A REVIEW PAPER ON DES, AES, RSA ENCRYPTION STANDARDS

Aljaafari Hamza[1], Dr Basant Kumar[2]

[1]Deptt. of Computer Sc, Modern Collage of Business Studies, Muscat, Sultanate of Oman,
[2]Deptt of Computer Sc, Modern College of Business & Sc, Muscat, Sultanate of Oman,

Abstract—Cryptography is wide domain with many subs. The objective of this review paper is to give light review for readers and students of the three common used algorithm two in symmetric cryptography DES, AES and one in asymmetric cryptography RSA. Allowing the reader to have simple understanding of the background history of the algorithm in review and the key functional cipher operation of the algorithm. Accordingly summary of strength and weakness of each algorithm under the review will be highlighted. And how the security goals is such confidentiality and integrity are achieve using the mentioned algorithms. The paper will sequentially list and review the said algorithms and clarify the relational between them. Such as the relation between the symmetric and asymmetric algorithm the one with secret key and the ones with key pairs. The paper may insight some of the research window for upcoming scholar research in the field of cryptography.

I. INTRODUCTION TO CRYPTOGRAPHY

The information security triad is based in three main angles availability, integrity and confidentiality (1).The goal of cryptography is to cover the major portion of integrity and confidentiality in different application such public and private algorithms, Key distribution management for confidentiality of stored and transmitted data, digital signature for authenticity of electronic transactions activities and for non-repudiation conformities. Citing reference (1) the word cryptography is based on the Greek words “kryptos” that is means (hidden) & “grafi” which means (writing). So for us IT and cybersecurity professional cryptography is the mathematical equations to manipulate piece of information that help to prevent and protect the information from being disclosed or altered from it is original and intended use. Data can be approach wither in transit or in rest therefore cryptography provides the means for confidential transmission of data, and provides the means of confidential for storing data. There are many terms are used in the cryptography science some of which will be used in this paper such as (plaintext/cleartext-Vs-ciphertext/cryptogram), (encrypt/encipher-Vs-Decipher/decrypt/decode) and so on. Cryptography science and techniques goes way back were the earliest example of cryptograph date back set of ancient Egyptian hieroglyphics from approximately 2000 BC. That were using a simple substitution algorithm (1).as our paper will be very much limited to briefly review the DES,AES,RSA encryption standards. The below figure illustrate the hierarchy of the RSA, DES, AES standards under review:

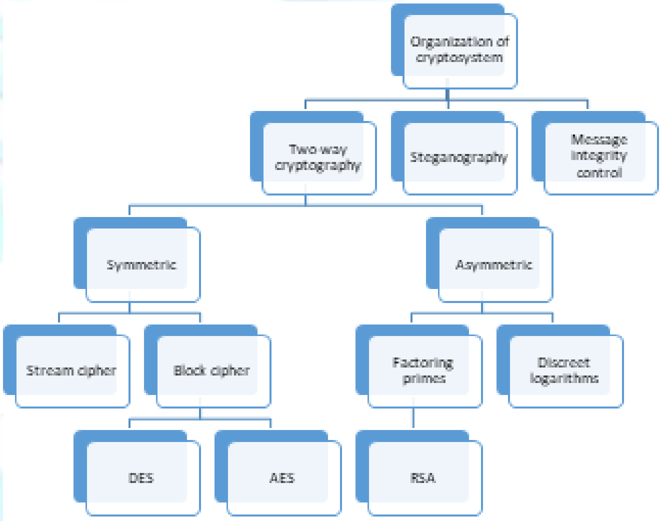

Fig. 1

II. SYMMETRIC ENCRYPTION

A. *Starter to Symmetric Encryption*

Symmetric encryption is the art and the science in transferring readable information to un-readable format. Using one single key share with trusted participant and intended recipient of information

There are two main type of encryption system in symmetric encryption.one is stream cipher and second is block cipher (1).below table 1 have small summary of both symmetric encryption the stream and block ciphers:

Item	Stream cipher	Block cipher

	RC-4	AES (Rijndael)
	Seal	IDEA
	A5/1	RC5
	A5/2	RC6
	A5/3	Blowfish
	Salsa20	Twofish
	Scream	CAST
	HC-256	DES
	ISAAC	Triple DES
	Etc …	Etc..

Table 1 Compile by Hamza ALJaafari from Reference (1)(2)

B. *Understanding the working mechanizm of symmetric ciphers*

It's very important to understand the way these two type of symmetric cipher works. As the encryption protocol under review in this paper are AES and DES. Where according to our small matrix above all of which are classified as symmetric block ciphers.

Citing reference (1) Stream cipher bits used in sequence as keystream are generated & combined with plaintext using bitwise exclusive-OR (XOR). Where this keystream could be generated independently from the plaintext (synchronous stream) or it could be linked and dependent of the plaintext (self-synchronous stream). Allowing higher performance on transforming the plaintext to ciphertext and via versa. And according to (3) stream ciphers are averagely small and fast, and it is most particular for small applications with limited computational resources, such as cell phones or other small embedded devices. But that does not means it is not used in big internet traffic encryptions.

In the other hand block cipher are mathematical algorithm made up of a series of basic mathematical functions such the (XOR) along with addition & substation. The key trick of block cipher is the differing key length, block size and number of rounds (1). Allowing the plaintext to be encrypted to ciphertext1 than ciphertext1 to encrypt again to ciphertext2 and so on. Basic number of round and fix plaintext block size allow the block cipher to be stronger than the historical counterparts cipher techniques (1).

The Key difference between the stream cipher and block cipher is Stream ciphers encrypt bits individually. This is achieved by adding a bit from a key stream to a plaintext bit and Block ciphers encrypt an entire block of plaintext bits at a time with the same key. This means that the encryption of any plaintext bit in a given block depends on every other plaintext bit in the same block (3).

The block cipher are commonly used in web browsers (SSL, TLS) protocols and IPsec suite for VPN tunneling. And also it can be used in encrypting data on rest such disk encryption technologies with higher security and encryption level hard to break and lower performance on storage in compare to stream cipher used for disk encryption.

All Other symmetric algorithms are based on simple mathematical process allowing the transformation of readable text to unreadable format and via versa using single key value called secret key share between the participants the writer and the reader and sometimes the data owner (1).

According to (1), (3) the symmetric algorithm proven it is worthy and importance and it ability to serve the purpose and survive to the recent days. Preserving the goals of consistent confidentiality & integrity to messages and data transfers and Data on rest. But non-repudiation is not achieved using the symmetric ciphers alone where the same key is share and used by multiple parties.

III. ASYMMETRIC ENCRYPTION

A. *Starter to Asymmetric Encryption*

Asymmetric way of encryption involves higher number of key (key pairs) used in the encryption and decryption process, the key pairs are refer to as **private key** & **public key** pairs. Where each participant has his owns set of key pairs. And the two keys in the key pairs have mathematical relation (1).allowing non-repudiation by allowing self-signed has using of the pair (private key). And confidentiality is achieve when the sender use the receiver public key to encrypt the message and the receiver decrypt using his own private key.

Achieving the goals of the asymmetric algorithm. It is must be true that the users owns the private key can easily compute and generate the value of public key. Therefor is not possible for the users holds the public key to compute the value of private key (1), (3). Hence the private key must kept secret with owner and public key can be easily distributed. As when you encrypt with the one of key pairs wither for confidentiality or for non-repudiation you can only decrypt with other pair.

Yes The Asymmetric way of encryption is computationally resource intensive and consuming and it's much slower than symmetric key encryptions (1) but in other hands it comes with many strengths some of which but not limited to are:

- Greater and stronger privacy and confidentiality as the data cannot be decrypted without the associated private key.
- Allows liner key management.
- Introduce the non-repudiation (proof of origin) & authenticity of sender identity.
- Integrate of data confirming data has not been tampered with

- Access control where only the holder of the key pair (private key owner) can actually open the message in contrast with symmetric encryptions where the key is share with multi participates.

B. *Common Asymmetric ciphers*

There are few well known algorithms in asymmetric encryptions such as RSA, ECC, Diffie-Hellman Menezes-Qu-Vanstone, Digital Signature standards (DSS), Oakley. Our paper will be limit to review some the RSA algorithm, and how RSA is associated with Block cipher in symmetric encryption such as AES and DES in hybrid encryption systems.

IV. Data Encryption Standard (DES)

One of the most widely used encryption standards from 1970s is the DES data encryption standards (5). Where Till today still some the legacy application and system are using the DES encryption although it is consider insecure now days due the small key size used in DES encryption which can be break easily using today modern computing systems. The US National Bureau of Standards (NBS) which were renamed as National Institute of Standards and Technology (NIST).The NBS in early 1970s specifically on 1972 has called for tender to commercialize the unified mechanism to encrypt government classified electronic data (5). And in 1974 two IBM cryptographers proposed working cipher based on Horst Feistel Lucifer cipher family (5). The Proposed cipher was submitted to NBS .where NBS pass it to NSA to review it. than after finally amendments by the U.S government bodies and in 1977 the final DES standards encryption was approved with 56 bit key length and data block size of 64 as the Data Encryption Standard (FIPS Publications 46) and to enable it for the common public use and commercial use (5). The DES was design to stand against cryptanalysis attack till 1990s. And yes the DES was approved to be used in U.S. government sector for 10 years till 1887 and by the time U.S government has extended the use of DES till 1999 and till it was replaced by the AES advance encryption standards (5) in the year 2001 which will be explored in the upcoming section of this paper.

The Approved DES has 56 bit key size, and can process a 64 bit data block size in 16 round block cipher. (1)(5). So basically the plaintext data block size of 64 bit will be ciphered 16 times in each time different sub-key will be used which generated from the original 56 bit secret key. There few concepts are applied to make the transformation of data block to cipher block stronger such as techniques are the Confusion & Diffusion techniques. Where the confusion techniques where substation will take place between Keys and the plaintext or data block size. And where the diffusion techniques depends on replacing one plaintext bit or symbols with multiple cipher bit or symbols making it more harder to make the statically calculations of the perceived plaintext after encryption(5).

Citing (1)(3)(5) DES plaintext block is split into two half's lift half Li and Right half Ri where i is the round sequence in the encryption process. And in each round the two half's swap places in way lift have will be using the right bit of the sub-key and right half will be in the lift side , and the following round the swapped again and so on till round 16 and this is express by the following equation:

$$Li=Ri\text{-}1 \quad \text{And} \ / \ Ri= Li\text{-}1 \oplus F(Ri\text{-}1,Ki). \ (3)$$

Where the XOR function is represented by ⊕.

Breaking down the DES block cipher of 16 Rounds (i) 16 Sub Key (Ki) for each round , Two block half's of 32 bit Ri & Li , Half's are swapped in each round. As the below Fig 2 will simplify the statement.

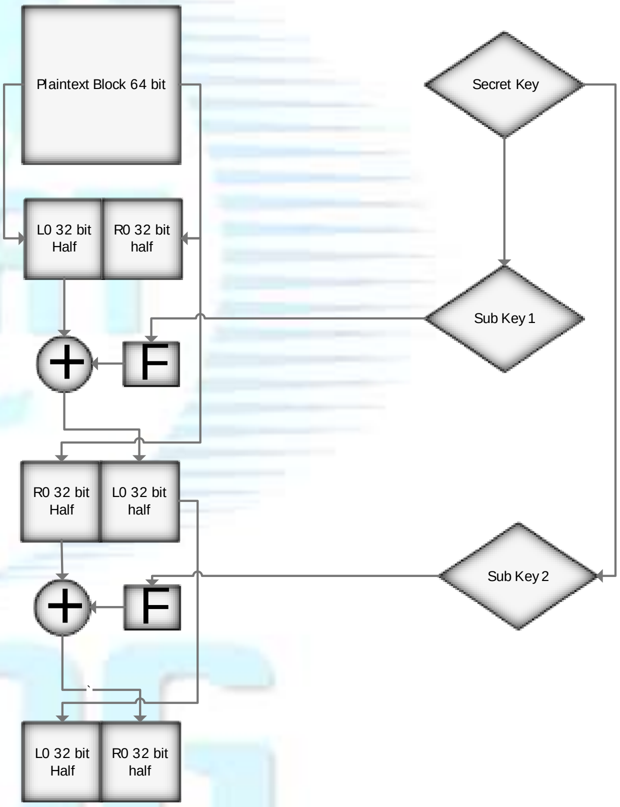

Fig. 2

Looking at the diagram paper illustrate the DES require Key Schedule for both encryption and deception. And it requires F function to be designed on the hardware or software level where the Sub Key taken from the key schedule for each specific round will be as input value for the F function and the result of F function will be use in XOR operation to the second half of the plaintext block. It worth to mention that the half size 32 bit and the key length can be up to 54 bit key. The DES mechanism allows bit by bit allocation scheme with Confusion & Diffusion techniques. Where the half block size will be increased in each round as it will match the key size , as if the right half in round 1 = 32 and Key 1 in the first round = 48 bit the output half will be 48 bit and it will be passed to the following rounds.(5)

V. Advance Encryption standards (AES)

AES the Advance Encryption standards is one of the symmetric block cipher explained early. AES was developed by to Belgian cryptographers (Joan Daem and Vincent Rijmen) in 1998 (1). The AES was published as the federal information processing standards FIPS-publication 197 in 2001 (1)(4).

About three key lengths are support in AES encryption 128,192,256 bit lengths (1)(4). And standard data block size of 128 bit the variable number of encryption rounds of each block to be ciphered. Basically 128 plaintext block size applies to it one of three key length 128, 192,256 bit size key in multiple rounds as shown the below table 2:

Plaintext block size of 128 bit	**Key Length**	**Encryption rounds**
	128 bit	10 rounds
	192 bit	12 rounds
	256 bit	14 rounds

Table 2 Compile by Hamza ALJaafari Reference (1)(4)

AES despite the DES it use to encrypt the plaintext block of 128 bit at once were it gives the AES faster encryption performance in compare to the early DES block cipher and that is way the number of rounds comparatively smaller than the DES (4). And The beauty of AES Algorithm reside behind the layers imbedded in each round assuming using the standard key length of 128 bit main key there are few layers has to be completed to finish the one round excluding the first round and the last round. As the below Fig 3 illustrate:

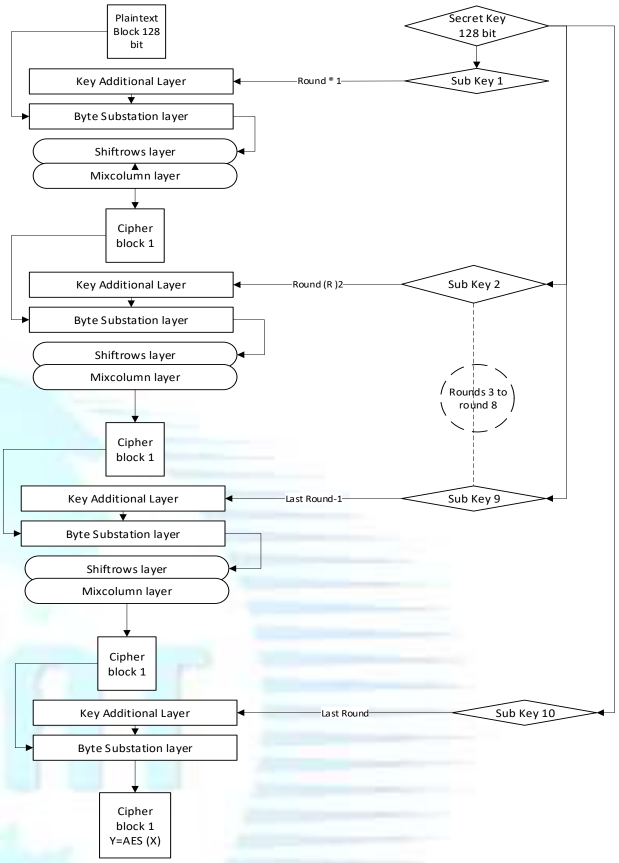

Fig. 3

Now let see and explore the layers of AES encryption the value of AES strength to stands all these years in cryptography science. The Key Addition layer where new set of sub- key is generate in each round from the main AES secret key. Where all sub-keys derived from the main secret key are store in key Schedule. The second layer add confusion by subsisting the bits of data or sequenced cipher blocks in prior's rounds from defined reference lookup table or matrix and this layer called Byte Substitution layer (S-Box). The third layer is Diffusion layer which consist of two sublayers the ShiftRows layer & the MixColumn layer. Basically it is re-poisoning process of bits different rows and column of bytes as shiftRows re-position the bits in given byte, and the Mixcolymn re-position the byte set to different byte set position. The bellow reference figure from (4) give summary highlight of the l shiftRows and Mixcolymn layering function in AES encryption.

The below Table 3 show byte distributions how the bytes is are ordered in AES data block size of 128 bit:

Byte set	Bit position	Byte set	Bit position	Byte set	Bit position	Byte set	Bit position
Byte 0	1	**Byte 1**	1	**Byte 2**	1	**Byte 3**	1
	2		2		2		2
	3		3		3		3
	4		4		4		4

	5		5		5		5
	6		6		6		6
	7		7		7		7
	8		8		8		8
Byte 4	1	**Byte 5**	1	**Byte 6**	1	**Byte 7**	1
	2		2		2		2
	3		3		3		3
	4		4		4		4
	5		5		5		5
	6		6		6		6
	7		7		7		7
	8		8		8		8
Byte 8	1	**Byte 9**	1	**Byte 10**	1	**Byte 11**	1
	2		2		2		2
	3		3		3		3
	4		4		4		4
	5		5		5		5
	6		6		6		6
	7		7		7		7
	8		8		8		8
Byte 12	1	**Byte 13**	1	**Byte 14**	1	**Byte 15**	1
	2		2		2		2
	3		3		3		3
	4		4		4		4
	5		5		5		5
	6		6		6		6
	7		7		7		7
	8		8		8		8

Table 3 Compile by Hamza ALjaafari from reference (4)

So changing either the whole byte set with another or chaining the four bit location with another four but in another byte or changing single bit to another bit in the same byte set each round of the 8 round out of the total 10 rounds and encrypting the bits at once with different sub key of 128 bit. That what really makes the block cipher of AES really strong. And dependable in disk encryption or Data base encryption or transmit and internet encryption.

VI. Rivest, Shamir,Adleman RSA

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

Ronald Rivest, Adi Shamir and Leonard Adleman has formed a cryptographers group as sub-sequence to Whitfield Diffie and Martin Hellman introduced public-key cryptography in their landmark 1976 paper (6). Research way realizing the usage of public key encryption. In 1977 the group announced the scheme which was later realized to be the most wide use asymmetric encryption scheme known as RSA (6). The RSA encryption was not designed to replace the symmetric Block or stream encryptions mechanism. As the RSA algorithm is slower than the common AES and older DES and triple DES encryption in symmetric encryption algorithms.as the RSA require significant amount of mathematical computing process that will decrease the performance and result in slower processing result in compare to the common symmetric encryption such AES and DES. Rather the RSA is used to securely transfer and exchange the symmetric encryption secret keys and validation of sender and receiver (digital signature, non-repudiation). And the symmetric encryption is used to encrypt data bulks (6).

Leaving RSA core mathematical function with creating Key pairs from prime numbers RSA Encryption Given the public key (n,e) = kpub and the plaintext x, the Encryption function is:

$$\mathbf{y = e_{kpub}\,(x) \equiv Xe \text{ mod } n. \text{ and where } x,y \in Z_{n}.} \text{ (6)}$$

RSA Decryption Given the private key

$$\mathbf{d = k_{pr}} \text{ (6)}$$

And the ciphertext y, the decryption function is:

$$\mathbf{x = d_{kpr}\,(y) = Y_{d} \text{ mod } n.} \text{ (6)}$$

And where x, y ∈ Zn. (6)

Usually these number x,y,n,d are very large number about 1024 bit in size(6). And the private key number d is refer as decryption number and the public key number e is refer to as encryption number (1) (6). The RSA key generation involves five steps illustrated below (1) (6):

RSA Key Generation Output: public key: kpub = (n,e) and private key: kpr = (d)

1. Choose two large primes p and q
2. Compute n = p * q.
3. Compute Φ(n)=(p−1)(q−1).
4. Select the public exponent e ∈ {1,2,...,Φ(n)−1} such that gcd(e,Φ(n)) = 1.
5. Compute the private key d such that d · e ≡ 1 mod Φ(n).

(6)

Message x if computed by (e) the public key of the recipient and the resulted can by computed using the (d) the private key and it will give the same x message . is the below equation will take place in this process.

$$d_{k_{pr}}(y) = d_{k_{pr}}(e_{k_{pub}}(x)) \equiv (x^{e})^{d} \equiv x^{de} \equiv x \bmod n. \qquad (6)$$

Now the trick in RSA is the selection of the prime numbers. How the software / hardware engines is are design to generate the two prime number in each time new key pairs are need. But from 1977 there was no major threat or weakness was exploited in the algorithm used in RSA rather than targeting the process or the software and hardware engines use to produce the key pairs. Some of these attacks but no limited to Protocol attacks, Mathematical attacks, Side-channel attacks (6).

VII. Conclusion

By now readers and reviewers reading this paper could understands that the asymmetric encryption could work side by side with symmetric encryption such as AES and DES. And that DES was the first approved encryption standards replaced by AES standards on year 2000. By reviewing the RSA,AES,DES algorithms we discovered the asymmetric encryption algorithms are quit slower and lower in performance in compare to the symmetric encryption algorithms such AES. And usually the asymmetric algorithms such RSA and diffie-hillman are used in digital signature and non-repudiations and in symmetric encryption such AES secret key exchange. We have seen in the paper that asymmetric encryption RSA is self-key contained mechanism where the generation of both key will take place with owner and then distributions of key pair is not a security concern verses the symmetric encryption such the DES and the AES encryption standards where secret key has to be hold by all exchanged parities. Never the less the symmetric encryption algorithms al relevantly faster than the asymmetric encryption algorithm such as RSA. But in general the symmetric encryption algorithms (AES, DES) are limited to provide only congeniality with no digital signature or non-repudiations. And it is quit risky to exchange the symmetric encryption secret key through transmission media such as the internet. So it became clear that in hyper cryptosystem the symmetric cryptography such as AES, DES will provide actual bulk Data encryptions like Disk encryption Data Base encryption and file system encryption and the asymmetric cryptography such RSA will facility the secure key exchange of the symmetric algorithms, the integrity check and the non-repudiation functions. Small illustration table 4 is shown below as function matrix of bot symmetric and asymmetric algorithms.

Matrix item	RSA	AES	DES
Categorized symmetric encryption algorithms	No	Yes	Yes
Categorized asymmetric encryption algorithms	Yes	No	No
Number of key	Two pairs	Secret key with subs	Secret key with subs
Require Secure Key exchange	No	Yes	Yes
Data encryption	Small data	Bulk data	Bulk data
Encryption speed	Slow	Sufficient	Sufficient
Encryption performance	Low	Sufficient	Sufficient
Security and strength	High	Sufficient	Low
Complexity of encryption process	High	High	Medium
Disk encryption	No	Yes	Yes
Data base encryption	No	Yes	Yes
Token encryption	Yes	No	No
Non-repudiation	Yes	No	No
Message encryption	Yes	Yes	Yes
Non-reputations	Yes	No	No
Compute resource consummation	High	Low	Low
Factoring primes	Yes	No	No

Table 4

It worth to highlight the prospective research paper for scholars in this field that may add value to Literature of encryption to the new technology in business world:

1- Based on the advancement of Mobile Ad-hoc Network sensors and controller it worth to investigate the best possible way to develop the fit symmetric and Asymmetric encryption standards that will help integrate the mentioned Mobile Ad-hoc Network perphilers that will allow them to be a security element in the IoT technology and the 5th industrial revolution phenomenon overall.

2- Reference to the advancement in the backend computing and storage, networking hardware. It would great if there will a scholar research help to identify the next version of cipher standards that will utilize the power of these compute resource such fully independent Ship based on IA for Encryption. Allowing more advance encryption that will extremely hard to be cracked even with quantum computing.

3- Research to explore the visibility on how to use the quantum computing to develop more advance encryption standards.

Acknowledgment

Acknowledgment to MIT Faculty members at modern collage of business studies Doctor Basant Kumar & Doctor Hothefa Shaker. And to my beloved class mates in MIT Program Ms. Thuriya ALyaribi and Mr. Hamad ALDrai.

REFERENCES

[1] Official (ISC2) CISSP CBK training Seminar, student handbook Course content Match CISSP CIB effective date : January 1st , 2012.

[2] Canteaut A. (2011) Stream Cipher. In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA

[3] Paar C., Pelzl J. (2010) Stream Ciphers. In: Understanding Cryptography. Springer, Berlin, Heidelberg.

[4] Paar C., Pelzl J. (2010) The Advanced Encryption Standard (AES). In: Understanding Cryptography. Springer, Berlin, Heidelberg.

[5] Paar C., Pelzl J. (2010) The Data Encryption Standard (DES) and Alternatives. In: Understanding Cryptography. Springer, Berlin, Heidelberg.

[6] Paar C., Pelzl J. (2010) The RSA Cryptosystem. In: Understanding Cryptography. Springer, Berlin, Heidelberg.

[7] Jonsson J., Kaliski B.S. (2002) On the Security of RSA Encryption in TLS. In: Yung M. (eds) Advances in Cryptology — CRYPTO 2002. CRYPTO 2002. Lecture Notes in Computer Science, vol 2442. Springer, Berlin, Heidelberg.

[8] Bleichenbacher D. (1998) Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1. In: Krawczyk H. (eds) Advances in Cryptology — CRYPTO '98. CRYPTO 1998. Lecture Notes in Computer Science, vol 1462. Springer, Berlin, Heidelberg.

[9] Kurosawa K., Takagi T. (2003) Some RSA-Based Encryption Schemes with Tight Security Reduction. In: Laih CS. (eds) Advances in Cryptology - ASIACRYPT 2003. ASIACRYPT 2003. Lecture Notes in Computer Science, vol 2894. Springer, Berlin, Heidelberg.

[10] Fujisaki, E., Okamoto, T. Secure Integration of Asymmetric and Symmetric Encryption Schemes. J Cryptol 26, 80–101 (2013). https://doi.org/10.1007/s00145-011-9114-1.

[11] Canteaut A. (2011) Stream Cipher. In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA.