd Edition, John Wiley & Sons, Inc, 1027 p.

Yıldırım, K., Demiray, H.E. (2008). Methods for integrating symmetric and asymmetric encryption schemes: scrambled and combined KEM-DEM. *J. Fac. Eng. Arch. Gazi Univ., 23*(3), 539-548.

Yıldırım, K. (2006). Aplication of symmetric and asymmetric encryption algorithms used in data security (Hybrid Encryption). Master's Thesis, Kocaeli University Institute of Science and Technology, 90 p.