2019 5th International Conference for Convergence in Technology (I2CT)
Pune, India. Mar 29-31, 2019

A Scheme for Latency Analysis of Different Cryptography Methods for Security in 5G Era

G. Mallikharjuna Rao
Department of ECE
Chaitanya Bharathi Institute of Technology
Osmania University
Hyderabad, India
mallikharjunag@gmail.com

K. Deergha Rao
Department of ECE
Vasavi College of Engineering
Osmania University
Hyderabad, India
korraidrao@yahoo.com

***Abstract*—In this paper, we present a scheme for performance analysis of different cryptography methods namely symmetric ciphers, and asymmetric ciphers to encrypt and decrypt the text, and audio data for online secure data access in the browser window using LabVIEW approach on myRIO hardware module for 5G systems. In this work, the text message with the different payloads is encrypted and decrypted. Similarly, the same process repeated for audio data. First, the text, and audio data are converted into string format; then the data format is encrypted using different cryptography methods from the sender side. On the receiver side, same cryptography method is used to decrypt the data with a generated key associated among the parties. In the case of symmetric ciphers, AES, Blowfish, DES, and IDEA are used to encrypt and decrypt the data. Further, the asymmetric ciphers, RSA, ECC, and DSA are used to encrypt and decrypt the data. LabVIEW programming tools are used to develop a scheme of cryptography methods. Finally, latency analysis is made on text, and audio data with symmetric and asymmetric ciphers.**

***Index Terms*—Symmetric ciphers, AES, Blowfish, DES, IDEA, asymmetric ciphers, RSA, ECC, DSA**

I. Introduction

The Pervasive computation process in the 5G era plays a crucial role to understand data security [1]. The Cryptography methods, namely symmetric and asymmetric ciphers, are used for encryption and decryption on text, and audio data by sharing a private and public key between the sender and receiver. When selecting a cryptography algorithm for 5G user case, low area, low power, and low latency options are to be considered. The first two terms are to be considered for area and power constrained applications. Certain applications are more effected by latency rather than throughput, such applications require low latency. The latency is to be considered for applications that require low latency. The fifth generation (5G) communications have to support a multitude of services. The URLLC (ultra-reliable low latency communications) is one of the services to be supported by 5G. URLLC transmission, that requires a short information block lengths at low code rates with a low BLER (block error rate) at low error flows. URLLC is required for ultra-reliable and latency-sensitive applications and services. In contrast to the current communication systems that are modeled for human-to-human (H2H) interactions, URLLC aim to human-to-machine (H2M) [2] interactions and high reliable machine-type interactions such as telesurgery, factory automation, autonomous vehicles, tactile internet, and remote control. All of these applications have the most strict requirements on low latency, which cannot be accomplished in Long-Term Evolution (LTE) systems. However, the performance analysis of different cryptography methods based on audio files for low latency applications is lacking in literature. Therefore, in this paper, a scheme is proposed for comparative timing analysis of various cryptography algorithms using LabVIEW.

II. Proposed Scheme

The block diagrams of the proposed schemes based on symmetric ciphers and asymmetric ciphers are shown in Figs.1 and 2, respectively.

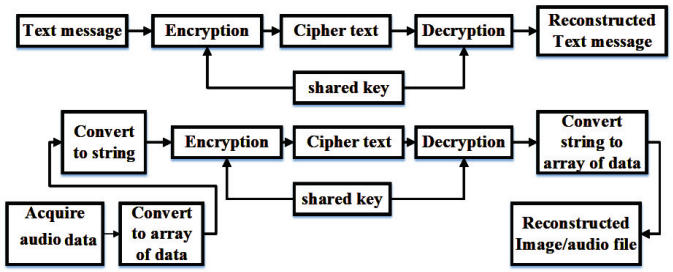


Fig. 1. Block diagram of symmetric ciphers on text, and audio signals

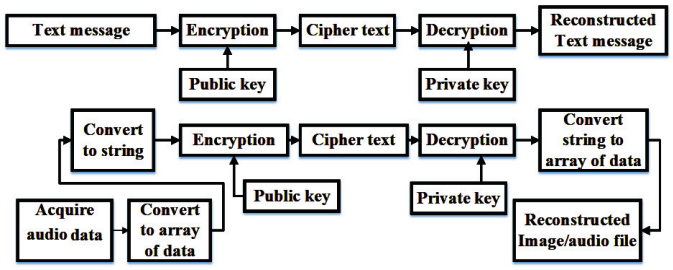


Fig. 2. Block diagram of asymmetric ciphers on text, and audio signals

The text message is encrypted with the shared key, and then converted into a ciphertext; again at the receiver, it is

978-1-5386-8075-9/19/$31.00 ©2019 IEEE

decrypted to reconstruct the text message. This process is also continued for an audio file. In symmetric ciphers, the similar key is used to encrypt and decrypt the plain text. In the case of asymmetric ciphers, the public key, and private key are used to encrypt and decrypt the plaintext. Therefore, different symmetric cipher algorithms and different asymmetric cipher algorithms are used to compare and analyse. To show the comparison between the symmetric and asymmetric ciphers regarding latency, we rely on different cryptography methods. Symmetric ciphers are consistent with message authentication, integration check, and payload. Whereas asymmetric ciphers are allied with public key cryptography, these are related the critical management operations and non-repudiation.

III. Approach with cryptography algorithms

In this section, different symmetric ciphers and asymmetric ciphers are discussed in brief.

A. Symmetric Ciphers

The strength of the cryptography cannot exceed the length of the key applied in the respective algorithms the symmetric cipher attached with crucial shared establishment between two parties communicating with each other, for encryption and decryption of the data. These cryptography methods [3-6] are more suitable for lightweight cryptography analysis. The algorithms are based on two categories, one is block ciphers another one is stream ciphers. In the case of block ciphers, it rely on the substitution-permutation network (SPN) with a fixed length of block size and Feistel networks. Substitution infers to change the number of bits concerning their position with well-defined rules. Permutation allows changing the order of the bits based on the algorithm approach. The effectiveness of algorithm, depends on the distribution of plain text bits across the enormous structures of the cipher text.

Data Encryption Standard (DES), a fixed string length of plain text bits are converted into a cipher text. The decryption standard is considered, which is same as encryption structure in the reverse order. In decryption, round keys are inverted to retrieve the information. The data encryption standard is of key size 56-bits and 64-bit block size with Feistel network structure. The successor of DES is 3DES, in equivalent to AES.

AES is the most popular cryptography method, the block size is 128-bits with different keys of sizes 128, 192 and 256 bits are used with substitution-permutation network structure, the key size depends on the number of rounds 10, 12 or 14. Blowfish algorithm is a block cipher [7-8], with different key sizes ranging from 32 bits to 448 bits with a Feistel network structure. It takes 16 rounds to obtain the encryption standard. It is an altered structure of DES or IDEA.

International Data Encryption Algorithm (IDEA), is a block cipher with 128-bit key size and 64-bit block size followed by eight rounds of operation with Lai-Massey scheme. The decryption is the same as encryption standard, the process is to provide inverted round keys and Inverse techniques for odd rounds.

B. Asymmetric Ciphers

In asymmetric cipher cryptography to encrypt and decrypt the data is done using a public key and a private key [9]. The public key can be shared, but the private key is kept back a secret, the key used for encryption, and the opposed key used for the decryption

Rivest-Shamir-Adleman (RSA) is well-known for public key algorithm, modular multiplications are used on large numbers, whereas the key size varies from 1024-bits to 2048-bits long.

Elliptical curve cryptography (ECC) [10] is an alternative to RSA is based on public key cryptography. ECC key size is quite smaller than RSA security key. Recommended Elliptic Curve Parameters over Prime fields [11,12] parameters are secp112r1, secp112r2, secp128r1, and secp128r2.

The DSA (Digital Signature Algorithm) for digital signature [13], the key size is 1024 bytes and longer it can create a valid signature.

IV. Implementation of the proposed scheme

The following procedure adopted for encrypting and decryption of the text, and audio signals.

A. Encryption Process

Step 1: Obtain the text message/audio signal from database.

Step 2: Convert an audio signal into an array of data, it is represented as a plain text.

Step 3: Convert the array of data into a string.

Step 4: Apply symmetric cipher or asymmetric cipher with the generated shared key or private key on the string format to convert into the cipher text.

B. Decryption Process

Step 1: Obtain the cipher text and process it with the shared key or the public key, for decryption of the symmetric or asymmetric cipher to generate the plain text.

Step 2: Convert the plain text into the array of data.

Step 3: Then convert the array of data into text / an audio of size based on the method applied while encrypting on the sender side.

V. Experiment results

The myRIO-1900 device is Re-configurable I/O (RIO), an embedded hardware module. It will perform for both the analog input/output and the digital input/output operations. It consists of Xilinx zynq 7010 integrated system on chip Technology, a dual-core ARM A9 Cortex processor, analog inputs, analog outputs, audio channels, Wi-Fi, 3 Axis accelerometer and mini system port connectors. The cryptography algorithm is deployed on myRIO-1900 device to check the latency of algorithm applied. The experimental setup using myRIO module, for implementation of the proposed scheme is shown in Fig.3. Once code is executed, the latency is viewed on the front panel of LabVIEW in PC, after encrypting and decrypting the text/audio data on a myRIO hardware device, where the processor speed is 667 MHz.

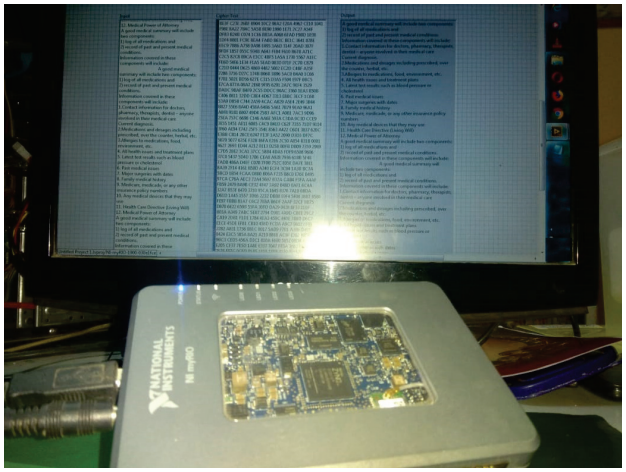


Fig. 3. The myRIO hardware interfaced to PC to exhibit results

A. Symmetric and Asymmetric Ciphers on Text Message

The timing analysis of symmetric ciphers is made on a plain text of payload varying from 256 bytes to 2 kilobytes using AES-128, 3DES, BLOWFISH, and IDEA algorithms. The total time taken for both encryption and decryption is computed. Therefore, the Payload vs. Average time taken for execution is as shown in Fig.4.

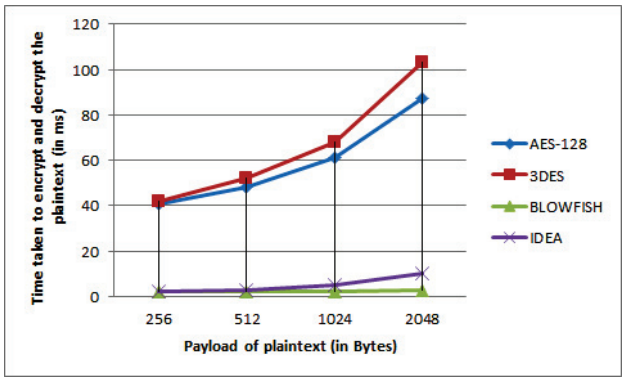


Fig. 4. Timing analysis of text message with different payloads using symmetric ciphers

The timing analysis of asymmetric ciphers is made on a plain text by varying payload from 256 byte to 2 kilobytes. The asymmetric methods, RSA, secp112r1, secp112r2, secp128r1, secp128r2, and DSA algorithms are applied on text message. Therefore, the Payload vs. average time required for execution is as shown in Fig.5. To illustrate the effectiveness of AES-128 on plaintext of 256 bytes is encrypted and decrypted on myRIO and the results are viewed on LabVIEW front panel as shown in Figs. 6 (a), (b) and (c) respectively.

B. Symmetric and Asymmetric Ciphers on Audio Signal

The timing analysis is prepared on symmetric ciphers on audio signal of payload varying from 10 Kilobytes to 27 Kilobytes. Different algorithms namely, AES-128, 3DES, BLOWFISH, and IDEA are used for the process. The total time taken for encrypting as well as decrypting the audio signal is plotted on a graph. Therefore, the audio signal Payload vs.

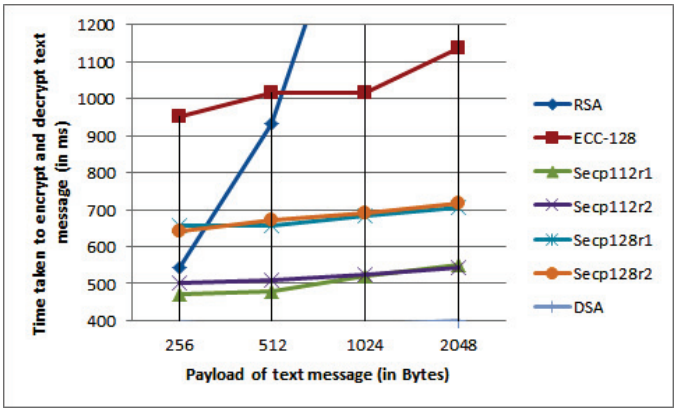


Fig. 5. Timing analysis of text message with different payloads using asymmetric ciphers

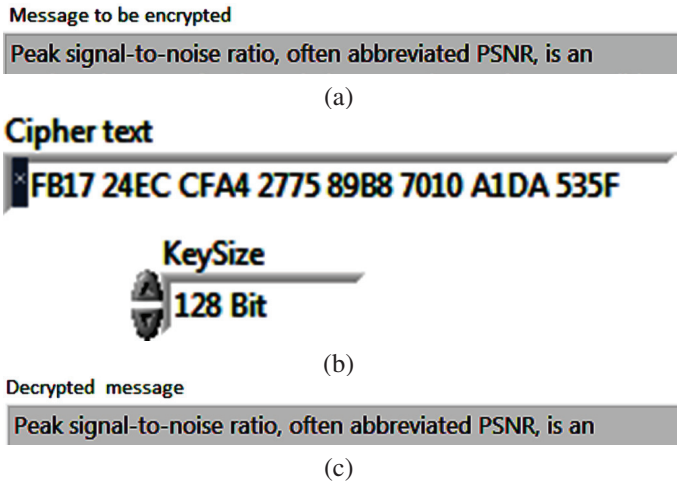


Fig. 6. (a) Text message to be encrypted (b) ciphertext with keysize (c) Decrypted text message using AES algorithm

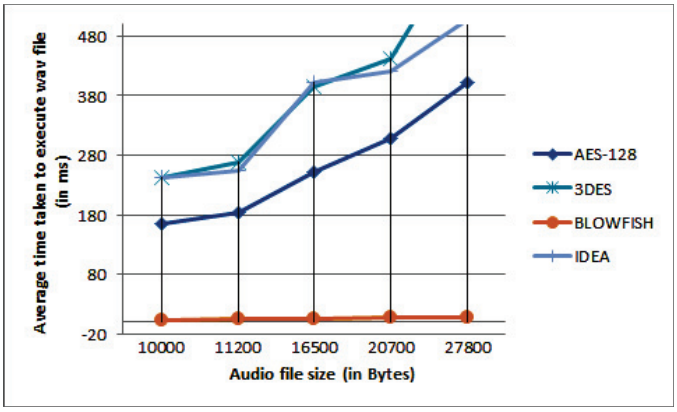


Fig. 7. Timing analysis of audio signal with different payloads using symmetric ciphers

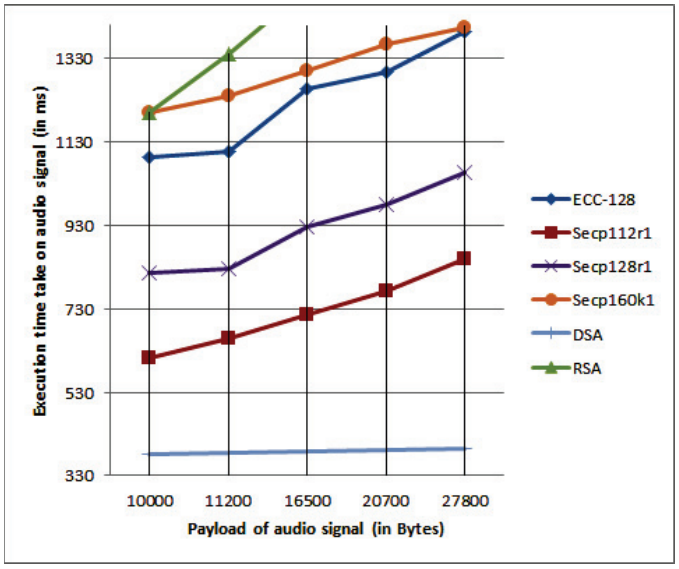
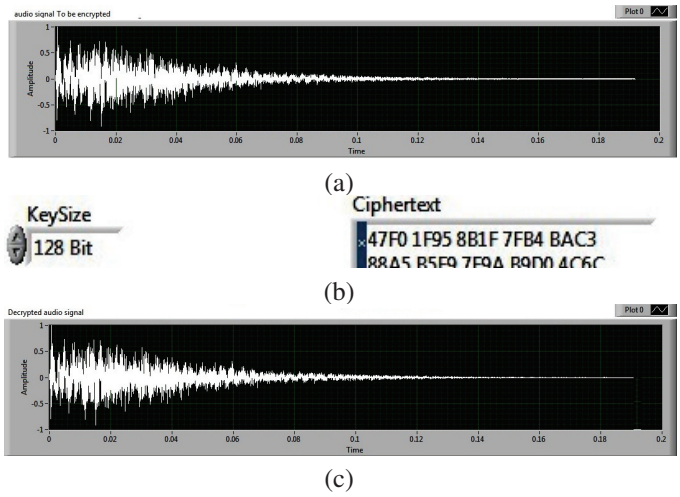


Fig. 8. Timing analysis of audio signal with different payloads using asymmetric ciphers



(a)

(b)

(c)

Fig. 9. (a) Audio signal to be encrypted (b) ciphertext and decrypted (c) Audio signal using AES algorithm

Average time taken for execution is as shown in Fig.7.

The timing analysis is through asymmetric ciphers on an audio signal of payload varying from 10 Kilobytes to 27 Kilobytes. Different ECC-128, secp112r1, secp112r2, secp128r1, secp128r2, and DSA algorithms are used. The total time taken for encryption as well as decryption for both is simulated and plotted on a graph. Therefore, the audio signal Payload vs. Average time taken for execution is shown in Fig.8. To illustrate the effectiveness of ECC on audio signal of 10 kbytes is encrypted and decrypted on myRIO hardware, and the results are viewed on LabVIEW front panel as shown in Fig. 9.

C. Comparative analysis of the cryptography methods

The security features and latency of the cryptography algorithms are shown in table 1, based on the following categories given below:

Very low $<$ 50ms
50ms $<$ low $<$ 100ms
100ms $<$ moderate $<$ 500ms
500ms $<$ high $<$ 1000ms
Very high $>$ 1000ms

The results are based on the execution of cryptography algorithms, on myRIO-1900 hardware module at a processor speed of 667MHz. However, the speed of operation may vary according to the module chosen to execute the algorithms.

Table 1: Comparison of the cryptography methods

Algorithm	**Features**	**Latency**	
		Text	**Audio**
DES	Inadequate security	Low	Low
3DES	Adequate Security and Fast cipher	Very high	Moderate
AES	Highly secured and Fast cipher	**Low**	**Low**
BLOWFISH	Fast Cipher and weak keys	Low	Very low
IDEA	Slow cipher	Very high	High
RSA	Excellent Security and Low Speed	Very high	Very high
ECC	Excellent Security and high Speed	**Moderate**	**Moderate**
DSA	Good Security and high Speed	High	Low

VI. Conclusions

The different symmetric and asymmetric algorithms are tested on myRIO-1900 hardware module using LabVIEW graphical programming software for latency analysis. The algorithms are applied on text, and audio files. In the case of a symmetric cipher, as a trade off between latency and high security, AES has low latency with high security. Similarly, in the case of asymmetric ciphers, the ECC algorithm is providing low latency and high security. Thus, the AES, ECC algorithms may be useful in 5G communication, when compared to other cryptography algorithms for audio signal and plaintext. For further reduction in latency to meet the requirements of 5G, implementation of AES and ECC algorithms may be done on hardware with high processor speed or FPGA.

References

[1] Dimitris Schinianakis, "Alternative Security Options in the 5G and IoT Era," IEEE Circuits and systems magazine, fourth quarter 2017.
[2] Hyoungju Ji, Sunho Park, Jeongho Yeo, Younsun Kim, Juho Lee, and Byonghyo Shim, "Ultra-Reliable and Low-Latency Communications in 5G Downlink: Physical Layer Aspects" IEEE Wireless Communications, June 2018.
[3] Ghulam Mustafa, Rehan Ashraf, Muhammad Ayed Mizra, Abid Jamil, Muhammad, "A review of data security and cryptographic techniques in Iot based devices," ACM, ICFNDS' 18, 2018.
[4] Omar G. Abood, Mahmoud A. Elsadd, Shawkat K. Guirguis, "Investigation of Cryptography Algorithms used for Security and Privacy Protection in Smart Grid," IEEE 2017 Nineteenth International Middle East Power Systems Conference (MEPCON), Menoufia University, Egypt, 19-21 December 2017
[5] Omar G. Abood, Shawkat K. Guirguis, "A Survey on Cryptography Algorithms," International Journal of Scientific and Research Publications, Volume 8, Issue 7, pp. 495-516, 2018.

[6] Sattar B.Sadkhan, Akbal O. Salman, ”A Survey on Lightweight-Cryptography Status and Future Challenges,” IEEE 2018 International Conference on Advances in Sustainable Engineering and Applications (ICASEA), Wasit University, Kut, Iraq.
[7] Sourabh Chandra, Smita Paira, Sk Safikul Alam, Goutam Sanyal, ”A comparative survey of symmetric and asymmetric key cryptography,” IEEE 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE),pp. 83-93, 2014.
[8] Ashwak. A.Labaichi, Faudziah Ahmad, Security Analysis of Blowfish algorithm, IEEE Journal,vol. 10, No. 10, June 2013.
[9] Manju Suresh , Neema M. ”Hardware implementation of blowfish algorithm for the secure data transmission in Internet of Things”, ScienceDirect, Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology, PP. 248-255, 2016.
[10] J. W. Bos, C. Costello, P. Longa, and M. Naehrig, Selecting elliptic curves for cryptography: An efficiency and security analysis, J. Cryptographic Eng., pp. 128, 2015.
[11] SEC 2 Recommended Elliptic Curve Domain Parameters. Standards for Efficient Cryptography Group, September 2000.
[12] R. Sinha, H. K. Srivastava, and S. Gupta, Performance-based comparison study of RSA and elliptic curve cryptography, Int. J. Sci. Eng. Res., vol. 4, pp. 720725, 2013.
[13] FIPS PUB 186-4 Digital Signature Standard (DSS) COMPUTER SECURITY, CRYPTOGRAPHY, Information Technology Laboratory National Institute of Standards and Technology, 2013.