CRIPTOGRAFIA E SEGURANÇA DE SISTEMAS COMPUTACIONAIS

CRIPTOGRAFIA POR CHAVE BINÁRIA DE ARQUIVOS

OBS: INSTRUÇÕES DE INSTALAÇÃO E EXECUÇÃO DO CÓDIGO ESTÃO NO README.MD DO REPOSITÓRIO CITADO

Feio por:
Felipe Cavlacante Lacerda
Luiz Henrique da Silva de Oliveira

Disponível em:
HTTPS://GITHUB.COM/FELIPECAVLACANTE/W/ENCRYPT-WITH-AUDIO-KEY

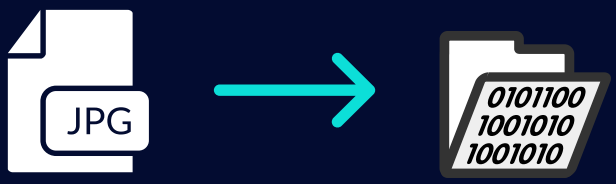
EXPLICAÇÃO DO ALGORITMO

FASE INICIAL

Inicialmente, é utilizado um arquivo qualquer para a leitura e um texto para cifrar.

PROCESSAMENTO

Após a leitura, ambos são convertidos para tipo binário.



VERIFICAÇÃO

Em seguida é verificado a diferença de tamanho do bínario do texto aberto para o arquivo selecionado.

GERAÇÃO DA CHAVE

Essa diferença é suprimida com a geração de bits aleatórios. Esses gerados bits são salvos em um arquivo .txt.

REALIZAÇÃO DO XOR

Em seguida, é realizado a operação XOR com os bits do áudio e com o texto aberto o qual foi somado aos bits aleatórios gerados.

CRIPTOGRAFIA FINAL

Por fim, o resultado do XOR é armazenado em uma variável que recebe uma criptografia do algoritmo AES.

POSSIBILIDADES DE CHAVES

Considerando um arquivo de 44520 bytes e um texto aberto de 44.488 bytes podemos fazer a seguinte análise:

- Possibilidade do tamanho do texto original e arquivo

O tamanho do texto original é de 44.488 bytes, o que significa que existem 2^(44.488 * 8) possíveis combinações para o texto original. Além disso, o arquivo de áudio tem 44.520 bytes, o que corresponde a 2^(44.520 * 8) possibilidades.
No entanto, é importante destacar que a informação sobre o tamanho do texto original não é diretamente contida no texto cifrado resultante. Isso significa que é difícil determinar exatamente onde o texto cifrado termina, pois ele pode ter um tamanho próximo ao do arquivo de áudio, tornando difícil discernir onde o texto termina e onde começa a diferença de 256 bits (considerando que o algoritmo AES funcione corretamente).
Além disso, existe uma margem de variação na diferença de tamanho entre o texto cifrado e a chave, que pode variar de 4 a 32 bytes. Essa variação ocorre devido à operação de soma dos bits aleatórios à diferença de 256 bits e à criptografia AES. Portanto, é difícil determinar com precisão o tamanho exato da chave com base apenas no texto cifrado.
Em resumo, devido às complexidades do algoritmo de criptografia, é desafiador determinar o tamanho exato da chave com base no texto cifrado e nas informações fornecidas. A variação de tamanho e a falta de informações específicas dificultam a obtenção de um valor preciso para o tamanho da chave.

- Possibilidade dos 'random bits'

Considerando que sabemos o tamanho do texto original, a diferença de tamanho entre o arquivo (44536 bytes) e o texto original (44.488 bytes) é de 32 bytes. Esses 32 bytes são utilizados para gerar os "random bits" que serão somados ao texto original. O tamanho dos "random bits" é de 32 bytes, o que resulta em 2^(32*8) possíveis combinações para os "random bits".

- Possibilidade de chave do AES

Considerando que a chave do AES é utilizada na criptografia, a possibilidade total de chaves dependerá do tamanho da chave do AES. O AES suporta chaves de 128 bits, 192 bits e 256 bits. Para cada tamanho de chave, existem 2^(tamanho da chave) possíveis combinações.

- Possibilidade total

Para calcular a possibilidade total de chaves, devemos multiplicar as possibilidades dos "random bits" gerados, o tamanho de bits do texto original e o tamanho de bits do arquivo.

- Tamanho do arquivo: 2^(44520 * 8)
- Tamanho do texto aberto: 2^(44488 * 8)
- Tamanho do 'random bits': 2^(32*8)

$$\text{Total} = 2^{392.320}$$

*OBS: Considerando as variáveis do arquivo de áudio e do texto original, conforme mencionado anteriormente, é importante destacar que o tamanho da possibilidade de chaves pode variar dependendo do tamanho desses elementos.

VANTAGENS

Alta cifragem em pequenos arquivos

É possível identificar uma vantagem significativa no uso dessa criptografia devido à extrema improbabilidade de decifrar um texto aberto. Devido à natureza variável do tamanho do texto, as chances de sucesso na decifragem se tornam assustadoramente reduzidas. Mesmo quando se trata de arquivos pequenos, a probabilidade de decifrar o texto corretamente é realmente ínfima.

Chave aleatória para cada arquivo

Além dessa vantagem, a geração de uma chave aleatória para cada arquivo também contribui para a garantia de alta segurança e improbabilidade de decifragem. A utilização de chaves aleatórias aumenta significativamente a complexidade do processo de criptoanálise, tornando extremamente difícil obter acesso aos dados originais sem a chave correta. Essa abordagem reforça a segurança do sistema, oferecendo uma camada adicional de proteção contra tentativas de decifragem não autorizadas.

DESVANTAGENS

Muitos arquivos, muitas chaves

Essa cifragem se mostra altamente eficiente quando aplicada a arquivos de pequeno porte que contenham informações sensíveis em quantidades reduzidas. No entanto, é importante ressaltar que, ao utilizar essa cifragem em um grande número de arquivos, o processo de geração de chaves individuais para cada um deles pode se tornar um desafio até mesmo para o próprio usuário decifrá-los posteriormente.

Essa dificuldade está relacionada ao gerenciamento e armazenamento seguro das chaves, uma vez que é essencial manter a correspondência precisa entre cada arquivo e sua chave associada. A tarefa de acompanhar uma quantidade considerável de chaves pode se tornar complexa e propensa a erros, especialmente se não for utilizada uma abordagem adequada para organizar e gerenciar as chaves.

Portanto, é importante considerar cuidadosamente a implementação dessa cifragem em cenários que envolvam um grande volume de arquivos, a fim de garantir que haja um sistema eficiente de gerenciamento de chaves. Isso ajudará a simplificar o processo de decifragem para o usuário e a evitar problemas de perda ou confusão das chaves necessárias para cada arquivo criptografado.

Arquivos grandes, chaves grandes

Com arquivos de grande tamanho, a chave necessária para realizar a operação XOR cresce proporcionalmente. Isso significa que, para arquivos consideravelmente grandes, será necessário armazenar uma chave de tamanho igual, resultando em uma demanda de espaço de armazenamento duplicado.

Esse aumento no tamanho da chave pode representar um desafio adicional em termos de gerenciamento e armazenamento de dados. É importante considerar a capacidade de armazenamento disponível e a eficiência do sistema ao lidar com arquivos maiores e as chaves correspondentes.

Uma abordagem viável pode ser o uso de técnicas de criptografia simétrica, como a cifra de bloco, que permite criptografar arquivos grandes sem a necessidade de uma chave do mesmo tamanho. Nesse caso, é utilizada uma chave de tamanho fixo, independentemente do tamanho do arquivo, o que facilita o armazenamento e o manuseio das chaves.

Ao considerar a escolha do método de criptografia mais adequado, é importante levar em conta não apenas a segurança, mas também a eficiência e a praticidade, especialmente ao lidar com arquivos de grande porte.