

Pontifícia Universidade Católica de Campinas Faculdade de Engenharia de Computação - FECOMP

Sistemas Operacionais B – Relatório Experimento 2

Chamada de sistema criptográfica no kernel Linux

Beatriz Morelatto Lorente RA: 18071597

Cesar Marrote Manzano RA: 18051755

Fabrício Silva Cardoso RA: 18023481

Pedro Ignácio Trevisan RA: 18016568

**Sumário**

1. **Introdução.....................................................................................................3**
2. **Algoritmo de criptografia utilizado.............................................................4**
3. **Programa de teste.........................................................................................5**
4. **Módulo de criptografia**

**Introdução**

O experimento desenvolvido pretende demonstrar os passos feitos para o desenvolvimento de chamadas de sistema (system calls) que podem armazenar e ler arquivos usando a API criptográfica do kernel. Foram feitas duas chamadas de sistema:

* Na primeira system call, o usuário envia uma mensagem que é criptografada e depois gravada no arquivo
* Na segunda system call, a mensagem armazenada no arquivo é lida, decifrada e enviada para o usuário.

Para a cifragem e decifragem da mensagem foi usado o algoritmo AES em modo ECB

**Algoritmos de criptografia utilizados**

Como citado anteriormente, para cifrar e decifrar a string fornecida pelo usuário foi utilizado o algoritmo AES em modo ECB.

Primeiramente é necessário entender como o algoritmo AES (Advanced Encryption Standard) funciona. O algoritmo consiste em uma criptografia simétrica de blocos de tamanho fixo (utilizamos blocos de 16 bytes, 128 bits). O algoritmo usa uma chave para cifrar e decifrar os blocos e esta também tem 16 bytes.

O modo de criptografia ECB (Eletronic CodeBook), é um dos mais simples que temos, é a primeira geração dos modos AES. A mensagem é dividida em blocos que são critografados separadamente. Como o modo é bem simples, ele não oferece muita segurança, uma vez que não oculta padrões de dados, não sendo recomendado caso o sistema necessite de uma confiabilidade alta. O esquema abaixo mostra como o algoritmo funciona.

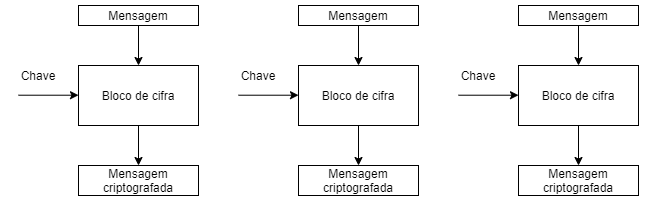


Figura 1 - Funcionamento do algoritmo AES em modo ECB

**Programa de teste**

Para testarmos o experimento foi feito um programa em espaço de usuário que chama as system calls quando necessário. O esquema abaixo representa como essa comunicação é feita.