



Chapter 9

An Encryption and Decryption Model for Data Security Using Vigenere With Advanced Encryption Standard

Udochukwu Iheanacho Erundu

 <https://orcid.org/0000-0002-5388-9048>
Landmark University, Omu-Aran, Nigeria


Emmanuel Oluwatobi Asani

 <https://orcid.org/0000-0002-6774-8529>
Landmark University, Omu-Aran, Nigeria


Michael Olaolu Arowolo

Landmark University, Omu-Aran, Nigeria

Amit Kumar Tyagi

 <https://orcid.org/0000-0003-2657-8700>
National Institute of Fashion Technology, New Delhi, India

Nehemiah Adebayo

 <https://orcid.org/0000-0001-5838-8843>
Landmark University, Omu-Aran, Nigeria

ABSTRACT

As the amount of data being sent has risen dramatically in recent years; protecting that data has become increasingly important. Cryptography is the process of transforming plain text messages into ones that can no longer be decoded. An information security system's algorithm for encrypting and decrypting data cannot function without them. Data transmission via a communication network can benefit greatly from the use of encryption. Short message service (SMS) is still popular despite the availability of several online messaging platforms. Despite this, these services can be easily cracked, making SMS less secure for transferring critical information. The usage of appropriate cryptographic algorithms is essential to ensuring the safety of your data. Cryptanalysis and pattern prediction are better protected. This study uses a hybridized version of the Vigenère cipher with AES. In tests, the Vigenère-AES came out on top, and it may be used to keep sensitive data safe from prying eyes.

DOI: 10.4018/978-1-6684-5741-2.ch009

INTRODUCTION

As computer technology improves at an exponential rate, so does the amount of data being sent and received over the internet. That's why both academics and researchers are concerned about the safe transfer of data through public networks (Obotivere & Nwaezeigwe, 2020). Privacy is one of the many challenges that Information Security tries to address. It is possible to prevent a third party from deciphering given information over an unsecured connection by broadcasting signals encrypted using cryptographic methods. In today's world, digital content security is increasingly dependent on the use of cryptographic technologies. Security breaches and the misuse of confidential information intercepted by unauthorized parties are key concerns in the field of information security (Casino et al., 2019).

Intruders or third parties may be able to access messages transmitted via networks because of the rising use of digital media. In today's modern age, it is essential to encrypt messages to protect data sent via communications channels and make it harder to decrypt. Even though the internet is open to the public, it is widely believed to be the most efficient medium for transmitting data. As a result, several researchers have proposed efficient algorithms for encrypting this data into ciphers to offset this weakness (Gür et al., 2015).

Encryption is the process of turning data into a form that cannot be deciphered by anybody save the person who generated the encryption key. When encoding and decoding plain text and ciphertext with the same cryptologic keys, symmetric and asymmetric algorithms are the most common options. Unobtrusive transitions between the keys could be the difference between success and failure. For the sake of maintaining a secure evidence link, the keys signify a public and undisclosed text among users (Shankaran, 2004).

Symmetric algorithms include the Advanced Encryption Standard (AES), the Triple Data Encryption Standard (3DES), Blow-fish, and Serpent. For the sake of privacy and security, asymmetric or public key encoding encrypts data such that only the holder of the matching private key may decode it. This is done to prevent unauthorized access by the public key holder (Abdul et al., 2009).

Asymmetric encryption methods include Rivest Shamir Adleman (RSA), the Diffie–Hellman key communication protocol, and the Digital Signature Standard (DSS), which includes the Digital Signature Algorithm (DSA) Advanced mathematics and image-encryption techniques are used in modern cryptography to encrypt text as well as jumble images using Red, Green, and Blue (RGB) pixel displacement. Using a combination of encryption and decryption (Hassan & Hijazi, 2017a). Several security issues have afflicted this. The attacks can be extremely subtle.

The Vigenère cipher and AES were combined in this study to produce a cryptographic application for multimedia data and texts. As a result, the key is less likely to be known by third parties when using Vigenère Cipher and AES; this can minimize computational complexity and make it a good alternative for lightweight applications where resources may be constrained.

RELATED WORKS

Encryption Algorithms designed by (AbdElminaam et al., 2014), were created to compare the new protocols to four current hybrid protocols in terms of power consumption. Different parameters, such as data block sizes and encryption/decryption speeds, were used to compare the various methods. Experiments prove the value of each technique.

17 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/an-encryption-and-decryption-model-for-data-security-using-vigenere-with-advanced-encryption-standard/314930

Related Content

Automatic Pitch Type Recognition System from Single-View Video Sequences of Baseball Broadcast Videos

Masaki Takahashi, Mahito Fujii, Masahiro Shibata, Nobuyuki Yagiand Shin'ichi Satoh (2012). *Methods and Innovations for Multimedia Database Content Management* (pp. 119-142).

www.irma-international.org/chapter/automatic-pitch-type-recognition-system/66691

A Model for Dynamic QoS Negotiation Applied to an MPEG4 Applications

Silvia Giordano, Piergiorgio Cremonese, Jean-Yves Le Boudecand Marta Podesta (2002). *Multimedia Networking: Technology, Management and Applications* (pp. 255-268).

www.irma-international.org/chapter/model-dynamic-qos-negotiation-applied/27036

Tissue Image Classification Using Multi-Fractal Spectra

Ramakrishnan Mukundanand Anna Hemsley (2012). *Methods and Innovations for Multimedia Database Content Management* (pp. 81-95).

www.irma-international.org/chapter/tissue-image-classification-using-multi/66689

P2PTunes: A Peer-to-Peer Digital Rights Management System

Ramya Venkataramuand Mark Stamp (2009). *Handbook of Research on Secure Multimedia Distribution* (pp. 137-156).

www.irma-international.org/chapter/p2ptunes-peer-peer-digital-rights/21311

Designing Multimedia for Improved Student Engagement and Learning: Video Lectures

Kuki Singh (2022). *Online Distance Learning Course Design and Multimedia in E-Learning* (pp. 1-36).

www.irma-international.org/chapter/designing-multimedia-for-improved-student-engagement-and-learning/299830