Quiz3

Criptografia

O e-mail do participante (**igor.ribeiro@unifesp.br**) foi registrado durante o envio deste formulário.

Sobre criptografia, assinale as alternativas corretas:

- [x] Cifra de César consiste em substituir letras de um texto claro através do deslocamento de caracteres.
- [ ] O one-time-pad é uma cifra de fluxo que utilizam chaves aleatórias de tamanho fixo.
- [ ] Cifras de bloco cifram um texto claro seqüencialmente byte a byte formando um único bloco cifrado
- [x] Em uma estrutura de cifra de Feistel o número de rodadas pode ser variável sendo essa variação totalmente independente do tamanho das chaves utilizadas.
- [x] O DES utiliza a estrutura de cifra de Feistel para realizar a cifra de blocos.

Sobre DES e AES, assinale as alternativas corretas.

- [x] O DES foi considerado vulnerável a ataques de força bruta, isso motivou o desenvolvimento do 3-DES.
- [x] O 3-DES é considerado vulnerável ao ataque do homem-do-meio.
- [x] O algoritmo atual AES (Advanced Encryption Standard) foi escolhido entre vários outros algoritmos após um concurso e possui como característica utilizar blocos de cifras com tamanho de 128 bits.
- [ ] O AES usa estrutura de cifras de Feistel e chaves de tamanho variável.
- [ ] O AES quanto o DES podem são classificados como cifradores de fluxo.

Resposta correta

- [x] O DES foi considerado vulnerável a ataques de força bruta, isso motivou o desenvolvimento do 3-DES.
- [x] O algoritmo atual AES (Advanced Encryption Standard) foi escolhido entre vários outros algoritmos após um concurso e possui como característica utilizar blocos de cifras com tamanho de 128 bits.

No S-DES, considerando K = 1010100111 qual seria o valor de k1:

- (●) 10101110
- ( ) 10101111
- ( ) 10101101
- ( ) 11001110
- ( ) 10100111

Usando criptografia de chave pública, suponha que Bob quer enviar uma mensagem secreta a Alice e, Alice, quer certificar-se de que a mensagem foi realmente enviada por Bob. Então Bob deve:

- ○ Cifrar a mensagem com a chave pública de Alice, cifrar o resultado com sua chave pública e então enviar a mensagem.
- ◉ Cifrar a mensagem com sua chave privada, cifrar o resultado com a chave pública de Alice e então enviar a mensagem.
- ○ Cifrar a mensagem com sua chave privada, cifrar o resultado com a chave privada de Alice e então enviar a mensagem.
- ○ Cifrar a mensagem com sua chave pública, cifrar o resultado com a chave pública de Alice e enviar a mensagem
- ○ NDA

Considere uma transmissão massiva de dados em rede entre duas entidades A e B, em que elas não compartilham qualquer informação sobre chaves a priori. Para maximizar o desempenho de transmissão e utilizando criptografia visando a confidencialidade dos dados, qual seria a combinação de algoritmos mais eficiente?

- ○ AES, RSA e DH
- ○ RC4 e DH
- ○ DES e RC4
- ◉ AES e RSA
- ○ RSA, RC4 e DH

Resposta correta

- ◉ RC4 e DH