CIÊNCIA DA COMPUTAÇÃO - UNIP

AS TÉCNICAS CRIPTOGRÁFICAS, CONCEITOS, USOS E APLICAÇÕES

GABRIEL FARIA RODRIGUES DOS SANTOS – N604476

Índice

Objetivo do trabalho

O objetivo do trabalho foi realizar um programa em python, onde nele é possível passarmos uma senha e o programa encriptografar a mesma para nós, sendo assim é possível através do contexto dito proibirmos a entrada de pessoas impróprias no local, através da biblioteca “cryptography” nós podemos encriptografar possíveis senhas, e dentro do mesmo programa podemos também setar uma quantidade limite de tentativas para o usuário que está tentando entrar no local.

Sendo assim só pessoas que teriam acesso à senha poderiam entrar no local.

Introdução

Com o avanço muito grande da devastação ambiental no mundo, os navios são uma das maiores fontes de poluição, o conjunto dos navios no mundo constituem o sexto maior poluidor mundial, nos cinco maiores países (China, Estados Unidos da América, Índia, Rússia e Japão), é um dado muito importante e relevante do trabalho do Consórcio Europeu de Investigação Colaborativa, financiado pelo Investigative Journalism for Europe e alguns media europeus.

Como dito na proposta do trabalho é muito importante que, por razões legislativas o navio permaneça a uma distância segura de pelo menos 50 quilômetros da Costa, vale ressaltar também que eu acesso ao entorno do navio deverá ser feito apenas com roupas especiais para a situação, evitando quaisquer problemas tóxicos.

Conceitos gerais de Criptografia

O principal objetivo de uma criptografia é visar a segurança de uma determinada frase, palavra, senha, nomes ou quaisquer outras coisas que sejam muito importantes para uma determinada situação, como objetivo também a tornar ininteligível para os que não devem obter o acesso.

A criptografia é um elemento fundamental da segurança de dados. É a forma mais simples e mais importante de garantir que as informações do sistema de um computador não sejam roubadas e lidas por alguém que deseja usá-las para fins maliciosos, ou até mesmo obter acesso a uma determinada área de alto risco de valor ou de segurança, como descrito na proposta do trabalho.

Quando informações ou dados são compartilhados na Internet, passam por uma série de dispositivos em rede espalhados pelo mundo, que fazem parte da Internet pública. À medida que passam pela Internet pública, os dados correm o risco de serem comprometidos ou roubados por hackers. Para evitar isso, os usuários podem instalar um software ou hardware específico para garantir que os dados ou as informações sejam transferidos com segurança. Esses processos são conhecidos como criptografia em segurança de rede.

Quanto mais complexa for a chave criptográfica, mais segura será a criptografia, pois é menos provável que terceiros a descritografem por meio de **ataques de força bruta** (ou seja, tentar números aleatórios até que a combinação correta seja adivinhada).

Os dados criptografados com a chave pública do destinatário só podem ser descriptografados com a chave privada correspondente.

Os algoritmos de criptografia são usados para transformar os dados em texto cifrado. Um algoritmo usa a chave de criptografia para alterar os dados de forma previsível para que, mesmo que os dados criptografados apareçam aleatoriamente, eles possam ser transformados em texto simples usando a chave de descriptografia.

No código desenvolvido para este trabalho utilizei a linguagem Python juntamente com a biblioteca cryptography, a mesma inclui ideias de alto nível em interfaces de baixo nível para algoritmos criptográficos comuns, como cifras simétricas, resumos de mensagens e funções de derivação de chaves.

Para fazer o uso desta biblioteca devemos realizar a instalação da mesma via pip, para isto, em seu console digite: “pip install cryptography”, sendo assim teremos acesso a diversas importações no topo de nosso código, como: “Fernet, MultiFernet, InvalidToken” e etc...

Técnicas criptográficas mais utilizadas

Como ressaltado a importância da criptografia acima, quando desejamos obter o máximo de segurança digital, juntamente com o alto nível de dificuldade em um possível acesso indevido, as formas de fazer isso, com as mais utilizadas técnicas são:

Chave simétrica

A chave simétrica é o modelo mais comum e simples. Nela, uma mesma chave é utilizada tanto pelo emissor como pelo receptor da mensagem — ou seja, ela é usada tanto para a codificação como para a descodificação dos dados.

Esse tipo de criptografia foi responsável por lançar as bases para outros modelos, como o DES e o IDEA.

DES (Data Encryption Standard)

Esse é um dos modelos mais básicos, tendo sido um dos primeiros a ser criados (pela IBM, em 1977) e implementados. Consequentemente, é um dos mais difundidos mundialmente, pois fornece uma proteção básica de apenas cerca de 56 bits, oferecendo até 72 quatrilhões de combinações.

Esse método pode ser decifrado por meio de uma técnica chamada “força bruta”. Nesse caso, um programa testa, constantemente, todas as possibilidades de chave, de forma automatizada e por horas seguidas. Como é um sistema de proteção básica, oferece uma segurança reduzida para o usuário.

IDEA (International Data Encryption Algorithm)

Criada em 1991, essa é uma chave simétrica que opera em blocos de informações de 64 bits e utiliza chaves de 128 bits. Ela atua de forma diferenciada, fazendo uma espécie de confusão para cifrar o texto, protegendo as informações e impedindo o realinhamento para a sua leitura de forma correta. Sua estrutura é bastante semelhante à do DES.

SAFER (Secure and Faster Encryption Routine)

Nesse modelo, a criptografia é feita em blocos de 64 bits. Não raro, o usuário poderá encontrá-la pelo nome de SAFER SK-64. Porém, é uma criptografia na qual muitos especialistas encontraram diversas fragilidades,

fazendo com que fossem desenvolvidas novas opções mais complexas, como o SK-40 e o SK-128 bits.

AES (Advanced Encryption Stardard)

É um dos algoritmos de criptografia mais seguros da atualidade, sendo utilizado até mesmo pelo Governo dos Estados Unidos e, também, por diversas organizações de segurança. Sua criptografia é feita em blocos de 128 bits, mas as chaves podem ser aplicadas também em 192 e 256 bits, tornando essa chave extremamente difícil de ser quebrada em ataques convencionais de cibercriminosos.

Chave assimétrica

Também conhecida como “chave pública”, trabalha tanto no modo privado quanto no público. No primeiro, a chave é secreta. Já no modelo público, o usuário deverá criar uma chave de codificação e encaminhá-la para o receptor, para que possa ter acesso ao conteúdo.

Para fazer a escolha da melhor técnica de criptografia devemos levar em conta o nível de sigilo dos dados do seu negócio, como grande bancos de dados de clientes e usuários, ou empresas relacionadas a área de segurança necessitam de proteções extras.

Conseguimos concluir que realmente vale a pena o uso de criptografia, levando em conta o seu alto nível de complexidade.

Relatório com o código comentado

```
from cryptography.fernet import Fernet

# mensagem ao tentar ser acertada para ter o acesso liberado ao navio
senha = "Titanic"

# encriptografa a mensagem
chave = Fernet.generate_key()
fernet = Fernet(chave)
encSenha = fernet.encrypt(senha.encode())

# entrada da tentativa da senha
print('')
print('---- SENHA ENCRIPTOGRAFADA - 3 TENTATIVAS ----')

# senha descript.
decSenha = fernet.decrypt(encSenha).decode()

num_tentativas = 0
acertou = False
while num_tentativas <= 3 and acertou == False:
    tentativa = input("Para obter acesso ao navio, digite a senha
descriptografada: ")
    # print(tentativa)

    num_tentativas = num_tentativas + 1

    # validacao da tentativa
    if tentativa == decSenha:
        print('')
        print('---- ACESSO CONCEDIDO ----')
        print("Senha descriptografada: ", decSenha)
        acertou = True
        break
    else:
        print('')
        print('--- SENHA INVÁLIDA - NÚMERO DE TENTATIVAS: ',
num_tentativas, ' ----')
        acertou = False

print('')
print('---- ACESSO NEGADO ----')
```