**ESQUEMA DE PLANO DE AULA PRÁTICA**

**TAREFA 1** "Criptografia Simétrica com DES"

Tópico no Moodle: “Tarefa 1 – Criptografia Simétrica com DES”

Data: 23-08-2013

Tempo de Aula: 2 horas-aula

Grupo: <Aluno\_1> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 <Aluno\_2> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# ASSUNTO Data Encryption Standard

Origem: Wikipédia, a enciclopédia livre.

História do DES

As origens do DES remontam ao início da década de 1970. Em 1972, após concluir um estudo sobre as necessidades de [segurança de informação](http://pt.wikipedia.org/wiki/Seguran%C3%A7a_de_informa%C3%A7%C3%A3o) do governo norte-americano, o então NBS (National Bureau of Standards), atualmente conhecido como [NIST](http://pt.wikipedia.org/wiki/NIST) (National Institute of Standards and Technology), na época o órgão de padrões do governo norte-americano) identificou a necessidade de um padrão governamental para criptografia de informações não confidenciais, porém sensíveis. Em conseqüência, em [15 de Maio](http://pt.wikipedia.org/wiki/15_de_Maio) de [1973](http://pt.wikipedia.org/wiki/1973), após uma consulta à [NSA](http://pt.wikipedia.org/wiki/NSA) (A **Agência de Segurança Nacional** (em [inglês](http://pt.wikipedia.org/wiki/L%C3%ADngua_inglesa): ***National Security Agency*** - **NSA**) é a [agência de segurança](http://pt.wikipedia.org/wiki/Ag%C3%AAncia_de_seguran%C3%A7a) dos [Estados Unidos](http://pt.wikipedia.org/wiki/Estados_Unidos), responsável pela **SIGINT**, abreviatura de *signals intelligence*, o termo inglês usado para descrever a atividade da colheita de informações ou inteligência através da interceptação de sinais de comunicações entre pessoas ou máquinas.

O NBS (NIST) solicitou proposta para um [algoritmo](http://pt.wikipedia.org/wiki/Algoritmo) de criptografia que atendesse a critérios rigorosos de projeto. Entretanto, nenhuma das propostas recebidas se mostrou viável. Uma segunda solicitação foi aberta em [27 de Agosto](http://pt.wikipedia.org/wiki/27_de_Agosto) de [1974](http://pt.wikipedia.org/wiki/1974). Desta vez, a [IBM](http://pt.wikipedia.org/wiki/IBM%22%20%5Co%20%22IBM)submeteu uma proposta candidata que foi considerada aceitável: um algoritmo de criptografia desenvolvido no período de 1973-1974 baseado num algoritmo mais antigo, o algoritmo Lúcifer de [Horst Feistel](http://pt.wikipedia.org/wiki/Horst_Feistel). A equipe da IBM envolvida no projeto do algoritmo incluía Feistel,[Walter Tuchman](http://pt.wikipedia.org/wiki/Walter_Tuchman%22%20%5Co%20%22Walter%20Tuchman), [Don Coppersmith](http://pt.wikipedia.org/wiki/Don_Coppersmith), Alan Konheim, Carl Meyer, Mike Matyas, Roy Adler, [Edna Grossman](http://pt.wikipedia.org/wiki/Edna_Grossman), Bill Notz, Lynn Smith, and [Bryant Tuckerman](http://pt.wikipedia.org/wiki/Bryant_Tuckerman%22%20%5Co%20%22Bryant%20Tuckerman).

O **Data Encryption Standard** (**DES**) é uma cifra (método de [criptografia](http://pt.wikipedia.org/wiki/Criptografia)) selecionado como [FIPS](http://pt.wikipedia.org/wiki/FIPS) oficial (Federal Information Processing Standard) pelo governo dos [EUA](http://pt.wikipedia.org/wiki/EUA) em 1976 e que foi utilizado em larga escala internacionalmente. O [algoritmo](http://pt.wikipedia.org/wiki/Algoritmo) era inicialmente controverso, com um pequeno [tamanho de chave](http://pt.wikipedia.org/wiki/Tamanho_de_chave) e suspeitas de um [backdoor](http://pt.wikipedia.org/wiki/Backdoor%22%20%5Co%20%22Backdoor) da [NSA](http://pt.wikipedia.org/wiki/NSA). O DES foi estudado academicamente e motivou os sistemas modernos de entendimento da [criptoanálise](http://pt.wikipedia.org/wiki/Criptoan%C3%A1lise%22%20%5Co%20%22Criptoan%C3%A1lise). O DES é atualmente considerado inseguro para muitas aplicações. Isto se deve principalmente a pequena chave de 56-bit.

Em Janeiro de 1999 a [distributed.net](http://pt.wikipedia.org/wiki/Distributed.net) e a [Electronic Frontier Foundation](http://pt.wikipedia.org/wiki/Electronic_Frontier_Foundation%22%20%5Co%20%22Electronic%20Frontier%20Foundation) juntas violaram uma chave DES em 22 horas e 15 minutos (veja na [cronologia](http://pt.wikipedia.org/wiki/Data_Encryption_Standard#Cronologia)). Também existem alguns resultados analíticos, obtidos teoricamente, que demonstram a fragilidade da cifra, no entanto são improváveis de se montar na prática.

Acredita-se que o algoritmo seja seguro na forma de [3DES](http://pt.wikipedia.org/wiki/3DES) (construção do DES usando 3 chaves) embora existam ataques teóricos. Recentemente o DES foi substituído pelo [AES](http://pt.wikipedia.org/wiki/AES) (**Advanced Encryption Standard**), muito usado em várias aplicações em elementos de rede (por exemplo, pontos de acesso de Wi-Fi).

**BIBLIOGRAFIA BÁSICA**

<http://pt.wikipedia.org/wiki/Data_Encryption_Standard>
 **OBJETIVOS DA AULA**

Conhecer um algoritmo de criptografia simétrica, relativo às seguintes características:

1. Estrutura geral
2. Tamanho de chave
3. Modo de Cifra (bloco ou fluxo) e qual o modo de cifra usado.
4. O ambiente criptográfico da linguagem de programação usada na implementação.

**SELEÇÃO DE CONTEÚDO – A PRÁTICA**

Um conteúdo mínimo, consistindo de um roteiro de aula para o DES, visando o objetivo acima, pode ser colocada como:

1. Leia rapidamente o histórico acima.
2. Abra o link <http://pt.wikipedia.org/wiki/Data_Encryption_Standard>
3. Veja sua **Descrição**, **Estrutura Geral**, a **Função de Feistel**, o **Escalonamento de Chaves** (a geração de sub-chaves para cada de um de seus 16 *rounds*).
4. Use os arquivos (java\_Text\_DES.txt) e (java\_File\_DES.txt), encontrados na página da disciplina nos tópicos da Aula 2, e realize a execução dos dois códigos correspondentes. Procure completar estes códigos, caso falte alguma parte como a leitura de arquivo. No arquivo (java\_File\_DES.txt) o arquivo (original.txt) é a entrada legível para o programa, o qual é apresentado criptografado em (encrypted.txt) e fornece a resposta descriptografada no arquivo (decryptd.txt).
5. Identifique no **JCE** (**Java Cryptography Extension** é um conjunto de extensões da [Java](http://pt.wikipedia.org/wiki/Java) [API](http://pt.wikipedia.org/wiki/API) que provê um *framework* para ser utilizado durante a criptografia de dados, geração de chaves, código de autenticação e algoritmos de *Hash*. Ela ainda possui a tarefa de interagir com dispositivos criptográficos como tokens, leitoras de Smart Card, ...), o que foi usado para executar estes programas.
6. Quantas chaves o algoritmo utiliza ? Por que ? Qual o tamanho da chave usada ?
7. O que você pode concluir com este tamanho de chave usado no DES ?
8. Qual o modo de cifra usado ? Poderia existir um modo de cifra mais seguro para este algoritmo ?
9. Veja se consegue executar com outro Modo de Cifra.
10. Curiosidades sobre a **Segurança e Criptoanálise**.

**MOSTRE SEU EXPERIMENTO**

Ao final da aula, deposite sua tarefa no Moodle, no tópico Tarefa 1.

O Moodle será fechado a partir de 22:00 na data desta aula. É a comprovação de sua participação na Tarefa 2 da disciplina.

**CONCLUSÃO**

Para o DES, foram levantadas questões a respeito da suficiência do tamanho de sua chave – 56 bits (mesmo o DES tendo sido adotado como um padrão) e foi o tamanho pequeno de sua chave, frente a criptoanálises teóricas, que ditou a necessidade de mudança de seu algoritmo, e o surgimento de sua substituição no meio comercial para o AES. Veja a seção, **Segurança e Criptoanálise** no DES, em <http://pt.wikipedia.org/wiki/Data_Encryption_Standard> .