Nome: _____	**Matrícula:** _____	**Nota:** _____
Disciplina: Criptografia	**Período:** **Prova (P1)**	
Professor: Frederico Sauer	**Data:** **08/10/2014**	**Ass. Professor**
Curso: MBA em Gestão da Segurança da Informação		

Esta avaliação será SEM CONSULTA e SEM USO DE CALCULADORA E OUTROS RECURSOS COMPUTACIONAIS, a menos que sua utilização seja autorizada abaixo

Recursos permitidos nesta prova:	**SIM**	**NÃO**	Observações do Professor para os alunos e/ou aplicador da prova:
Consulta ao Material Didático		**X**	A prova é composta de um texto com incorreções. Estas devem ser identificadas e numeradas, e nas linhas de comentário o aluno deve indicar a correção para os erros encontrados
Utilização de Calculadora		**X**	
Outros. Especificar:		**X**	

ATENÇÃO !

1. O aluno que responder a lápis, esta prova, total ou parcialmente, perderá o direito a solicitar revisão.
2. Não é permitido destacar folhas da prova. Todas as folhas deverão ser devolvidas junto com a prova.
3. Apenas os alunos cujos nomes constem na lista de freqüência (ou seja, que estejam regularmente matriculados na disciplina) podem realizar esta prova.
4. Quando solicitado pelo aplicador da prova, o aluno deverá apresentar documento de identificação com foto.
5. **A interpretação das questões faz parte da prova.**
6. Não é permitido sair de sala nos primeiros 40 minutos do início da prova. Após esse tempo, o aluno que sair de sala estará necessariamente concluindo a sua prova.
7. Não será permitido que alunos iniciem a prova **APÓS** a saída do primeiro aluno da sala.
8. **Ao terminar a prova, o aluno deve permanecer sentado e solicitar ao professor que a recolha.**
9. **A lista de freqüência deve ser assinada pelo aluno no momento em que pegar a prova. Não é permitida a saída de sala sem assinar a lista.**
10. A leitura das orientações para a realização de provas é obrigatória e deve ser realizada por todos os alunos.

Secretaria Acadêmica

Declaro estar ciente dos procedimentos acima

_____

Assinatura do aluno

Questão 01:

O texto abaixo contém incorreções conceituais. Você deve identificá-las e numerá-las, indicando no espaço para comentários como seria correto.

Alice e Bob são Analistas da Petrobras e foram incumbidos de planejar o robustecimento dos seguintes serviços de TI, com o uso de recursos criptológicos e de certificação digital:

a) Nuvem privada;

b) Email corporativo; e

c) Uso de aplicações corporativas em ambiente web.

Bob sugere à Alice que sejam adotadas a Criptografia Simétrica e a Assimétrica, bem como o apoio de Certificados Digitais emitidos pela própria Petrobras, uma vez que a mesma é Autoridade Certificadora.

Na elaboração do projeto, foram decididos pelos seguintes produtos:

A. **Para criptografia simétrica será adotado o DES, que dará a possibilidade de chaves de 128, 192 ou 256 bits e blocos de 128 bits**(1), com a melhor combinação de desempenho, complexidade e robustez entre os algoritmos simétricos;

B. Para criptografia assimétrica, o **RSA**(2), que é **a solução assimétrica com o melhor desempenho entre os algoritmos assimétricos** atualmente disponíveis e **com demanda de chaves menores que os demais** para nível de segurança equivalente;

C. Para certificados digitais, será adotado o **mais atual de todos, que é o padrão X.509 versão 1**(3a). As chaves armazenadas nestes certificados, denominadas **chaves privadas**(3b), devem ser de no **mínimo 128 bits**(3c).

No esboço das linhas gerais da segurança dos três serviços a serem oferecidos, foram definidos os seguintes requisitos:

I. Nuvem privada:

- ✓ Todos os dados classificados como sensíveis deverão ser mantidos criptografados **com criptografia assimétrica**(4), para garantir menor latência na recuperação e independência do tamanho da informação a ser criptografada; e
- ✓ O acesso aos dados na nuvem será feito exclusivamente mediante mecanismo de autenticação baseado na **criptografia simétrica**(5), com o uso dos respectivos certificados digitais de cada usuário.

II. Email corporativo:

- ✓ Será adotado um sistema onde todos os email serão criptografados e autenticados, usando **apenas a criptografia assimétrica**(6).

III. Uso de Aplicações corporativas em ambiente WEB:

- ✓ O ambiente padronizado para o e-commerce (SSL/TLS) será mantido, porém, para evitar a possibilidade do ataque do *man-in-the-middle*, serão fixados os seguintes requisitos:

i. Não será admitido o uso do Diffie-Hellmann. Em seu lugar, para troca de chaves, será usada a criptografia assimétrica, da seguinte forma:

1. O origem gera um número randômico de **56 bits**[7], que será a chave secreta para criptografia do tráfego;
2. O origem criptografa esta chave com a sua chave **pública**[8], para autenticar a chave, e em seguida com a chave **privada**[9] do destino, para garantir a sua confidencialidade**;**
3. O origem envia esta chave para o destino, que ao recebê-la, a decriptografa com a sua própria chave **pública**[10] e verifica a sua autenticidade, usando a chave **privada**[11] do emissor;

ii. Informações sensíveis serão criptografadas fim-a-fim, ou seja, o campo ficará bloqueado até a aplicação de destino, quando o usuário deverá usar seu certificado para provar sua identidade e obter a chave simétrica usada para criptografá-la[12];

✓ A **criptografia (confidencialidade)** do tráfego da sessão SSL será feita com **criptografia assimétrica (RSA)**[13].

1. Com a ressalva de que deve ser a melhor combinação entre desempenho, robustez e complexidade, a única resposta admissível substitui DES por AES;
2. Solução ideal: substituir o RSA pelo ECC. Outra opção é corrigir, dizendo que o RSA tem desempenho e tamanho de chaves aceitáveis, apesar de não serem os melhores atualmente;
3. 3 erros na assertiva:
    a. O padrão atual é a versão 3;
    b. As chaves nele armazenadas são as chaves PÚBLICAS; e
    c. Se você escolheu trocar pelo ECC na questão anterior, o tamanho mínimo da chave, ficará entre 160 bits a 256 bits. Se manteve RSA, no mínimo 1024 bits até 4096 bits são aceitáveis.
4. Criptografia SIMÉTRICA.
5. Criptografia ASSIMÉTRICA.
6. Criptografados com criptografia SIMÉTRICA e autenticados com criptografia ASSIMÉTRICA.
7. No mínimo 128 bits.
8. PRIVADA.
9. PÚBLICA.
10. PRIVADA.
11. PÚBLICA.

12. Questão mal redigida, ANULADA. O erro seria que, para obter a chave simétrica usada para criptografar a informação o usuário deveria usar a sua chave PRIVADA, e não a chave contida no certificado que é a PÚBLICA.
13. Duas formas possíveis de corrigir:
    a. Trocar apenas de “criptografia (confidencialidade)” para “autenticação (autenticidade)”; ou
    b. Manter criptografia, mas trocar a parte final grifada por CRIPTOGRAFIA SIMÉTRICA (AES).