Instal : Jurnal Komputer

E-ISSN: 2808-683X
Edisi : Volume 17 Nomor 08 | 2025

Available online at https://journalinstal.cattleyadf.org/index.php/Instal/index

Implementation of RC4 Stream Cipher for Data Security in Internet Café Billing Systems

Nasib Marbun
Universitas Negeri Manado

ARTICLE INFO

Article history:

Received : 05 May 2025
Revised : 06 June 2025
Accepted : 30 September 2025

Keywords:
Cryptography, Data Security, RC4, Stream Cipher, Internet Café, Billing System.

ABSTRACT

In the field of data communication, cryptography plays a crucial role in ensuring data confidentiality, authenticity, and integrity. This technique is essential when transmitting sensitive information over public networks, preventing unauthorized access or manipulation. In the context of internet cafés (warnet), which provide global computer network access, a secure billing system is vital to prevent data tampering related to user activity duration and associated charges. This study applies the RC4 stream cipher encryption algorithm to protect the billing data. By encrypting user data before storage, the system ensures its confidentiality and integrity. The implementation, developed using Visual Basic 6.0, demonstrates that the encrypted data (ciphertext) maintains a consistent structure with the plaintext, indicating effective encryption without increasing data size. This solution enhances security in internet café billing systems.

Corresponding Author:
Nasib Marbun
Universitas Negeri Manado
Email: nasibmarb@gmail.com

INTRODUCTION

In the digital era, information technology has become a fundamental component in almost every aspect of life, particularly in data communication and information processing. With the increasing reliance on interconnected systems such as the internet, securing digital information from unauthorized access has become a critical concern. The integrity, confidentiality, and authenticity of transmitted or stored data must be ensured to maintain trust and operational continuity. This has led to the growing importance of data security as a core requirement in both personal and enterprise-level applications. One specific environment that demonstrates the urgency of data security is the internet café (warnet). Internet cafés provide users with public access to the internet, allowing them to engage in browsing, communication, online transactions, and more. These interactions are typically logged and processed through a billing system, which records session duration, cost calculations, and usage logs. The information generated in this system is sensitive, as it involves both user behavior and financial data. Without proper protection, this data is susceptible to manipulation, unauthorized modification, or malicious exploitation, which could harm both users and business owners. To address this vulnerability, cryptographic

Doi : https://doi.org/10.54209/jurnalinstall.v17i03.366

methods can be integrated into the billing system to ensure the security of stored and transmitted data. Cryptography is a branch of science that focuses on techniques for secure communication by transforming data into a form that cannot be easily understood by unauthorized parties. Among the various cryptographic algorithms available, the RC4 stream cipher stands out for its simplicity, speed, and ease of implementation. Despite being an older algorithm, RC4 has been widely used in protocols like SSL (Secure Sockets Layer) and WEP (Wired Equivalent Privacy), particularly in lightweight applications where computational resources are limited. This research proposes the application of the RC4 stream cipher to secure the data stored in an internet café billing system developed using Visual Basic 6.0. The main objective is to encrypt session data, making it unreadable to anyone who does not possess the correct decryption key. Through this approach, the billing records—such as user activity duration and charges—are protected against tampering, thereby ensuring accurate, secure, and reliable data management within the café environment. The rest of this paper is organized as follows: Section 2 discusses the methodology and technical implementation of data security, billing systems, and the RC4 algorithm. Section 3 presents the results and implementation details, followed by an analysis of system performance. Section 4 concludes with key findings and recommendations for further research and development.

METHODS

Data Security

Data is a file that can be confidential so it requires a data security process to maintain its confidentiality. Cryptography is the process of securing data that can be used based on the use of algorithms, one of which is[8]RC4 Stream Cipher. Cryptography is one of the appropriate data security solutions or methods to maintain the confidentiality and authenticity of data, and can improve the security aspects of data or information. Cryptography is a field of science that studies data encoding techniques[9]. Text data is data that has characteristics such as letters, numbers, symbols contained in a document or is a form that does not have objects such as images. Securing text data in the form of ciphertext and the resulting ciphertext results do not increase the capacity of the original data to be one of the commonly known problems that the dominant ciphertext results increase capacity, for that the author tries to secure it with Block Cipher and Stream Cipher[10]. Data security can be done in two ways. The first way is setting the permissions of each user by the database administrator. The second way is data security in terms of data content stored in the database[11].

Internet Cafe Billing System

In this billing, all data is stored in a mysql database, so it can be easier for the owner to seethe number of consumers and the length of time consumers make rentals[12]. Billing Hotspot is an application used for managing internet access users, such as recording transactions and monitoring users[13]. The input of this research is data that is sent in real time from the billing machine, from a series of trials that have been carried out it can run smoothly, which is evidenced by measuring data transmission with speed in accessing article data an average of 0.7833 seconds / transaction data manually[14].

RC4 Stream Cipher

The RC4 algorithm (Ron's Code/Rivest's Cipher) is an algorithm that can be used to encrypt data so that the original data can only be read by someone who has the encryption key.[4].The RC4 stream cipher algorithm is used to convert the actual data into certain symbols, so that the data will not be understood by parties who do not have access rights.[15]. The hardware specifications used for the implementation of making andrunning

Doi : https://doi.org/10.54209/jurnalinstall.v17i03.366

the program so that it runs properly are as follows:

1. Processor : Minimum Pentium III-800 Mhz
2. Memory : Minimum 64 MB
3. Hard disk : Minimum 5 GB
4. Graphics Card : VGA 8 MB with SVGA monitor
5. Monitor : SVGA 1924x78 pixels into 16 Bit color.

In making this program required some software, namely:

1. Operating system : Windows 98 SE, Windows ME, or Windows XP
2. Application : Visual Basic 6.0

RESULTS AND DISCUSSION

Training Data With VB 6.0

RC4 has an S-Box, S0, S1,……, S255, which contains permutations from 0 to 255. It usestwo indexes, namely i and j in its algorithm. Index I is used to ensure that an element changes, while index j will ensure that an element changes randomly. In essence, in the encryption algorithm this method will generate pseudorandom bytes from the key which will be subjected to XOR operations on the plaintext to produce ciphertext. And to produce the original plaintext, the ciphertext will be subjected to an XOR operation against the pseudorandom bytes. In the following, a chart will be provided illustrating the series of processes that are executed to encrypt or decrypt data.

The following will explain the parts of the RC4 Stream Cipher algorithm along with its implementation as follows:

plaintext : encryption
Ascii plaintext : 101 110 107 114 105 112 115 105
Key : computer
Ascii key 107 111 109 112 117 116 101 114

Implementation

To run this image processing software, it is enough to run the Billing.exe file, after runningit will display a flash display as follows:

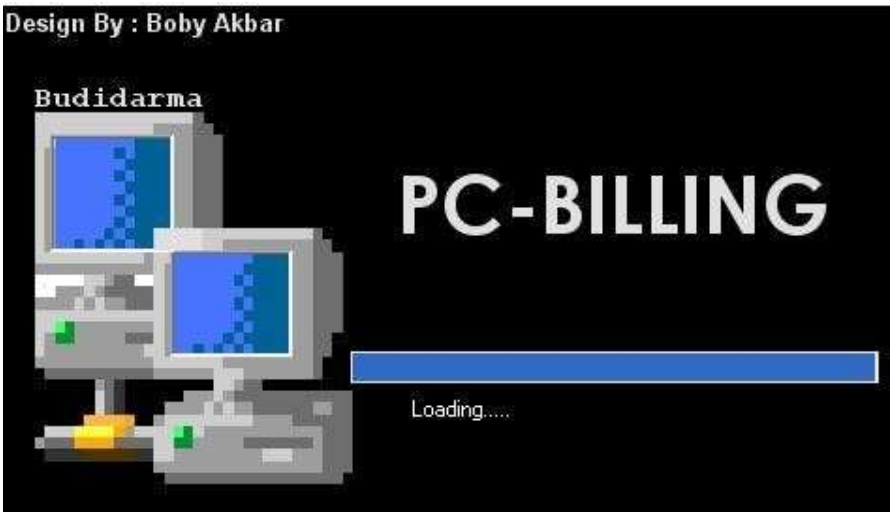

Figure 1. Flash Display

Doi : https://doi.org/10.54209/jurnalinstall.v17i03.366

This form is used as the main menu of the system, as shown in the image below:

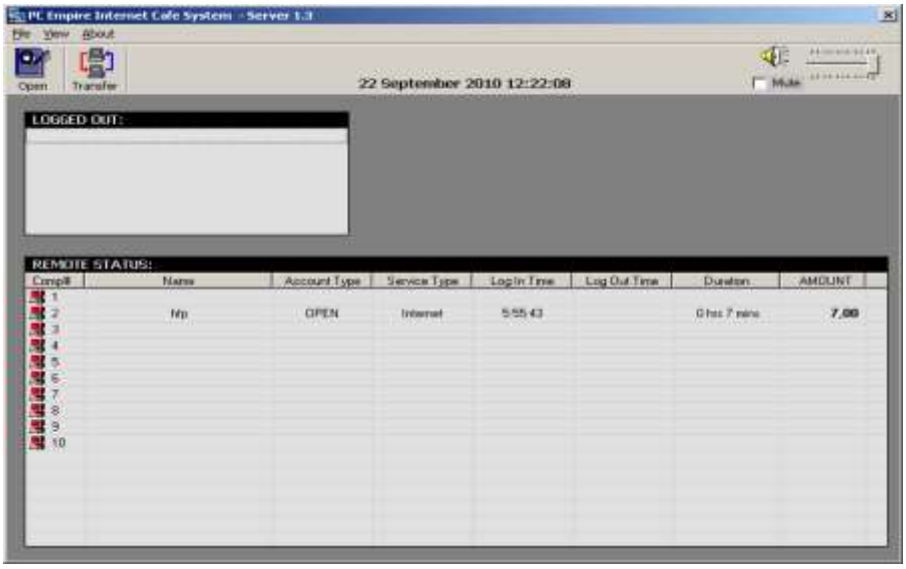

Figure 2. Main Menu Form

This menu is a sub menu of the file menu, as shown in the image below:

Figure 3. File Menu

This menu is a sub menu of the view menu, as shown in the image below:

Figure 4. View Menu

This form is used to perform the process of switching usage between computers, as shownin the image below:

Doi : https://doi.org/10.54209/jurnalinstall.v17i03.366

This form is used to view encrypted information, as shown in the image below:

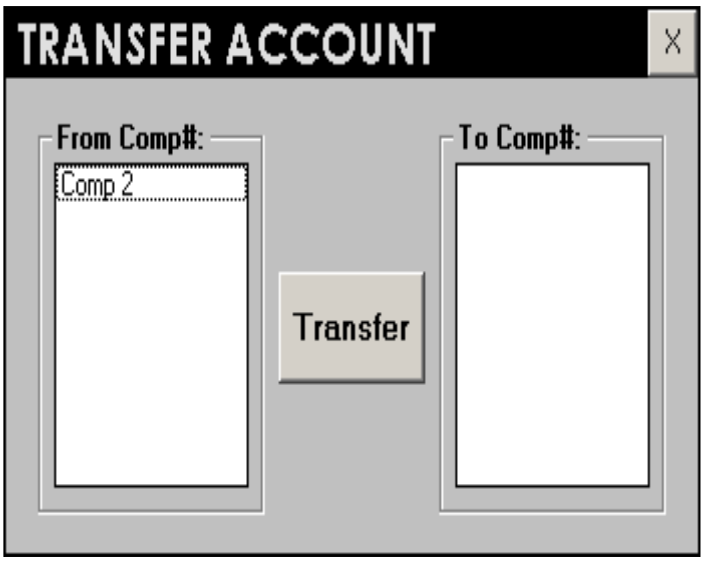

Figure 5. Transfer Account Form

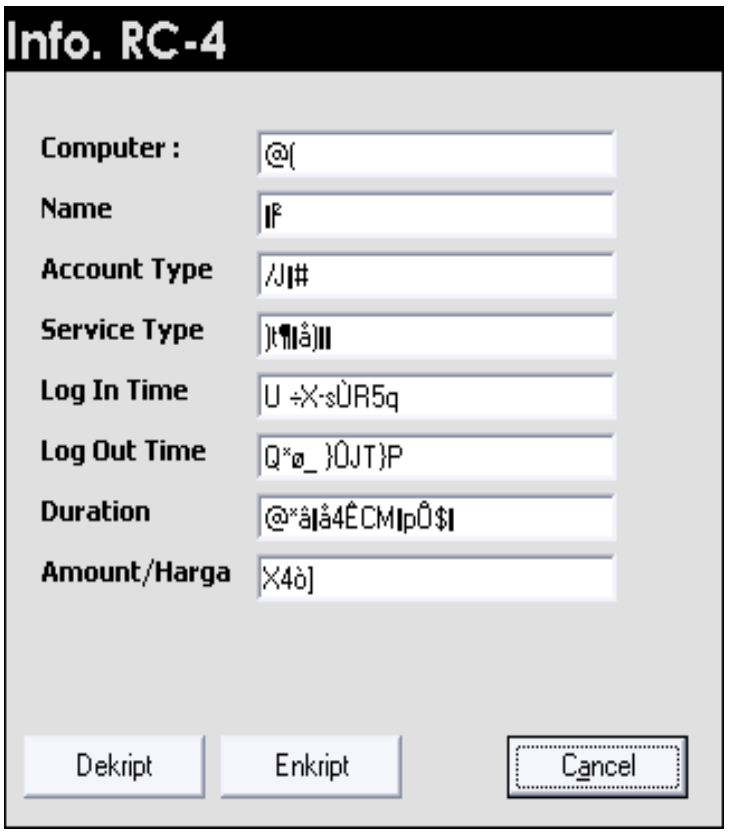

Figure 6. Encryption Results

This form is used to view decrypted information, as shown in the image below:

Doi : https://doi.org/10.54209/jurnalinstall.v17i03.366

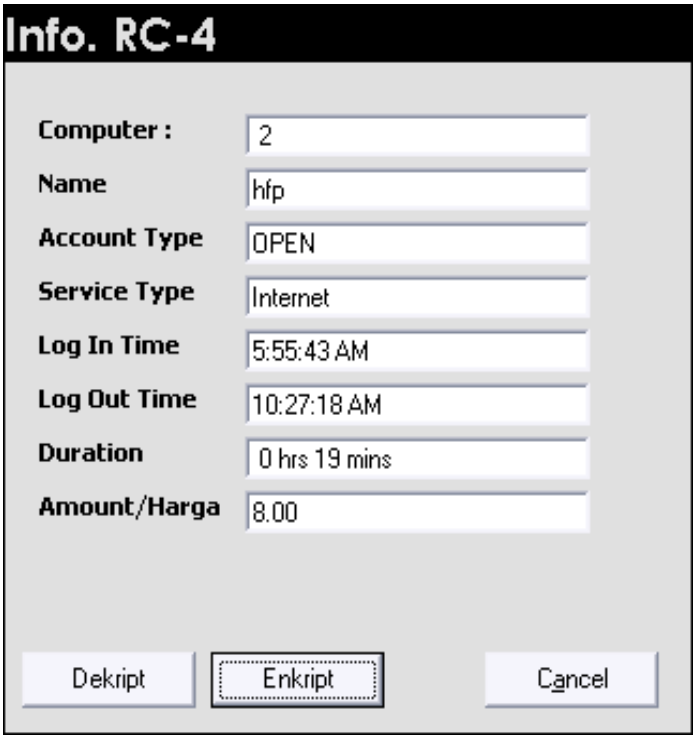

Figure 7. Decryption Results

This form is used to view connected client information, as shown in the image below:

Figure 8. Users Are Connected

CONCLUSION

Based on the implementation and evaluation of the internet café billing system secured using the RC4 stream cipher, it can be concluded that the integration of cryptographic techniques significantly enhances the confidentiality and integrity of user data. The RC4 algorithm, despite its simplicity, has proven effective in encrypting session records such as user duration and usage charges, preventing unauthorized access or manipulation of billing information. The encryption process ensures that each user's activity data is transformed into ciphertext before storage, and can only be decrypted with the corresponding key. This method not only protects sensitive data but also ensures that any attempt to tamper with the data results in unreadable content. The system developed using Visual Basic 6.0 demonstrates consistent and accurate encryption-decryption functionality, with ciphertext output having equal length and structure to the original plaintext, thus maintaining data size efficiency. However, while RC4 was suitable for the purpose of this study due to its ease of implementation and computational efficiency, it is important to acknowledge that RC4 has known vulnerabilities in modern cryptographic standards. Therefore, for future

Doi : https://doi.org/10.54209/jurnalinstall.v17i03.366

enhancements, it is recommended to consider adopting more secure algorithms such as AES or ChaCha20, especially for applications requiring stronger resistance against cryptanalytic attacks. In conclusion, the research validates that the application of the RC4 stream cipher in a billing system context is a viable approach to securing data in internet cafés. This method provides an essential foundation for building trust in public computing environments by ensuring that user information is kept secure, confidential, and tamper-resistant.

REFERENCES

[1.] FN Pabokory, IF Astuti, and AH Kridalaksana, "Implementation of Cryptographic Data Security in Text Messages, Document File Contents, and Document Files Using the Advanced Encryption Standard Algorithm," *information. Mulawarman J. Ilm. Computer Science.*, vol. 10, no. 1, 2016.

[2.] M. Ula, "ANALYSIS OF DATA SECURITY METHODS IN CLOUD COMPUTING SERVICES," *TECHSI - J. Tek. information.*, vol. 11, no. 1, 2019.

[3.] MI Ukkas, R. Andrea, and ABP Anggen, "DATA SECURITY TECHNIQUES WITH END OF FILE STEGANOGRAPHY (EOF) AND VERNAM CIPHER CRYPTOGRAPHY," *Sebatik*, vol. 17, no. 1, 2017.

[4.] DR Saragi, JM Gultom, JA Tampubolon, and I. Gunawan, "Securing Text File Data (Word) Using the RC4 Algorithm," *J. Sis. computer. and Information.*, vol. 1, no. 2, 2020.

[5.] M. Syahril and H. Jaya, "Application of Steganography for Customer Data Security at Standard Chartered Bank Using Least Significant Bit and RC4 Methods," *Semin. Nas. Technol Science. inf.*, 2019.

[6.] R. Toyib and Y. Darnita, "Securing Text Data Using Zero-Knowledge Proof Algorithm," *J. MEDIA INFOTAMA*, vol. 16, no. 1, 2020.

[7.] R. Prasetyo and A. Suryana, "Data Security Application with AES Cryptographic Algorithm Technique and Desktop-Based SHA-1 Hash Function," *J. Sisfokom (Inf. System and Computer)*, vol. 5, no. 2, 2016.

[8.] S. Permatasari, A. Aminudin, and S. Arifianto, "Modification of AES Encryption and Decryption with Polybius Ciper in Data Security," *JRST (Journal of Ris. Science and Technology.*, vol. 4, no. 1, 2020.

[9.] S. Widyastuti, W. Ariandi, and V. Sulistiono, "Implementation of AES Cryptography in Security of JAMKESMAS Participant Selection Data," *J. Ilm. Intech Inf. Technol. J. UMUS*, vol. 1, no. 02, 2019.

[10.] D. Kurniawan, "PLANNING OF TEXT DATA SECURITY APPLICATIONS USING BLOWFISH AND RC6," *J. Pelita Inform. ISSN 2301-9425 (Print Media)*, vol. 17, no. 3, 2018.

[11.] D. Ekklesia, "Study and Implementation of Database Security with Stream Cipher Cryptography Techniques," *SAINTEKBU*, vol. 3, no. 1, 2016.

[12.] Z. reno Saputra, T. Ismail, HM M, and HP M, "DESIGN OF BILLING PLAYSTATION SYSTEMS BASED ON ARDUINO-BASED PLAYSTATION BILLING SYSTEM DESIGN," *Jusikom J. Sist. computer. Musirawas*, vol. 4, no. 02, 2019.

[13.] MY Setiawan, "Design and Implementation of Hotspot Billing Using PHP and Api on Mikrotik at Cybercity Networks," *library. UNIKOM*, no. 2014, 2016.

[14.] R. Dimas Adityo and H. Miawarni, "Application of Cloud Computing Based POS (Point Of Sales) Billing Applications for Restaurant / Restaurant Managers By Utilizing IoT (Internet Of Thing) Devices in Probolinggo Regency, East Java," *Sentia 2018*, vol. 10, no. 1, 2018.

[15.] SA Agusta and TA Fitri A, "Implementation of the RC4 Stream Cipher Algorithm in the Application for Data Collection for Alumni STMIK Amik Riau," *INOVTEK Polbeng - Inform Series.*, vol. 1, no. 1, 2016.