Universidade Federal do ABC	MCTA023-17 – **Segurança de Dados**	**Professora**: Denise Goya
	Prática 01 – Criptografia Simétrica e Confidencialidade: cifras de bloco e modos de operação de cifras	

Baixe e extraia para uma pasta local os arquivos de
SD_lab1_cifras_javascripts.zip, anexo à atividade

Resolva as questões abaixo. Submeta suas respostas **individualmente** no Tidia.

I) Sobre o **DES** (Data Encryption Standard), execute o simulador disponível em *JavaScriptDESExample.htm* e responda as questões a seguir:

1. Cifre algo com DES e observe a saída; mude 1 bit apenas na mensagem de entrada e cifre novamente usando a mesma chave. Quantos bytes foram alterados na saída em relação à anterior? _____ Pode-se tirar alguma conclusão sobre o que foi observado? _____
2. Observe a evolução do algoritmo passo-a-passo no quadro "Details". Quantas execuções da Função de Feistel (*f*) são efetuadas? _____ Quantas execuções de *f* ocorrem quando se escolhe Triple DES? _____
3. Qual é o tamanho da chave em bits, nessa implementação do Triple DES? _____ Observe que a chave não tem o mesmo tamanho da especificação vista em sala de aula; qual é mais segura e por quê? _____
4. Veja que nesse mesmo link, logo abaixo do quadro "Details", há um resumo da descrição do DES (*How DES Works*). Em linhas gerais, em que partes do algoritmo são aplicados os conceitos de Confusão e de Difusão, para aumento da entropia do texto cifrado? _____
5. Esse simulador do DES foi escrito em Javascript; exiba o código no próprio navegador. Em que vetor (variável do tipo *array*) são guardadas as diferentes chaves usadas em cada rodada da Função de Feistel (*f*)? _____ Quantas chaves derivadas são geradas para a execução do DES simples? _____
6. Para observar o comportamento do DES em uma única iteração, insira uma sequência de 8 zeros (em ASCII "0") como mensagem de entrada. Cifre. Em "Details", imediatamente antes de iniciar o *Round1*, L[0] e R[0] guardam os 8 zeros da entrada, com uma permutação inicial. Percentualmente, quantos bits em L[0] e R[0] são iguais a 0 e 1? _____ Imediatamente antes de iniciar o *Round2*, L[1] e R[1] guardam a mensagem original processada apenas uma vez com Feistel. Qual é o percentual de bits 0 e 1 nesse instante? _____ Uma cifra forte, após cada iteração, gera um estado intermediário em que cerca de 50% dos bits são iguais a zero, independentemente da entrada e da chave. Isso ocorre com o DES? Que conclusão você tira a respeito disso? _____

II) Sobre o **AES** (Advanced Encryption Standard), execute o simulador disponível em *JavaScriptAESExample.htm* e responda as questões a seguir:

1. Faça alguns testes para cifrar e decifrar com o AES. Veja o pseudo-código nesta mesma página (textos *Encryption Algorithm* e *AES Decryption*). Observe que para cifrar há um laço de repetição com 10 passos, enquanto para decifrar, o laço é de 9 passos. Em sua opinião, estão corretos esses pseudo-códigos? Justifique. _____
   _____
2. Qual é a função do vetor *w* nessa implementação? _____

III) Sobre os **modos de operação** de cifra de bloco, execute o simulador disponível em *JavaScriptAES-ChainExample.htm* e responda as questões a seguir:

1. Insira duas diferentes mensagens de 16 caracteres (128 bits) em *Message Part 1* e *Message Part 2*. Observe os textos cifrados nos modos *Electronic Codebook* (ECB) e *Cipher Block Chaining* (CBC). Os dois modos de operação produziram alguma semelhança na saída? Explique o motivo. _____
2. Repita o teste anterior para mensagens iguais (*Message Part 1 = Message Part 2*), para os mesmos dois modos de operação. O que é observado e o que se pode concluir?
   _____
3. A implementação dos modos ECB e CBC nesse Javascript não faz *Padding*, o que é necessário se fazer numa aplicação real. O que é *Padding* e como se pode perceber que esse Javascript não o faz? _____
4. Teste o modo de operação *Output Feedback* para mensagens de tamanhos menores que 16 caracteres. Por que funciona e o que se pode concluir? (veja a descrição dos modos de operação nessa mesma página) _____
   O AES com o modo *Output Feedback* poderia substituir uma cifra de fluxo?_____
   Para que tipo de aplicação seria mais vantajoso usar cifra de fluxo e porquê? _____
   Para que tipo de aplicação seria mais vantajoso usar AES com *Output Feedback* e porquê? _____
5. Localize nessa página observações a respeito do vetor de inicialização IV. Quais são as considerações de segurança feitas e suas justificativas?_____
   _____