Fig 9 shows the code of our substitution cipher.

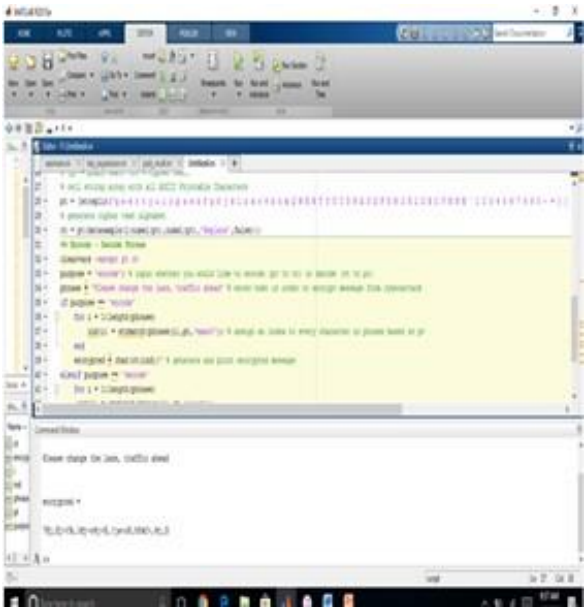
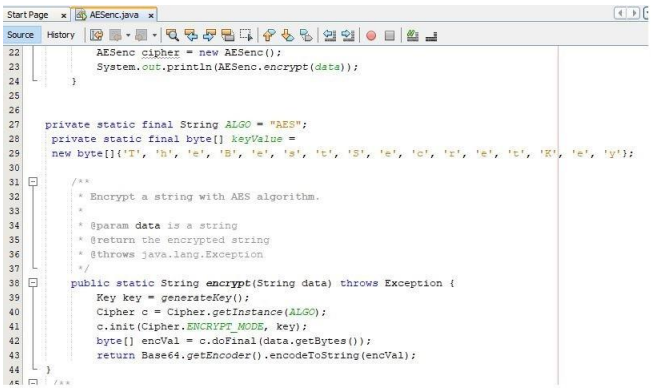


Fig. 9: Simulation of result on MATLAB

We used NetBeans to simulate the block cipher algorithm called AES-128. A message “Please change the lane, traffic ahead” will be encrypted by different round keys and XOR. AES-128 will create a threat free network by not only securing our information but also making it difficult for the attacker to decrypt the message. Fig 10 shows our encrypted message on net beans.

```
run:
Please change the lane, traffic ahead
VXPe+8wdpW8HC/+Emrc/moZAFEm+rrzenO8KpPPB6QbVdziEx/WvdN8OI/CVLd2b
BUILD SUCCESSFUL (total time: 14 seconds)
```

Fig. 10: Encrypted message



```
Start Page | AESenc.java
Source | History
            AESenc cipher = new AESenc();
            System.out.println(AESenc.encrypt(data));
        }

    private static final String ALGO = "AES";
     private static final byte[] keyValue =
     new byte[]{'T', 'h', 'e', 'B', 'e', 's', 't', 'S', 'e', 'c', 'r', 'e', 't', 'K', 'e', 'y'};

        /**
         * Encrypt a string with AES algorithm.
         *
         * @param data is a string
         * @return the encrypted string
         * @throws java.lang.Exception
         */
        public static String encrypt(String data) throws Exception {
            Key key = generateKey();
            Cipher c = Cipher.getInstance(ALGO);
            c.init(Cipher.ENCRYPT_MODE, key);
            byte[] encVal = c.doFinal(data.getBytes());
            return Base64.getEncoder().encodeToString(encVal);
        }
```

Fig. 11: Encrypted message

A base64 in our code will implement the encoding for both upper and lowercase letter. A secret key class represents the key providing independently. It is constructed through an array byte. Comparative to substitution method, our proposed algorithm stands out as a more secure one. During our implementation, the only drawback that we found was some delay in performance time of our proposed cryptographic algorithm. But a few seconds of delay can be compromised by the security of the network.

VI. Conclusion

In this paper we proposed the use of AES algorithm to secure the data theft and cyber attacks in the vehicles. The main idea of this solution is to implement a mechanism of message authentication using paired key values in the ECU which communicates with CAN protocol. Any harmful, hacked messages injected to an ECU or OBD-II port will be notified visually to the driver on the interface of the vehicle. This solution will help the driver recognize the attack and also take precautionary measures.

For future work, this solution can be used by the researchers for implementing this proposed model and test it according to the standards.

References

[1] Automotive cyber security: An iet/ktn thought leadership review of risk perspectives for connected vehicles.

[2] T. Padir L. Lai-T. R. Eisenbarth A. M. Wyglinski, X. Huang and K. Venkatasubramanian. Security of autonomous systems employing embedded computing and sensors. *IEEE Micro*, vol. 33(no. 1,):pp. 80–86, 2013.

[3] B. Groza and P. Murvay. Security solutions for the controller area network: Bringing authentication to in-vehicle networks. *IEEE Vehicular Technology Magazine*, 13(1):40–47, March 2018.

[4] Irshad & Ab Manan Jamalul-Lail Hasbullah, Halabi & Soomro. Denial of service (dos) attack and its possible solutions in vanet. *International Journal of Electronics and Communication Engineering*, Vol:4(No:5), 2010.

[5] K.Wilson I.Parkinson, P.Ward and J.Miller. Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE Transactions on Intelligent Transportation System*, 2017.

[6] A. L. Kun, S. Boll, and A. Schmidt. Shifting gears: User interfaces in the age of autonomous driving. *IEEE Pervasive Computing*, 15(1):32–38, Jan 2016.

[7] Irina-Georgiana Oancea and Emil Simion. Challenges in automotive security. In *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, pages 1–6, June 2018.

[8] Jamal Raiyn. Data and cyber security in autonomous vehicle networks. *Transport and Telecommunication*, volume 19(no. 4):325–334, 2018.

[9] S. Ray, Wen Chen, J. Bhadra, and M. A. Al Faruque. Extensibility in automotive security: Current practice and challenges. In *2017 54th ACM/EDAC/IEEE Design Automation Conference (DAC)*, June 2017.

[10] D. Rotar and H. Popa Andreescu. Face recognition in automotive applications. In *2018 20th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)*, pages 355–359, September 2018.

[11] M. Scalas and G. Giacinto. Automotive cybersecurity: Foundations for next-generation vehicles. In *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)*, 2019.

[12] M. Singh and S. Kim. Security analysis of intelligent vehicles: Challenges and scope. In *2017 International SoC Design Conference (ISOCC)*, pages 13–14, Nov 2017.

[13] Q. Wang and S. Sawhney. Vecure: A practical security framework to protect the can bus of vehicles. In *2014 International Conference on the Internet of Things (IOT)*, pages 13–18, Oct 2014.

[14] Q. Zeng, B. Jiang, and Q. Duan. Integrated evaluation of hardware and software interfaces for automotive human–machine interaction. *IET Cyber-Physical Systems: Theory Applications*, 4(3):214–220, 2019.