### QUESTÕES DE REVISÃO – TÉCNICAS CLÁSSICAS DE CRIPTOGRAFIA, CRIPTOGRAFIA SIMÉTRICA

### O que é um código ?

### O que é uma cifra ?

### Quais são as técnicas de criptografia clássica ?

### O que é uma cifra de transposição ?

### Qual é a finalidade de uma caixa-P ?

### O que é uma cifra de substituição ?

### Qual é a finalidade de uma caixa-S ?

### O que é uma cifra de produto ?

### O que é uma cifra monoalfabética ?

### O que é uma cifra polialfabética ?

### Quais são os ingredientes essenciais de uma cifra simétrica ? Texto claro, algoritmo de criptografia, chave secreta, texto cifrado, algoritmo de decriptografia.

### Quais são os dois requisitos para o uso seguro de criptografia convencional (para diferir de criptografia quântica). Algoritmo de criptografia forte. Uma oponente que conhece o algoritmo e tenha acesso a um ou mais textos cifrados, seja incapaz de decifrar o texto cifrado ou descobrir a chave. Emissor e receptor precisam ter cópias da chave secreta, de forma segura e precisam manter a chave protegida.

### Quantas chaves são necessárias para duas pessoas se comunicarem por meio de uma cifra simétrica ? Uma chave.

### Quais são as duas técnicas gerais para atacar uma cifra ? Criptoanálise e Ataque de força bruta.

### O que é criptoanálise ? É o tipo de ataque que explora as características do algoritmo para tentar descobrir um texto claro específico ou a chave.

### O que é uma ataque de força bruta ? O atacante experimenta cada chave possível em um texto cifrado, até obter uma tradu cão legível do texto claro. Na média, metade de todas as chaves possíveis precisam ser experimentas.

### Quando se analisa a segurança de um algoritmo criptográfico, deve-se especificar que tipo de ataque está sendo considerado. Os objetivos de um criptoanalista são: (a) quebrar um texto ilegível interceptado, ou (b) quebrar a chave K. Liste e defina os tipos de ataques criptoanalíticos com base naquilo que o atacante (o criptoanalista) conhece.

### Há outros tipos de ataque que são aplicáveis em outros cenários e que podem ser compostos com os ataques descritos na lista anterior. São estes:

### (a) Ataque por Repetição: o criptoanalista grava as comunicações legítimas e depois usa parte da gravação para seu proveito. Ataque passivo ou ativo.

### (b) Personificação: o criptoanalista simula um outro usuário legítimo.

### (c) Ataque por dicionário: usado para deduzir senhas quando o criptoanalista tem acesso ao arquivo de senhas criptografadas.

### Qual a diferença entre uma cifra incondicionalmente segura e uma cifra computacionalmente segura ? Incondicionalmente seguro: o texto cifrado não tem informações suficientes para determinar exclusivamente o texto claro. Computacionalmente seguro: o custo para quebrar a cifra é superior ao valor da informação codificada e o tempo exigido para quebrar a cifra é superior ao tempo de vida útil da informação.

### Qual é a finalidade de um modo operação de uma cifra de bloco ?

### O que é Esteganografia ? (não é criptografia)

**USO PRÁTICO DE CRIPTOGRAFIA SIMÉTRICA**

ALGORITMO DES (Data Encryption Standard)

1. Criptografia: Esquema Geral do DES
2. Uma iteração DES
3. A função de iteração
4. Geração de sub-chaves, geradas a partir de uma chave principal de 56 bits.
5. Descrição de caixas S de substituição
6. Decriptografia DES
7. Inverso de uma iteração do DES

Links Interessantes:

[**Encrypting a String with *DES* | Example Depot**](http://www.google.com.br/url?sa=t&source=web&cd=1&ved=0CCAQFjAA&url=http%3A%2F%2Fexampledepot.com%2Fegs%2Fjavax.crypto%2FDesString.html&rct=j&q=DES%20em%20Java&ei=8FKbTb-xM8XUgAe2s8mSBw&usg=AFQjCNEd8tcRD3OoRTbW8XcJwMyGMlCLXw&sig2=cQMP94DvvYn7yvjEIjuHNg&cad=rja)<http://exampledepot.com/egs/javax.crypto/DesString.html>

### [Encrypting a File or Stream with DES | Example Depot](http://www.google.com.br/url?sa=t&source=web&cd=2&ved=0CCgQFjAB&url=http%3A%2F%2Fwww.exampledepot.com%2Fegs%2Fjavax.crypto%2FDesFile.html&rct=j&q=DES%20em%20Java&ei=8FKbTb-xM8XUgAe2s8mSBw&usg=AFQjCNGkcEYNHhyINikZ3Y7Bj_KKrH13lg&sig2=zu7kJ3-vuNIDLRSebHyahg&cad=rja) <http://www.exampledepot.com/egs/javax.crypto/DesFile.html> [DES *« Security «* Java](http://www.google.com.br/url?sa=t&source=web&cd=3&ved=0CDIQFjAC&url=http%3A%2F%2Fwww.java2s.com%2FCode%2FJava%2FSecurity%2FDES.htm&rct=j&q=DES%20em%20Java&ei=8FKbTb-xM8XUgAe2s8mSBw&usg=AFQjCNFvOTzhHazZLpZ2IfCQILw0xwMFuQ&sig2=kV09X7ouGNSABKpLNQ45-Q&cad=rja)<http://www.java2s.com/Code/Java/Security/DES.htm>

### [DESAlgorithm - Java JCE SUN Implementation - herongyang.com](http://www.google.com.br/url?sa=t&source=web&cd=5&ved=0CEYQFjAE&url=http%3A%2F%2Fwww.herongyang.com%2Fcrypto%2Fdes_java_jce_sun_implementation.html&rct=j&q=DES%20em%20Java&ei=8FKbTb-xM8XUgAe2s8mSBw&usg=AFQjCNFuqDCHfESRRzG8aWkcfLK96sSX5g&sig2=e3eKeZLo9aoQaVN2NSrdxA&cad=rja) [www.herongyang.com/.../des\_java\_jce\_sun\_implementation.html](http://www.herongyang.com/.../des_java_jce_sun_implementation.html)

### [Criptografia utilizando algoritmo DES - Curso Classes Java - Parte 28](http://www.google.com.br/url?sa=t&source=web&cd=6&ved=0CE8QFjAF&url=http%3A%2F%2Fwww.devmedia.com.br%2Fpost-17596-Criptografia-utilizando-algoritmo-DES-Curso-Classes-Java-Parte-28.html&rct=j&q=DES%20em%20Java&ei=8FKbTb-xM8XUgAe2s8mSBw&usg=AFQjCNEmkBedRACRW5QGdhYkVicEkg9xCQ&sig2=05GzZzyB_eFixckVTgJDZg&cad=rja) <http://www.devmedia.com.br/post-17596-Criptografia-utilizando-algoritmo-DES-Curso-Classes-Java-Parte-28.html> [DES in java](http://www.google.com.br/url?sa=t&source=web&cd=7&ved=0CFYQFjAG&url=http%3A%2F%2Fwww.velocityreviews.com%2Fforums%2Ft146184-des-in-java.html&rct=j&q=DES%20em%20Java&ei=8FKbTb-xM8XUgAe2s8mSBw&usg=AFQjCNESVXyXB9dp5mS6g7Ei8Oki-vgs0w&sig2=-IblSQ7_WmZMTPF8JffjVw&cad=rja) <http://www.google.com.br/url?sa=t&source=web&cd=7&ved=0CFYQFjAG&url=http%3A%2F%2Fwww.velocityreviews.com%2Fforums%2Ft146184-des-in-java.html&rct=j&q=DES%20em%20Java&ei=8FKbTb-xM8XUgAe2s8mSBw&usg=AFQjCNESVXyXB9dp5mS6g7Ei8Oki-vgs0w&sig2=-IblSQ7_WmZMTPF8JffjVw&cad=rja> USO PRÁTICO DE CRIPTOGRAFIA COM Triple-DES <http://www.rodrigolazoti.com.br/pt/2009/07/06/criptografia-tripe-des-em-java/>

### Crypt  pure-ruby cryptographic ciphers (descreve características de alguns algoritmos criptográficos) <http://crypt.rubyforge.org/index.html> International Data Encryption Algorithm (IDEA) <http://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm> [IDEA NXT](http://www.google.com.br/url?sa=t&source=web&cd=4&ved=0CDwQFjAD&url=http%3A%2F%2Fen.wikipedia.org%2Fwiki%2FIdea_NXT&ei=1lebTefiBcbTgQeu1ZWLBw&usg=AFQjCNEbM6WOLUp-ba51CuPGzRG_9xG0EA&sig2=upGclM4ZeuuuT72J4tgB0A) <http://en.wikipedia.org/wiki/Idea_NXT> CRIPTOGRAFIA COM [Serpent (cipher)](http://www.google.com.br/url?sa=t&source=web&cd=2&ved=0CCQQFjAB&url=http%3A%2F%2Fen.wikipedia.org%2Fwiki%2FSerpent_%28cipher%29&ei=sY2bTfvsHM-H0QGoxo3qAg&usg=AFQjCNFCLXwcOybmKDsy5EzXfm-3xQXNrw&sig2=nLVmiZ74zhmI6nvUZ7SgcQ) <http://en.wikipedia.org/wiki/Serpent_(cipher)>

### [Serpent (GNU cryptographic primitives and tools, version 2.0.0)](http://www.google.com.br/url?sa=t&source=web&cd=9&ved=0CGoQFjAI&url=http%3A%2F%2Fwww.gnu.org%2Fsoftware%2Fgnu-crypto%2Fmanual%2Fapi%2Fgnu%2Fcrypto%2Fcipher%2FSerpent.html&ei=sY2bTfvsHM-H0QGoxo3qAg&usg=AFQjCNFaJGuClGnF_RwSkuOezoAqUEBCxg&sig2=EdKmNEKb9gW8NUBzu_mliQ) [www.gnu.org/.../gnu-crypto/.../crypto/.../Serpent.html](http://www.gnu.org/.../gnu-crypto/.../crypto/.../Serpent.html)

# CRIPTOGRAFIA COM AES Advanced Encryption Standard <http://pt.wikipedia.org/wiki/Advanced_Encryption_Standard> [Criptografia AES - Java e C#](http://www.guj.com.br/java/134647-criptografia-aes---java-e-c) <http://www.guj.com.br/java/134647-criptografia-aes---java-e-c>

# [Using AES with Java Technology](http://www.google.com.br/url?sa=t&source=web&cd=1&ved=0CBgQFjAA&url=http%3A%2F%2Fjava.sun.com%2Fdeveloper%2FtechnicalArticles%2FSecurity%2FAES%2FAES_v1.html&ei=cFybTYusBIfJgQe2toGEBw&usg=AFQjCNHisKpKMzCP2zC2tKPGzoyuopJOpg&sig2=GkyfVVGwpHU3m24BSdlqtw) <http://java.sun.com/developer/technicalArticles/Security/AES/AES_v1.html> AES String Encryption <http://www.example-code.com/java/aes_stringEncryption.asp>

### [Using AES Crypt - Advanced File Encryption for Java](http://www.google.com.br/url?sa=t&source=web&cd=6&ved=0CFIQFjAF&url=http%3A%2F%2Fwww.aescrypt.com%2Fjava_aes_crypt.html&ei=cFybTYusBIfJgQe2toGEBw&usg=AFQjCNGdAbk5NoVgIu8NvpyoGMr3wIFoug&sig2=a_ceYLPaa9crLG8qNWgvEQ) <http://www.aescrypt.com/java_aes_crypt.html> Encryption and decryption with AES/ECB/PKCS7Padding <http://www.java2s.com/Code/Java/Security/EncryptionanddecryptionwithAESECBPKCS7Padding.htm>

### Cryptographic Algorithms (Interessante !!!) <http://www.kremlinencrypt.com/algorithms.htm>

### [UK Mirror Service: sites/ftp.wiretapped.net/pub/security ...](http://www.google.com.br/url?sa=t&source=web&cd=8&ved=0CGIQFjAH&url=http%3A%2F%2Fwww.mirrorservice.org%2Fsites%2Fftp.wiretapped.net%2Fpub%2Fsecurity%2Fcryptography%2Falgorithms%2Fserpent%2Fserpent-c-bgladman%2F&ei=sY2bTfvsHM-H0QGoxo3qAg&usg=AFQjCNHHKKsmS0EetJTd8WMy9UoZukS7Kg&sig2=ygmgpnszg0DywX-KSIPNQA) (Importante) <http://www.google.com.br/url?sa=t&source=web&cd=8&ved=0CGIQFjAH&url=http%3A%2F%2Fwww.mirrorservice.org%2Fsites%2Fftp.wiretapped.net%2Fpub%2Fsecurity%2Fcryptography%2Falgorithms%2Fserpent%2Fserpent-c-bgladman%2F&ei=sY2bTfvsHM-H0QGoxo3qAg&usg=AFQjCNHHKKsmS0EetJTd8WMy9UoZukS7Kg&sig2=ygmgpnszg0DywX-KSIPNQA> Criptografia de Disco <http://www.madeira.eng.br/wiki/index.php?page=Criptografia+de+Disco+%E2%80%93+Garantindo+a+seguran%C3%A7a+de+suas+informa%C3%A7%C3%B5es>

### [Linux: Criptografia de disco [Artigo]](http://www.google.com.br/url?sa=t&source=web&cd=2&ved=0CB8QFjAB&url=http%3A%2F%2Fwww.vivaolinux.com.br%2Fartigo%2FCriptografia-de-disco%2F&ei=z9ecTfzTJ9SP0QHKqZzpAg&usg=AFQjCNEKG9A39WnBXhwB723vsLkZcvtPHw&sig2=DC9V4rBM5MXJWXmAGJZjcA) <http://www.vivaolinux.com.br/artigo/Criptografia-de-disco/>