A Note on Symmetric Key Cryptosystems

Pradeep Kumar Singh
Pranveer Singh Institute of Technology, Kanpur

ABSTRACT

In symmetric key cryptosystems, a common secret key is shared between transmitter and receiver. Symmetric key methods usually categorized as stream ciphers or block ciphers. DES (Data Encryption Standard) was used earlier which is replaced by AES (Advanced Encryption Standard) and it is most widely used symmetric key method now days. Here in this paper, we review some characteristics, advantages and disadvantages of symmetric key cryptosystems.

Keywords**: AES (Advanced Encryption Standard), DES (Data Encryption Standard), Security, Symmetric Key, Public Key**

INTRODUCTION:

Symmetric key cryptosystems use a common secret key for encrypting the data. Data communication is a necessity of life in modern world so the importance of symmetric key cryptosystems increases very sharply not only in cryptography and its allied areas [1-9] but also in wireless communication scenarios [10-15] and network security applications [16-20]. In cryptography, all cryptosystems can be divided into two categories. First is symmetric key cryptosystems and second is public key cryptosystems. In public key cryptosystems, a public-private key pair is used for securing the data. The following figures show the difference between the above mentioned cryptosystems.

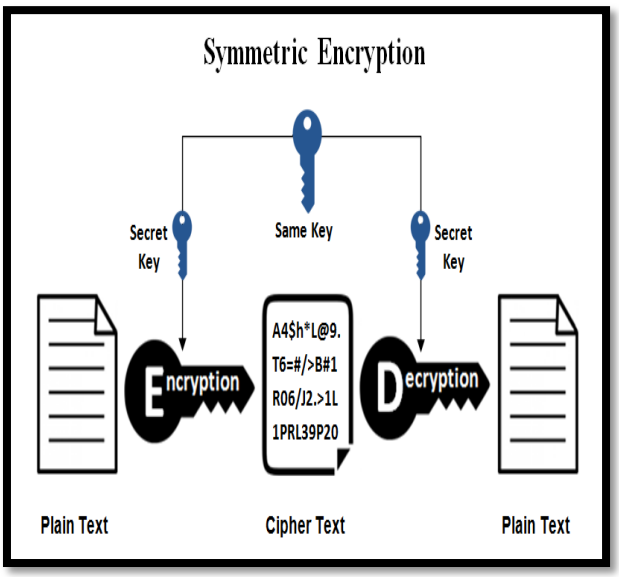

Fig.1. Showing Symmetric key encryption and decryption using the same key

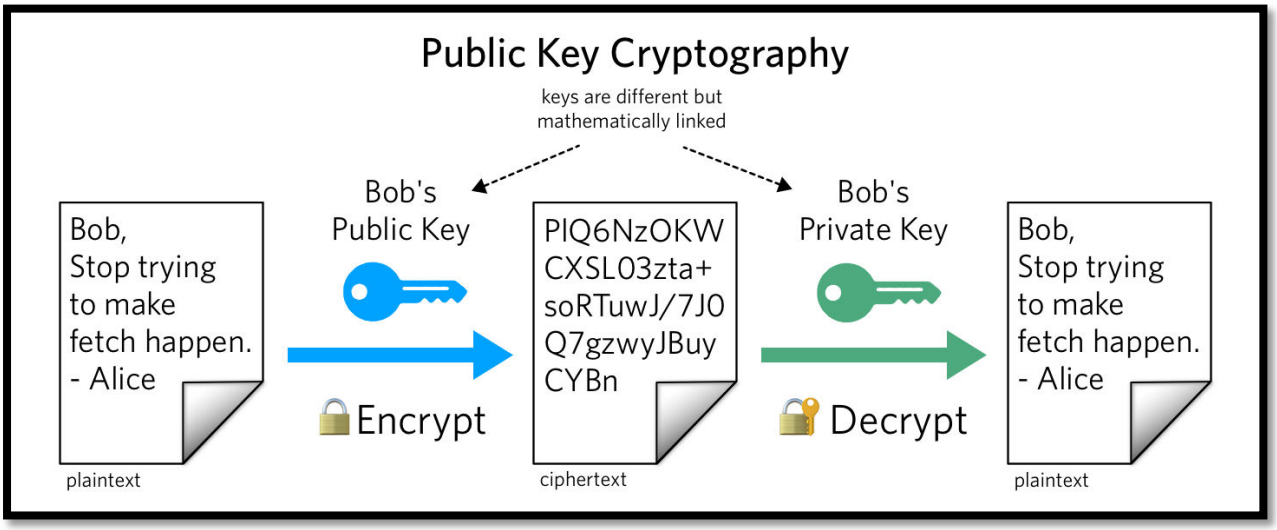

Fig.2. Showing public key encryption and decryption using the key pair

Now we discuss some of the famous symmetric key cryptosystems [21-22].

- **DES:** DES is a block cipher that means it encrypts data in 64 bits block size. The key length is 64 bits but effective key length is of 56 bits only because 8 bits are not used as a key and remains as check bits only.

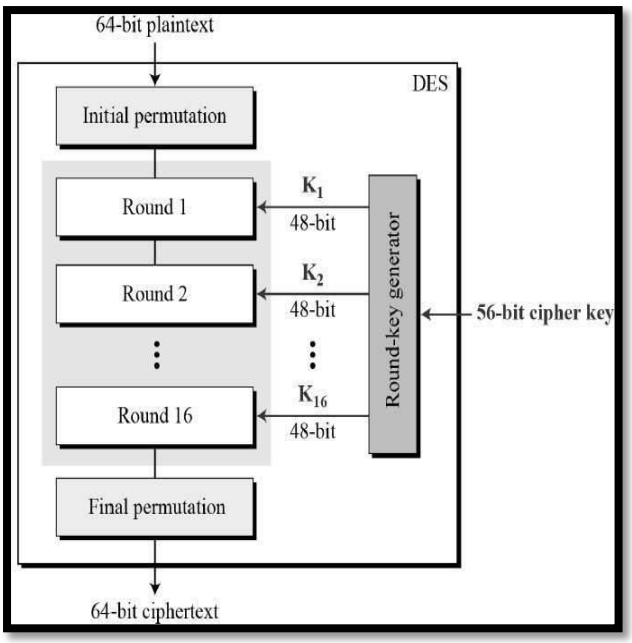

Fig. 3. Showing the process of DES

In DES, S-boxes are used. DES uses eight S-boxes each having 6 bit input and 4 bit output as shown in below figure.

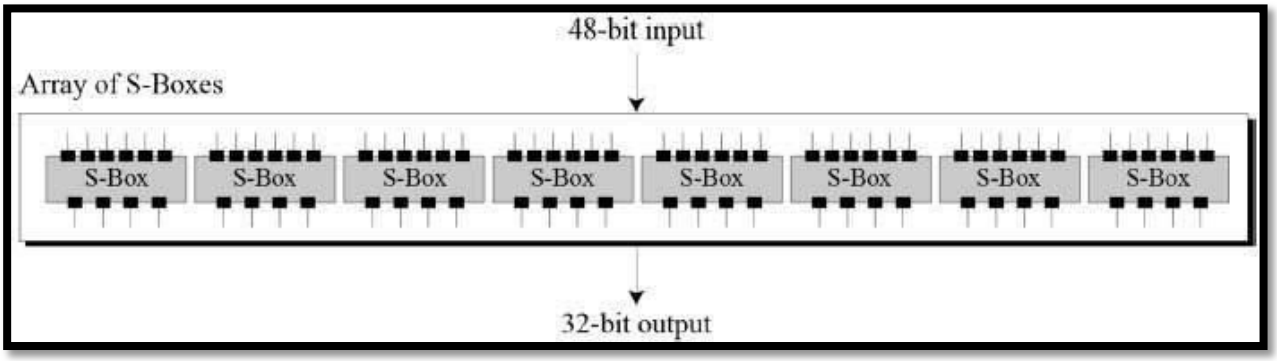

Fig 4. **Showing the working of S-boxes**

The rule of S-box is shown in the below figure.

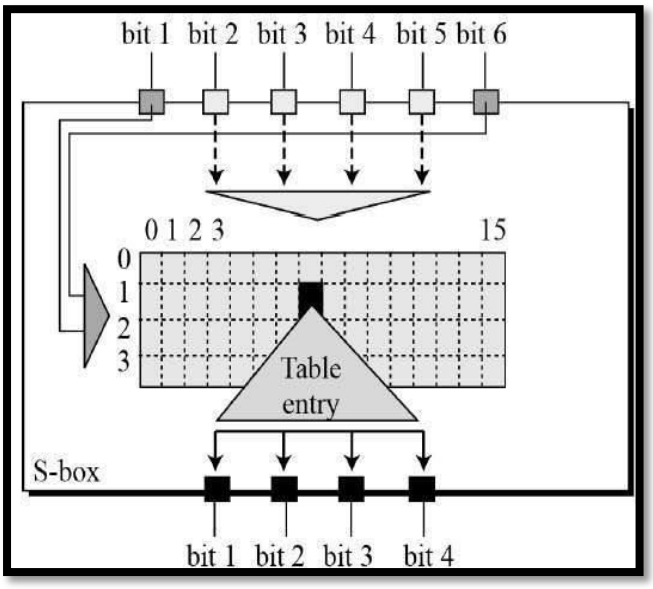

Fig 5. Showing the rule of S-box

DES satisfies all the desired properties of a block cipher. The speed of DES was a big concern and hence a modification of DES is formed named as Triple-DES. Triple-DES is comparatively faster than original DES but a replacement of DES was desired because of the small key size and the increasing computational power of intruders. So AES was designed to replace DES.

- **AES**: AES uses substitution–permutation structure. AES exhibits the following characteristics:

- Symmetric key block cipher
- 128-bit data, 128/192/256-bit keys options
- Much faster than Triple-DES
- Provide full specification and design details
- Software implementation is possible

The number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. The below figure denotes the above mentioned statement.

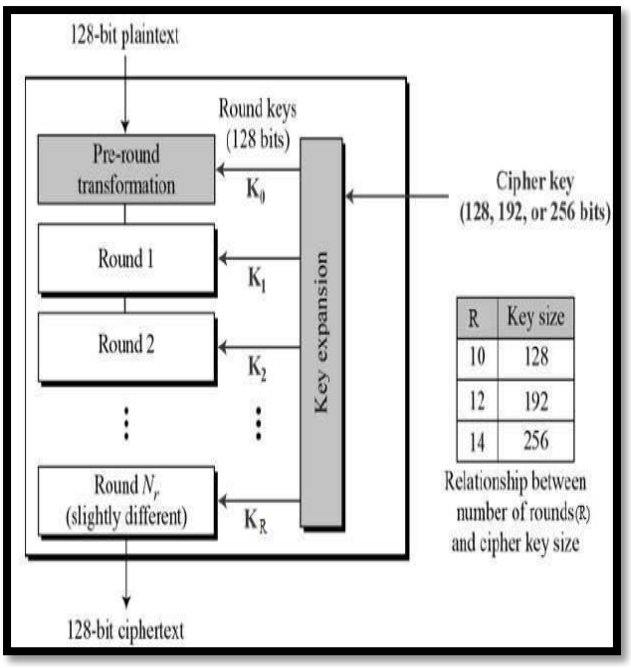

Fig. 6. Showing the structure of AES

The AES encryption follows four sub rounds stated below

- Byte Substitution (Sub Bytes)
- Shift rows
- Mix Columns
- Add round key

The decryption process follows steps in a reversible order given below

- Add round key
- Mix columns
- Shift rows
- Byte substitution

- **Advantages**: There are many advantages of using symmetric key cryptosystems stated below.
  - fast and convenient to set up
  - Highly secure
  - Wide acceptance
  - Requires low computational resources

- **Disadvantages**: There are several disadvantages of using symmetric key cryptosystems also. They are listed below
  - Key sharing is problematic
  - The message's origin and authenticity cannot be guaranteed (cannot provide digital signatures)
  - If your security is compromised (key leak), you will risk more damage

CONCLUSION:

It can be concluded that symmetric key cryptosystems are faster and easily implementable but they suffer with key transportation problem. The modern symmetric cryptosystem uses AES which offers different key sizes and much faster and efficient than DES or Triple DES. AES provides full specifications along with various possibilities of implementation. AES cryptosystems are unbreakable in computationally feasible time subject to the point that keys are shared in a secure fashion.

REFERENCES

[1]. V. Shukla, A. Chaturvedi, N. Srivastava, Nanotechnology and cryptographic protocols: issues and possible solutions, Nanomaterials and energy, volume 8, issue 1, 2019, 1-6,
DOI: 10.1680/jnaen.18.00006

[2]. M.K. Misra, A. Chaturvedi, S.P. Tripathi, V. Shukla, A unique key sharing protocol among three users using non-commutative group for electronic health record system, Journal of discrete mathematical sciences and cryptography, volume 22, issue 8, 2019, 1435–1451,
DOI: 10.1080/09720529.2019.1692450

[3]. A. Chaturvedi, N. Srivastava, V. Shukla, A secure wireless communication protocol using Diffie-Hellman key exchange, International journal of computer applications, volume 126, number 5, 2015, 35-38,
DOI: 10.5120/ijca2015906060

[4]. V. Shukla, A. Chaturvedi, M.K. Misra, On authentication schemes using polynomials over non commutative rings, Wireless personal communications, volume 118, issue 1, 2021, 1-9,
DOI: https://doi.org/10.1007/s11277-020-08008-4

[5]. V. Shukla, A. Mishra, S. Agarwal, A new one time password generation method for financial transactions with randomness analysis, Innovations in electrical and electronic engineering (Part of the lecture notes in electrical engineering book series (LNEE, volume 661)), 2020, 713-720,
DOI: https://doi.org/10.1007/978-981-15-4692-1_54

[6]. V. Shukla, A. Mishra, A. Yadav, An authenticated and secure electronic health record system, IEEE international conference on information and communication technology, 2019, 1-5,
DOI: 10.1109/CICT48419.2019.9066168

[7]. A. Chaturvedi, V. Shukla, M.K. Misra, Three party key sharing protocol using polynomial rings, 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2018, 1-5,
DOI: 10.1109/UPCON.2018.8596905

[8]. V. Shukla, A. Chaturvedi, N. Srivastava, Secure wireless communication protocol: to avoid vulnerabilities in shared authentication, Communications on applied electronics, volume 7, number 6, 2017, 4-7,
DOI: 10.5120/cae2017652680

[9]. V. Shukla, M.K. Misra, A. Chaturvedi, Journey of cryptocurrency in India in view of financial budget 2022-23, Cornell university arxiv, 2022, 1-6,
DOI: https://doi.org/10.48550/arXiv.2203.12606

[10]. V. Shukla, N. Srivastava, A. Chaturvedi, A bit commitment signcryption protocol for wireless transport layer security (wtls), IEEE international conference on electrical, computer and electronics engineering , 2016, 83-86,
DOI: 10.1109/UPCON.2016.7894629

[11]. V. Shukla, A. Chaturvedi, N. Srivastava, A new secure authenticated key agreement scheme for wireless (mobile) communication in an EHR system using cryptography, Communications on applied electronics, volume 3, number 3, 2015, 16-21,
DOI: 10.5120/cae2015651903

[12]. A. Chaturvedi, N. Srivastava, V. Shukla, S.P. Tripathi, M.K. Misra, A secure zero knowledge authentication protocol for wireless (mobile) ad-hoc networks, International journal of computer applications, volume 128, number 2, 2015, 36-39,
DOI: 10.5120/ijca2015906437

[13]. V. Shukla, A. Chaturvedi, N. Srivastava, Authentication aspects of dynamic routing protocols: associated problem & proposed solution, International journal of recent technology and engineering, volume 8, issue 2, 2019, 412-419,
DOI: 10.35940/ijrte.B1503.078219

[14]. V. Shukla, A. Kushwaha, S.S. Parihar, S. Srivastava, V. P. Singh, Authenticated wireless information display system using GSM module, Communications on applied electronics, volume 5, number 3, 2016, 7-11,
DOI: 10.5120/cae2016652251

[15]. V. Shukla, A. Chaturvedi, N. Srivastava, Double layer cryptographic protocol for mobile ad-hoc networks (MANETs) by commitment scheme, Communications on applied electronics, volume 7, number 9, 2017, 32-36,
DOI: 10.5120/cae2017652716

[16]. V. Shukla, A. Chaturvedi, N. Srivastava, A secure stop and wait communication protocol for disturbed networks, Wireless personal communications, volume 110, 861-872, 2019,
DOI: https://doi.org/10.1007/s11277-019-06760-w

[17]. V. Shukla, A. Mishra, A new sequential coding method for secure data communication, IEEE international conference on computing, power and communication technologies, 2020, 529-533,
DOI: 10.1109/GUCON48875.2020.9231252

[18]. A. Chaturvedi, V. Shukla, M.K. Misra, A random encoding method for secure data communication: an extension of sequential coding, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1189-1204,
DOI: https://doi.org/10.1080/09720529.2021.1932902

[19]. V. Shukla, A. Chaturvedi, N. Srivastava, A new one time password mechanism for client-server applications, Journal of discrete mathematical sciences and cryptography, volume 22, 2019, 1393-1406,
DOI: 10.1080/09720529.2019.1692447

[20]. V. Shukla, M.K. Misra, A. Chaturvedi, A new authentication procedure for client-server applications using HMAC, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1241-1256,
DOI: https://doi.org/10.1080/09720529.2021.1932908

[21]. A.J.Menezes, P.C.V.Oorschot, S.A.Vanstone, Handbook of applied cryptography, fifth edition, CRC press Inc., USA, ISBN: 9780849385230, 2001.

[22]. W.Stallings, Cryptography and network security, principles and practices, seventh edition, Prentice Hall, ISBN-13:978-0134444284, ISBN-10:0134444280, 2005.