FA-DIF-005

|  |
| --- |
| faesa_centro_universitario.png**FAESA CENTRO UNIVERSITÁRIO Valor: 1,0 (um) ponto****Unidade:** Unidade de Engenharia e Computação **Cursos**: CC, SI, TRC, TADS E ENG. AUTOMAÇÃO E CONTROLE**Disciplina**: Sistemas Distribuídos **Professor**: Howard Roatti **Nota:** **Nome do Aluno: ........................................................................... Turma:.................. Data: ...../...../.......** |

**Trabalho 01 – Sistema Distribuído de Criptografia de Mensagens**

***Em Duplas***

Deverá ser criado um sistema utilizando ***Sockets*** para comunicação entre cliente e servidor (fica a cargo do aluno a utilização de TCP ou UDP).

Do lado do cliente, será recebido via passagem de parâmetros pelo usuário uma mensagem em texto claro. O cliente deverá criptografar a mensagem de acordo com a chave e o algoritmo indicado. Após criptografar, o cliente deverá enviar a mensagem para o servidor que, por sua vez, deverá esse deverá exibir a mensagem criptografada e descriptografar a mensagem, então devolver para o cliente. Ao receber a mensagem do servidor o cliente deverá verificar se a mensagem é equivalente a mensagem que recebeu no início do processo exibindo MENSAGEM ENVIADA e MENSAGEM RECEBIDA.

**Observações**:

1. O sistema pode ser criado em qualquer linguagem da preferência de cada um (Java, C/C++, C#, Python, Ruby, etc);
2. Para a entrega deverá ser enviado no Envio de Trabalhos os fontes do sistema (sem compactação) e um arquivo informando como compilar e utilizar o sistema criado;
3. Atenção ao **prazo de entrega (21/04/2019)**, não será avaliado o trabalho entregue em atraso.

Os algoritmos de criptografia a serem utilizados nesse trabalho, no qual deverá criptografar e descriptar as mensagens, são:

(1) Chave da Cifra de substituição: 9

(2) Chave da Cifra de permutação: N-3 (Tamanho da mensagem - 3)

(3) Cítala Espartana: transposição de matrizes

(4) Cifra de César: mesma coisa que (1), porém com chave igual a 5

(5) ROT13: mesma coisa que (1), porém com chave igual a 7

(6) Cifra Atbash: não tem chave, troca a letra pelo sua posição invertida no alfabeto

(7) Cifra de Vigenère: SISTEMAS DISTRIBUÍDOS

Para saberem qual algoritmo implementar, efetue a seguinte função ((MATRÍCULA + 1) % 7) + 1

Onde a MATRÍCULA utilizada será do último componente do grupo em ordem de nomes (A-Z).

**O que será avaliado?**

1 – (0,33) Comunicação entre as aplicações cliente e servidor: a aplicação deve ter funcionando o envio e recebimento de mensagens entre o cliente e o servidor

2 – (0,33) A implementação do algoritmo de encriptação/desencriptação: a aplicação deve conseguir encriptar e desencriptar mensagens

3 – (0,34) Correto funcionamento do projeto, de acordo com o escopo: a aplicação deve conseguir atender os objetivos anteriores (1 e 2) e, somente após isso, verificar se a mensagem desencriptada é equivalente a mensagem recebida