INE5429 - Prova 1

prof. Ricardo Felipe Custódio

2 de maio de 2013

10 - 0,3

MOSTRE TODOS OS CÁLCULOS

1,0 1. (1,0) Cifre, usando o Playfair, a palavra "FLORIANOPOLIS", usando como chave seu último nome.

2. (1,0) Quanto a uma Cifra Simétrica:

0,0 (a) Qual é sua complexidade, sabendo que B e L são a quantidade de bits do bloco de entrada e da chave, respectivamente?

(b) Quando podemos considerar que uma cifra simétrica foi quebrada?

3. (2,0) Com o S-DES:

0,7 (a) Cifre, mostrando todos os passos, usando o S-DES, o número 33. Como chave utilize o número $(k+9)$, onde k é o dígito menos significativo do seu número de matrícula;

0,0 (b) Usado esse resultado, determine o efeito avalanche. Determine somente um valor e explique como obter um valor médio.

4. (1,5) Quanto ao PGP, explique com suas palavras

0,0 (a) como são criados e gerenciados os certificados digitais PGP;

0,0 (b) Por que e até quanto podemos confiar em um certificado PGP?

1,0 (c) Quando um certificado PGP expira?

0,0 (d) O que é necessário fazer para revogar um certificado PGP?

0,0 (e) É possível revogar uma assinatura digital que você colocou no certificado de alguém? Se sim, como isso é feito?

5. (1,0) Sobre sigilo de documentos ou mensagens:

0,0 (a) Dado um documento de 2 MBytes, o que deve ser feito para se enviar este documento de forma sigilosa para um destinatário?

(b) E se for para $n > 1$ destinatários, qual seria a forma mais indicada e por que?

(c) Como você faria, numa empresa, para que os documentos sigilosos de um funcionário possam ser (sempre) lidos (decifrados) também pelo dono da empresa?

0,0 6. (1,0) Por que a assinatura digital de uma mensagem também garante sua integridade?

0,0 7. (1.0) Explique o modo de operação Contador (*Counter Mode*). Compare este modo de operação com os outros modos de operação estudados em termos de: numero de operações booleandas; perda de bits dos blocos cifrados; o serviço oferecido seria de cifrador em cadeia ou cifrado de bloco (explique)?

MOSTRE TODOS OS CÁLCULOS

Boa Sorte