Performance Analysis of Linux Inter Process Communication with “Named Pipe” by Using Different Encryption Methods

*Harun Durmuş (270206025)*

*Abstract—This paper provides a comprehensive review of several filtering strategies used in biomedical signal processing, with a focus on electrocardiogram (ECG) signals. The MATLAB-based examination comprises FIR filtering, IIR filtering (Butterworth, Chebyshev Type I and II), Wavelet Transform, Wiener filtering, and adaptive filtering with the Least Mean Square algorithm. Each filter's performance is evaluated based on its ability to reduce noise and enhance signals, providing insight into its practical applications in biomedical engineering.*

# **INTRODUCTION**

## **Finite Impulse Response (FIR) Filtering**

## **Information Security**

Information security encompasses the techniques and processes that secure digital and non-digital information from unauthorized access, use, disclosure, disruption, alteration, or destruction. It includes a wide range of tactics for defending against cyber threats and protecting sensitive data. The goal of information security is to ensure data confidentiality, integrity, and availability, ensuring that information is accessible to authorized users when needed while also protecting against breaches or data loss. This field is crucial for controlling the risks connected with information technology and communications in a variety of industries, including government, banking, healthcare, and more.

metin, ekran görüntüsü, yazı tipi içeren bir resim

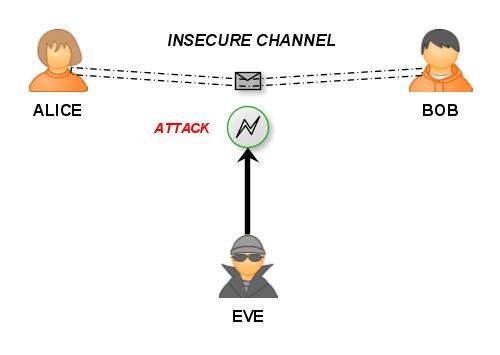
Açıklama otomatik olarak oluşturuldu

***Figure:*** *Layers of a Security System*

***Computer & Network Security***

Computer security protects computer systems and its components from illegal access or damage, which includes hardware, software, and data. It includes methods to avoid malware infections and illegal data intrusions.

Network security, a type of computer security, focuses on securing data transfer via networks. It involves policies and procedures for preventing and monitoring unauthorized access, misuse, or alteration of network-accessible resources.



***Figure:*** *Schematic of a Two-Party Communication*

Information security, handles with several issues:

* ***Confidentiality:*** It ensures that data is only available to authorized users, protecting privacy and secrecy.
* ***Authentication:*** It confirms the identification of people or systems, allowing only authorized access.
* ***Data integrity:*** It ensures the correctness and completeness of data while avoiding unauthorized changes.
* ***Anonymity:*** It safeguards users' identities throughout interactions.
* ***Non-repudiation:*** It precludes denial of actions, such as transmitting messages or conducting transactions.
* ***Availability:*** It ensures that data and resources are available to authorized users when needed.
* ***Traceability:*** It enables for the tracking of actions back to their source, which is critical for audits and investigations.

***Cryptography***

Cryptography is essential for safeguarding inter-process communication (IPC) in Linux, as it ensures data integrity, confidentiality, and authentication. This chapter digs into the core encryption mechanisms, providing insights into their operation, strengths, and uses in digital communication.

metin, ekran görüntüsü, diyagram, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu

***Figure:*** *Schematic of a Two-Party Communication Using Encryption*

Cryptography is the activity and study of ways for protecting communication and information from potential attackers. Its origins may be traced back to ancient times, with simple substitution ciphers employed in Egypt and Rome giving way to the complicated algorithms of the digital age. This evolution was fueled by the ongoing arms race between code makers and code breakers, which shaped the present landscape of information security. In the internet age, cryptography has become essential for protecting data in a variety of domains, including military communications, financial transactions, and personal privacy.

Cryptography is critical for maintaining the secrecy, integrity, and validity of information in the digital age. It safeguards sensitive data against unwanted access, guarantees that data is not altered during transmission, and confirms the identities of communication parties. Cryptography protects online transactions, communications, and data storage, making it vital for internet security, digital banking, and personal privacy. Its significance has grown in tandem with the increasing volume of data shared via the internet and the rising threat of cyber-attacks.

***Basic Terminology***

***Communication Participants***

* An ***entity*** or ***party*** is someone or something which sends, receives, or manipulates information. Alice and Bob are entities. An entity may be a person, a computer terminal, etc.
* A ***sender*** is an entity in a two-party communication which is the legitimate transmitter of information. In figure, the sender is Alice.
* A ***receiver*** is an entity in a two-party communication which is the intended recipient of information. In Figure, the receiver is Bob.
* An ***adversary*** is an entity in a two-party communication which is neither the sender nor receiver. Various other names are synonymous with adversary such as enemy, attacker, opponent, tapper, eavesdropper, intruder, and interloper. An adversary will often attempt to play the role of either the legitimate sender or the legitimate receiver.

***Channels***

* A ***channel*** is a means of conveying information from one entity to another.
* A ***physically secure channel*** or secure channel is one which is not physically accessible to the adversary.
* An ***unsecured channel*** is one from which parties other than those for which the information is intended can reorder, delete, insert, or read.
* A ***secured channel*** is one from which an adversary does not have the ability to reorder, delete, insert, or read.
* An ***information security service*** is a method to provide some specific aspect of security. For example, integrity of transmitted data is a security objective, and a method to ensure this aspect is an information security service.
* ***Breaking an information security service*** (which often involves more than simply encryption) implies defeating the objective of the intended service.
* A ***passive adversary*** is an adversary who is capable only of reading information from an unsecured channel.
* An ***active adversary*** is an adversary who may also transmit, alter, or delete information on an unsecured channel.

***Cryptology***

* ***Cryptanalysis*** is the study of mathematical techniques for attempting to defeat cryptographic techniques, and, more generally, information security services.
* A ***cryptanalyst*** is someone who engages in cryptanalysis.
* ***Cryptology*** is the study of cryptography and cryptanalysis.
* A ***cryptosystem*** is a general term referring to a set of cryptographic tools used to provide information security services. Most often the term is used in conjunction with primitives providing confidentiality, i.e., encryption.

## **Encryption Methods**

***Ceasar (Shift) Cipher***

The Caesar cipher is one of the most simple and well-known encryption methods. It is a type of substitution cipher in which each letter in the plaintext is shifted a set number of positions down or up the alphabet. For example, with a shift of one, 'A' would be replaced by 'B', 'B' by 'C', and so on. Also, spaces and punctuations are reserved. This approach is named after Julius Caesar, who allegedly used it to communicate with his generals. The Caesar cipher's simplicity makes it easy to comprehend, but equally easy to break, restricting its practical relevance to modern security requirements.

metin, ekran görüntüsü, yazı tipi, çizgi içeren bir resim

Açıklama otomatik olarak oluşturuldu

***Figure:*** *Table of Alphabet*

For an n-letter alphabet; P, C, K ∈ Zn, encryption EK(P) = P + K (mod n), decryption DK(P) = C – K (mod n). Let consider the K (shift key) is 4, and plain text is *“This is an encrypted message.”*, cipher text can be created from the alphabet table in the figure above. For example, the letter T becomes X since the key is 4. So cipher text becomes:

*“XLMW MW ER IRGVCTXIH QIWWEKI.”*

The Caesar cipher's simplicity is also its primary drawback. It is vulnerable to frequency analysis, which involves an attacker comparing the frequency of letters or groups of letters in the ciphered text to known frequencies in the original message's language. Because the cipher does not dramatically modify these frequencies, it is quite simple to calculate the shift and decrypt the message. Furthermore, because there are only 25 potential shifts in the English alphabet, an attacker can easily try all combinations to decrypt the message.

***Breaking Ceasar Cipher***

* Eliminating spaces can help to increase safety.
* Counting the number of characters in cipher text (letter E occurs the most frequently in English). So the substraction gives the shift key.
* If just one letter of the plain text along with the corresponding letter cipher text is known, it is easy to deduce the key.
* Choosing a letter as a plain text, The ciphertext gives the key. By trying this method it is possible to break the cipher in maximum 25 iterations.
* Choosing a letter as the cipher text, the plain text is the negative of the key. For example if the plain text is H, the key is -7 ≡ 19 (mod 26).

***RSA (Rivest, Shamir and Adleman) Cryptosystem***

The RSA method is a frequently used asymmetric encryption technology for safe data transport. RSA, named after its founders Rivest, Shamir, and Adleman, encrypts data with a public key that can be freely transmitted, whereas decryption requires a private key that the receiver keeps secret. RSA's security is predicated on the practical difficulty of factoring the product of two large prime numbers, making it a key component of digital security in applications such as safe online browsing, email, and corporate data protection.

RSA encryption uses two keys: a public key for encryption and a private key for decryption. Its security arises from the difficulty of factoring huge numbers into primes, which is computationally expensive for large numbers. RSA is used to ensure secure data transmission, digital signatures, and key exchange. Its effectiveness is determined by key size, with longer keys providing higher security but needing more processing resources. RSA's use in SSL/TLS protocols for secure web connections demonstrates its importance in current cryptography.

Considering one letter sized plain text, letter B to be encrypted. The number representation of B is 2. Let public key for encryption is defined as (5, 14). Thus, cipher text is calculated 25 (mod 14) ≡ 4 in this case. Then, the letter equivalent of this is D. Also, private key for decryption is chosen as (11, 14). When back-propagation is applied, original text can be reconstructed. 411 (mod 14) ≡ 2 (B).

***Generating Keys***

In RSA, keys are generated by selecting two large prime numbers (p and q), calculating their product (n), and then determining a number (e) that is coprime with (n) and the product of the primes' decrements. The public key consists of (n) and (e), but the private key is composed of (n) and a number (d) that solves a certain modular equation involving (e). The procedure assures that public and private keys are mathematically connected, allowing for secure encryption and decryption processes.

Let us choose p= 2 and p= 7. n= p\*q= 14 in this case. This value will be the modulo in encryption and decryption keys. Remainder numbers which are coprime with n (sharing no common factors with n) which are 1, 3, 5, 9, 11 and 13 in this case. In real scenerio, p and q might be enormous, so calculating coprimes would be hard. The number of remainder numbers is equal to Ø(n)= 6. This term can be also obtained as Ø(n)= (p-1)\*(q-1). Then, choosing number e under two conditions:

* 1 < e < Ø(n)
* Coprime with n, Ø(n)

5 can be choosen between four options (2, 3, 4, 5), because only 5 is coprime with n and Ø(n). Then the next step is determining number d for private key. Choosing d: d\*e (mod Ø(n)) ≡ 1. In this case, 11 can be chosen from all options (4, 11, 18, 25…). Finally, public and private keys for RSA cryptosystem is generated.

***Breaking RSA***

The information of the key has a form as: (e, n)(d). Since n and Ø(n) are unknown, p and q can not be determined easily while considering very large n. But it is known that n= p\*q, Ø(n)= (p-1)\*(q-1) and e\*d ≡ 1 (mod Ø(n)). Fastest way to calculate Ø(n) is using Fermat’s factorization:

* n = a2 – b2 = (a+b)\*(a-b)
* b2 = a2 – n
* a = ⌈√n⌉

After *i* number iterations of a, b and corresponding a for it can be calculated. Then p= (a+b) and q= (a-b) assumption will enable calculating the private key after this step. But p and q must be checked if they are prime numbers.

# **MATLAB DEMONSTRATION**

##### **REFERENCES**

1. The Scientist and Engineer's Guide to Digital Signal Processing, Chapter 15, Steven W. Smith, Ph.D., 1997.
2. "How Does An IIR Filter Change Depending On The Approximation Used?", Harry Svenson, Electrical Engineering Stack Exchange, 2018.
3. "Wavelet Transform Processor Based Surface Acoustic Wave Devices", Hagar A. Ali, 2022.
4. “Introduction to Probability for Data Science”, Chapter 10, Stanley H. Chan, 2022.

##### **APPENDIX**

[5] MATLAB code “main.m”