Iniciado em	terça, 16 mar 2021, 05:17
Estado	Finalizada
Concluída em	terça, 16 mar 2021, 11:32
Tempo empregado	6 horas 14 minutos
Avaliar	Ainda não avaliado

Questão **1**

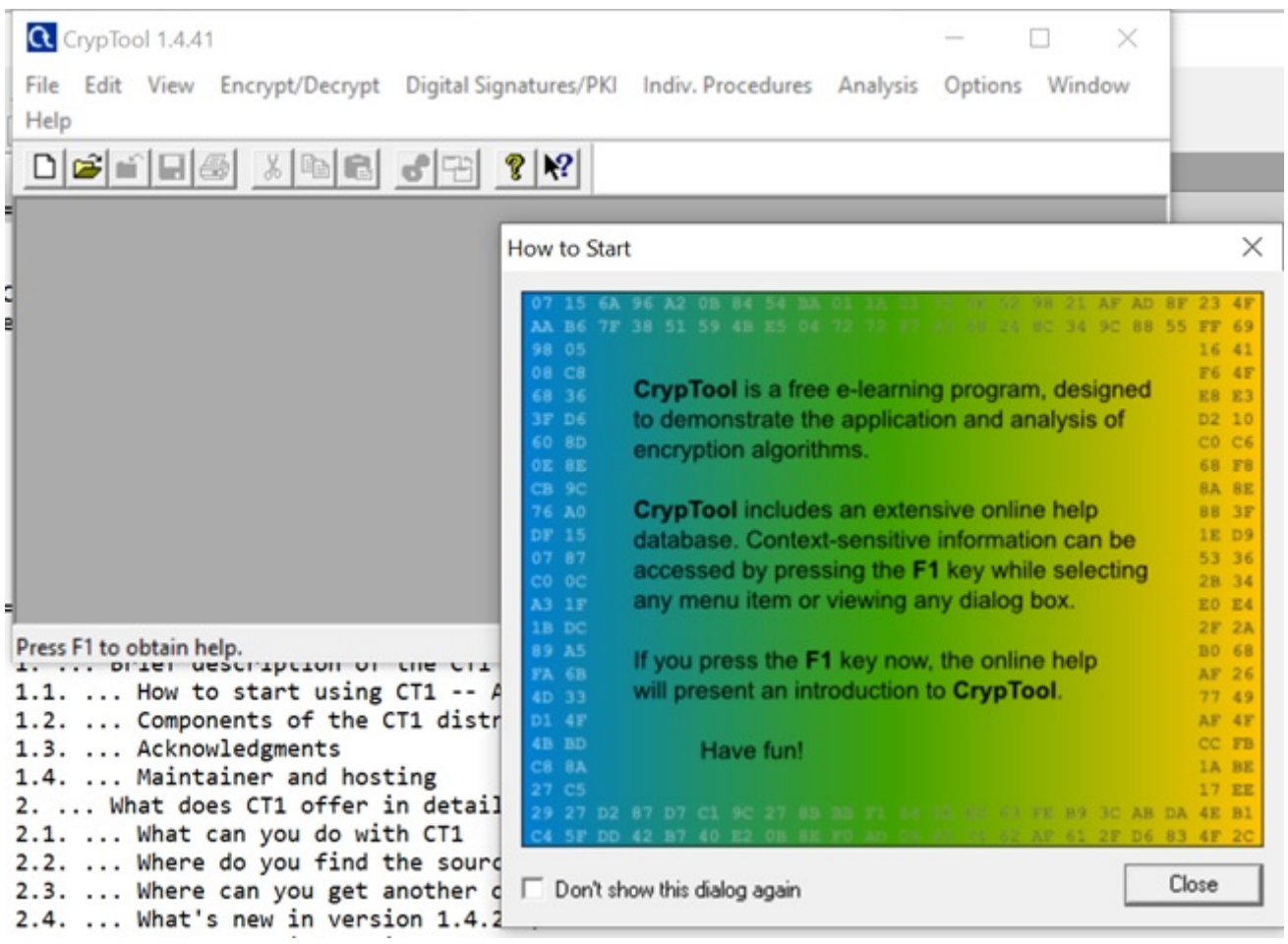
Correto

Atingiu 1,00 de 1,00

Na página https://www.cryptool.org/ há diversos simuladores didáticos de criptografia (software Livre), desenvolvidos em parceria com a universidade alemã de Kassel, pelo Prof. Bernhard Esslinger.

Para esta prática, baixe e instale a última versão do simulador CRYPTOOL 1 na página de downloads: https://www.cryptool.org/en/ct1-downloads

O software depois de instalado apresentará a seguinte interface:



Você realizou a instalação do software?

a. Sim. Instalei o software. ✔

b. Não, necessito de ajuda com a instalação.

Sua resposta está correta.

A resposta correta é: Sim. Instalei o software..

Questão **2**

Completo

Vale 2,00 ponto(s).

Utilizando o simulador Cryptool, decriptar o texto abaixo.

Tzgj vltd jw xuocvxg re qglyq

aw mccjt qmkq sjtcwpvr,

kgflv c ftkps mqvxg l hyqmjvl

w awgt lá kszehxub khvlxhbaaq

Sfwig Sgpnppcp

Para produzir o texto cifrado acima, foram realizadas duas codificações em sequência, conforme segue:

1ª Cifragem: Cifra de Cesar (Caesar), com deslocamento de 14 caracteres.

2ª Cifragem: Cifra de Vigenére, com a chave "PROJETO".

Procure no menu Encrypt/Decrypt opções para realizar a decriptação necessária, conforme dados fornecidos acima.

Faça o upload do texto decifrado obtido, em um arquivo no formato .txt.

Quem dera eu achasse um jeito

de fazer tudo perfeito,

feito a coisa fosse o projeto

e tudo já nascesse satisfeito

questao2.txt

Questão **3**

Completo

Vale 3,00 ponto(s).

Utilizando o simulador Cryptool, abra o arquivo a seguir (disponibilizado na página da disciplina):

13 Cry-DES-12 Cry-Vigenère-crypto2.hex

(https://moodle.utfpr.edu.br/mod/resource/view.php?id=640393)

O arquivo cifrado acima foi criado conforme o seguinte procedimento:

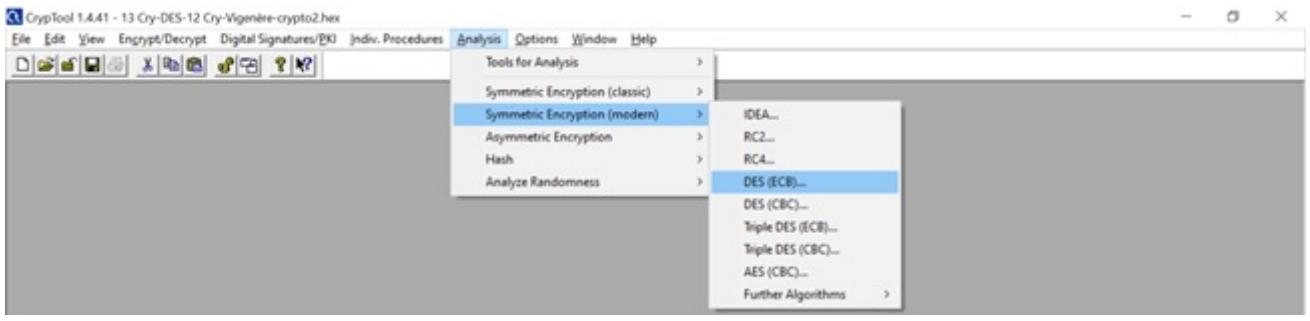
1ª Cifragem: Cifra **Clássica** de Vigenére, com chave **desconhecida**.

2ª Cifragem: Cifra **Moderna DES** (Data Encription Standard) formato **ECB.**

Para esta cifra, só há conhecimento **parcial da chave:** 01 02 03 04 05 XX XX XX em que os caracteres com "X" correspondem a uma parte desconhecida da chave.

a) Realize uma primeira criptoanálise DES (ECB) do texto codificado, utilizando a seguinte opção do menu:

Analysis > Symmetric Encryption (modern) > DES (ECB)



Utilize o seu conhecimento parcial da chave para agilizar a quebra da cifra DES (ECB). Deverá levar no máximo 2 minutos.

b) Faça o upload do código obtido nesta primeira decriptação em formato texto (.txt).

Dica: no menu direito em cima da janela do código, utilize a opção "show as text" para passar de formato "hex dump" para texto.

c) Realize uma segunda criptoanálise com base no texto resultante da etapa anterior, de forma a obter o texto decifrado final.

d) Faça o upload do texto decifrado final em formato texto (.txt).

Source: https://
Fuyeje: ybttf://
aengen riaen
 engenharia

questao3-parte1.txt

questao3-parte2.txt

Questão **4**

Completo

Vale 4,00 ponto(s).

Utilizando o simulador Cryptool, realizar criptoanálises e anotar os tempos, conforme segue:

a) Faça a encriptação do seguinte texto:

Com nada, já dá para começar.

Paulo Leminski

O arquivo deverá ser cifrado conforme o seguinte procedimento:

Cifragem: Cifra **Moderna DES** (Data Encription Standard) formato **CBC**.

Chave: qualquer.

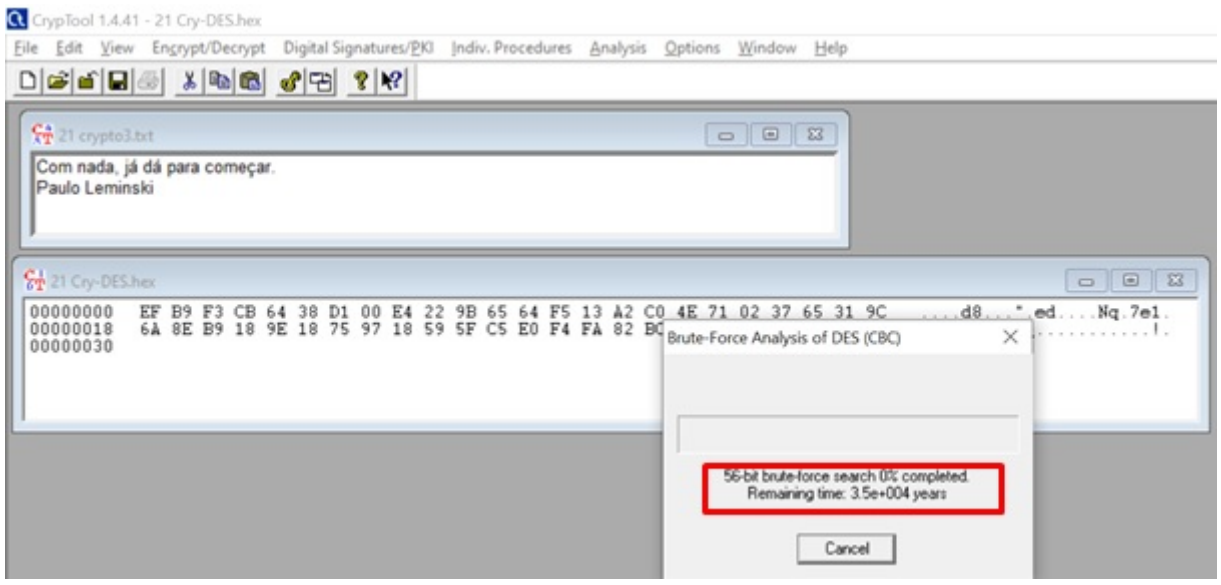
Após encriptado, inicie uma criptoanálise por força bruta, sem utilizar o seu conhecimento da chave:

Analysis > Symmetric Encryption (modern) > DES (CBC)

Anote o tempo inicial ESTIMADO PELA TELA para quebrar a chave na janela de análise que irá aparecer:

Exemplo: 3,5 x 10^4 anos.

Faça upload de um screenshot da tela de criptoanálise em formato imagem (.jpg), similar ao exemplo abaixo.



==========

b) Repita o processo realizado no item anterior, para a seguinte cifra:

Cifragem: Cifra **Moderna** Triple **DES** (**CBC) para 112bits de chave.**

Chave: qualquer.

Anote o tempo inicial ESTIMADO PELA TELA para quebrar a chave na janela de análise que irá aparecer.

Faça upload do screenshot da tela de criptoanálise, em formato imagem (.jpg).

==========

c) Repita o processo realizado no item anterior, para a seguinte cifra:

Cifragem: Cifra **Moderna AES** (**CBC) para 128 bits de chave**

Chave: qualquer.

Anote o tempo inicial ESTIMADO PELA TELA para quebrar a chave na janela de análise que irá aparecer

Faça upload do screenshot da tela de criptoanálise, em formato imagem (.jpg)

==========

d) Repita o processo realizado no item anterior, para a seguinte cifra:

Cifragem: Cifra **Moderna AES** (**CBC) para 256 bits de chave**

Chave: qualquer.

Anote o tempo inicial ESTIMADO PELA TELA para quebrar a chave na janela de análise que irá aparecer

Faça upload do screenshot da tela de criptoanálise. (.jpg).

==========

e) Faça uma breve análise comparativa dos tempos necessários para realizar a criptoanálise por força bruta obtido nos exercícios anteriores (DES, Triple DES, AES128 e AES256).

Explique qual o principal fator que causa a diferença de grandeza nos tempos estimados para a criptoanálise.

==========

OBS: Nesta questão espera-se a análise comparativa dos 4 algoritmos (questão e), bem como o upload dos 4 screenshots correspondentes (questões a, b, c, d).

Conforme foi aumentando o tamanho da chave que usou para encriptar, aumentou o tempo estimado para realizar a analise de decriptação por força bruta.
de 56bits para 1.2e+005 anos;
de 112bits para 8.2e+021 anos;
de 128bits para 3.6e+025 anos;
e 256bits para 1.5e+064 anos.

4-b.JPG

4-c.JPG

4-d.JPG

4-a.JPG

◄ AV03 - PR01 - Análise de Tráfego de Rede

Seguir para...

Arquivo para Prática PR02 - 13 Cry-DES-12 Cry-Vigenère-crypto2.hex ►