MINISTÉRIO DA CIÊNCIA E TECNOLOGIA (MCT)

CONCURSO PÚBLICO

NÍVEL SUPERIOR

CADERNO DE PROVAS – PARTE II

CONHECIMENTOS ESPECÍFICOS

Aplicação: 30/11/2008

CARGO:

TECNOLOGISTA JÚNIOR I (Y2)

ATENÇÃO!

» Leia atentamente as instruções constantes na capa da Parte I do seu caderno de provas.

» Nesta parte do seu caderno de provas, que contém os itens relativos à prova objetiva de **Conhecimentos Específicos**, confira inicialmente os seus dados pessoais transcritos acima. Em seguida, no rodapé de cada página numerada desta parte do caderno de provas, confira o seu nome e o código do seu cargo.

AGENDA (datas prováveis)

I **2/12/2008**, após as 19 h (horário de Brasília) – Gabaritos oficiais preliminares das provas objetivas: Internet — www.cespe.unb.br.

II **3** e **4/12/2008** – Recursos (provas objetivas): exclusivamente no Sistema Eletrônico de Interposição de Recurso, Internet, mediante instruções e formulários que estarão disponíveis nesse sistema.

III **30/12/2008** – Resultado final das provas objetivas e resultado provisório da prova discursiva: Diário Oficial da União e Internet.

IV **2** e **3/1/2009** – Recursos (prova discursiva): exclusivamente no Sistema Eletrônico de Interposição de Recurso, Internet, mediante instruções e formulários que estarão disponíveis nesse sistema.

V **26/1/2009** – Resultado final da prova discursiva e convocação para a entrega de documentos para a avaliação de títulos: Diário Oficial da União e Internet.

OBSERVAÇÕES

- Não serão objeto de conhecimento recursos em desacordo com o item 15 do Edital n.º 1 - MCT, de 28/8/2008.
- Informações adicionais: telefone 0(XX) 61 3448-0100; Internet – www.cespe.unb.br.
-

cespeUnB
Centro de Seleção e de Promoção de Eventos

De acordo com o comando a que cada um dos itens de **71** a **120** se refira, marque, na **folha de respostas**, para cada item: o campo designado com o código **C**, caso julgue o item **CERTO**; ou o campo designado com o código **E**, caso julgue o item **ERRADO**. A ausência de marcação ou a marcação de ambos os campos não serão apenadas, ou seja, não receberão pontuação negativa. Para as devidas marcações, use a **folha de respostas**, único documento válido para a correção das suas provas.

CONHECIMENTOS ESPECÍFICOS

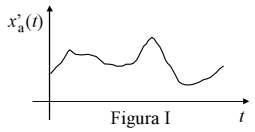


Figura I

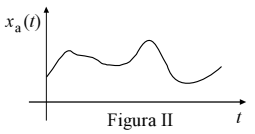


Figura II

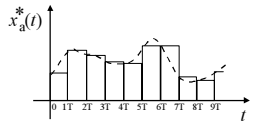


Figura III

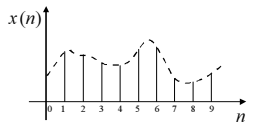


Figura IV

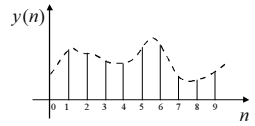


Figura V

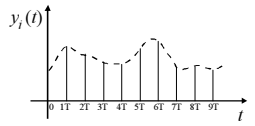


Figura VI

Considerando as figuras de I a VI acima, que apresentam gráficos de sinais no domínio do tempo, julgue os itens que se seguem.

71 A figura II pode ser a representação correta do sinal da figura I depois de este sinal — x' a (t) — ter passado por um filtro passa-baixas.

72 Do gráfico da figura II para o da figura III, o sinal pode ter passado por um processo de amostragem-e-retenção.

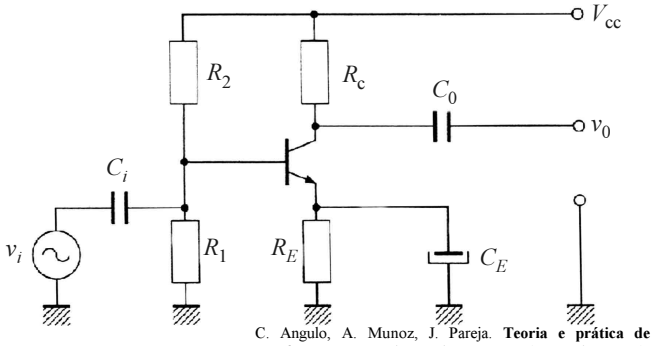
73 Considerando que o sinal mostrado no gráfico da figura V tenha passado por um processamento para obter o sinal do gráfico da figura IV, é possível que tenha havido uma etapa de inversão de fase e de rebatimento do sinal.

74 O gráfico da figura VI apresenta a transformada de Fourier do sinal do gráfico da figura V.

Com relação a sistemas digitais e a arquitetura de processadores digitais, julgue os próximos itens.

75 Memória, unidade de controle, registradores e unidade lógica e aritmética são elementos constituintes da arquitetura de um computador.

76 Um registrador, que pode ser formado por um conjunto de *flip-flops* sincronizados pelo mesmo relógio, possui a capacidade de armazenar informação. De maneira genérica, um computador pode ser definido como um conjunto de registradores comandados.



C. Angulo, A. Munoz, J. Pareja. **Teoria e prática de eletrônica**. São Paulo: Makron, 1993 (com adaptações).

No esquema elétrico da figura acima, R_1, R_2, R_c e R_E são resistores, C_i, C_0 e C_E são capacitores e V_{CC}, v_o e v_i são tensões elétricas. Considerando esse circuito, julgue os itens que se seguem.

77 Os capacitores C_i e C_E determinam a freqüência de oscilação do circuito.

78 O capacitor C_0 permite que a saída v_0 fique estabilizada, caso haja oscilações na alimentação V_{cc}.

79 Os quatro resistores auxiliam na determinação do ponto de operação do transistor, que está na topologia do tipo coletor comum.

Acerca de circuitos elétricos e eletrônica digital, julgue os itens a seguir.

80 Circuitos combinacionais podem ser construídos utilizando-se portas lógicas, sendo que a saída é função apenas da entrada. De outra forma, circuitos seqüenciais podem estar embasados em *flip-flops*, sendo que seu estado lógico depende das entradas atuais e passadas.

81 O leiaute de um circuito integrado define as geometrias das máscaras usadas no processo de fabricação. Algumas regras de projeto são: largura mínima, espaçamento mínimo, margem mínima e extensão mínima.

82 Os FPGAs (*field programmable gate arrays*) são dispositivos adequados para uso em prototipação de projetos de lógica digital e analógica. As principais vantagens desses dispositivos são a capacidade de personalização, o baixo custo de projeto e o alto desempenho desses componentes em comparação com outras soluções VLSI, que permitem integração em larga escala.

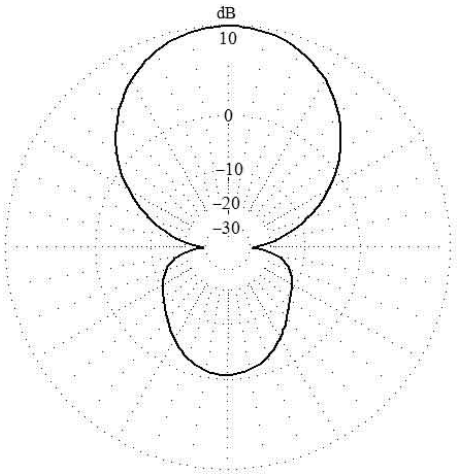
No referente a redes de comunicação de dados, julgue os itens subseqüentes.

83 No campo da criptografia, a criptoanálise diferencial analisa a evolução da diferença — operação de E de três *n*-gramas — entre duas mensagens conhecidas e cifradas com a mesma chave durante o processo de criptografia. A criptoanálise linear é uma técnica que se vale de convoluções lineares equivalentes ao algoritmo criptográfico.

84 O *frame-relay* é uma tecnologia de transmissão de dados que compartilha o meio e a banda de transmissão entre vários usuários, sendo que os pacotes são encaminhados ao destino por canais virtuais controlados por protocolo.

85 Na fase de elaboração de um projeto de rede de dados, devem ser analisados certos aspectos e necessidades como, por exemplo, os tempos de conexão e desconexão, a taxa de erro nas células transmitidas, a taxa de células perdidas e o tempo de retardo na propagação da célula.

Considere que um satélite de comunicação esteja em órbita geoestacionária, a 36.000 km de altura da Terra. Seu transmissor entrega 40 W à antena transmissora, que é assumida isotrópica com eficiência de 90%. O sinal transmitido é recebido por uma antena na Terra, que tem eficiência de 100% e cuja característica de radiação está mostrada na figura a seguir. O sistema trabalha em uma freqüência de 2 GHz, em condições de casamento de polarização entre as antenas transmissora e receptora.



Considerando a situação hipotética apresentada, julgue os itens de **86** a **90**.

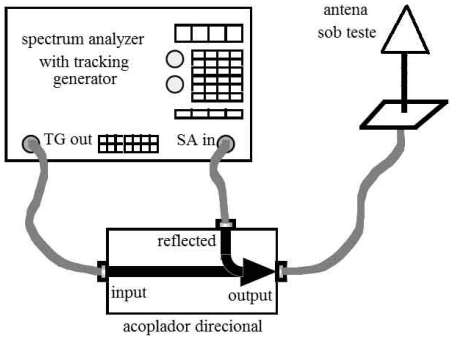
86 Na situação mencionada, a densidade de potência incidente na antena receptora é superior a $10^{-15}\ \mathrm{W \cdot m^{-2}}$.

87 A característica de radiação da antena na figura é compatível com o diagrama de radiação no plano-E de uma antena Yagi-Uda. Portanto, é correto inferir que a estação terrena pode estar usando uma antena desse tipo, a qual, na situação apresentada, tem ganho máximo de 10 dB com relação à antena isotrópica.

88 Para a onda eletromagnética transmitida pelo satélite na posição da antena de recepção, é correto afirmar que, em módulo, o campo elétrico tem a mesma intensidade do campo magnético.

89 Se a característica da antena mostrada na figura se refere a uma corneta cônica de comprimento *L* e raio de abertura *a*, então, para aumentar a diretividade dessa antena, é correto diminuir a dimensão *a*.

90 A figura a seguir ilustra um arranjo que permite avaliar se uma antena está corretamente sintonizada na freqüência desejada. Na freqüência em que ocorre a sintonia, a leitura do analisador de espectro (*spectrum analyzer*) deve indicar um valor de potência muito inferior, em relação à situação em que a antena é desconectada do acoplador direcional.



Com relação a sistemas de comunicação, julgue os itens seguintes.

91 Entre as técnicas de modulação linear, encontra-se a denominada *frequency modulation* (FM), que tem como uma de suas principais características ser imune a distorções não-lineares provocadas por amplificadores de potência, principalmente se o sinal FM for de faixa estreita e a amplificação for em classe F.

92 Em sistemas de microondas em visibilidade na primeira zona de Fresnel, quanto maior for um enlace interligando duas torres de comunicação, normalmente maior será a probabilidade de ocorrência de desvanecimento por múltiplos percursos.

93 Na modulação digital *M*QAM, quanto maior *M* menor a banda ocupada pelo sinal modulado, mantendo-se a taxa de transmissão constante.

94 Em canais de comunicação *wireless*, banda coerente designa a banda essencial de um sinal modulado que deve ser protegida por interferência por canal adjacente.

95 O uso de sistemas MIMO (*multiple input multiple output*) permite tanto ganho de diversidade quanto ganho de multiplexação monousuário e multiusuário, desde que esses sistemas sejam devidamente projetados.

RASCUNHO

Julgue os itens de **96** a **109**, acerca de tecnologias, protocolos, medidas administrativas e normas referentes à segurança dos sistemas de informação computacional e das redes de comunicação.

96 Na arquitetura do *secure socket layer* (SSL), são providos dois protocolos; o protocolo de sessão, destinado a fazer uso do *transmission control protocol* (TCP) para prover um serviço confiável fim-a-fim; e o protocolo de registro, destinado a prover capacidade mínima de autenticação de mensagens do *user datagram protocol* (UDP).

97 Na arquitetura de segurança do internet protocol (IP) — IPSec —, a associação de segurança é um relacionamento bidirecional entre um emissor e um receptor, que é identificada pelo número do soquete da aplicação usuária.

98 O Internet *security association key management protocol* (ISA KMP) pode ser usado para a automação da gerência de chaves criptográficas entre o emissor e o receptor no IPSec.

99 O sistema *kerberos* emprega um serviço de autenticação de uma terceira parte confiável para permitir a sistemas, clientes e servidores o estabelecimento de comunicações autenticadas.

100 A secure/multipurpose Internet *mail extension* (S/MIME) permite agregar uma assinatura digital a uma mensagem de correio eletrônico, o que torna essa mensagem incompatível com a proteção provida pelo *authentication header* (AH) do IPSec.

101 Na configuração de *firewall* denominada *screened subnet*, o roteador externo anuncia à rede externa somente a existência da sub-rede que o liga ao roteador interno, na qual podem estar presentes hospedeiros de guarda (*bastião*) e outros serviços de informação.

102 Para dificultar a um intruso a instalação de um programa mal-intencionado em um servidor *proxy* instalado em uma zona desmilitarizada na entrada de uma rede, o programa do *proxy* deve evitar, na medida do possível, os acessos ao disco no hospedeiro em que se encontra.

103 A contramedida que consiste em o *firewall* descartar todos os pacotes que usam a opção *source routing* visa proteger o hospedeiro cliente da comunicação contra a captura pelo servidor de dados privados do cliente.

104 O verme (*worm*) computacional Nimda é capaz de se propagar utilizando múltiplos mecanismos, como correio eletrônico, áreas de compartilhamento de aplicações distribuídas, exploração de falhas em servidores do *hypertext transfer protocol* (HTTP) e acesso de portas de entrada escondidas em sistemas operacionais.

105 Um vírus de macrocomandos de uma aplicação, como, por exemplo, um editor de textos, é independente da plataforma computacional e dos sistemas operacionais.

106 A contramedida que consiste em varrer portas de servidores locais para descobrir serviços que estão indevidamente ativos é um dos modos efetivos de realizar o rastreamento e a identificação das fontes de ataque do tipo negação de serviço distribuído.

107 O esquema de senhas de vários sistemas da família Unix, em que o sistema armazena em um arquivo cada senha cifrada com o algoritmo DES modificado pela presença de um parâmetro de *salt* é vulnerável a ataques que têm base na utilização de dicionários.

108 O *secure hash algorithm* (SHA) — padrão federal dos Estados Unidos da América FIPS 180 — aplica como função de uma via uma curva elíptica parametrizável em função do tamanho da mensagem da qual se deseja um resumo.

109 Segundo o padrão FIPS 180-2, os algoritmos SHA-384 e SHA-512 operam com tamanho de bloco de entrada de 1.024 *bits*.

Acerca das infra-estruturas de chaves públicas (ICP) e dos protocolos, algoritmos e normas a elas subjacentes, julgue os itens seguintes.

110 Todo certificado X.509 possui um campo de assinatura que contém o *hash* dos demais campos do certificado. Esse *hash* é cifrado com a chave privada do usuário ao qual o certificado se refere.

111 Na *public key infrastructure* X.509 (PKIX), o processo de registro é definido como sendo aquele em que uma autoridade certificadora (CA) se registra junto a outra CA, tornando-se a primeira uma CA subordinada à segunda.

112 O algoritmo de chave pública RSA pode ser utilizado nos processos de registro, assinatura e revogação de certificados da PKIX.

113 Uma das extensões de certificados da versão 3 do X.509 permite indicar uma restrição imposta ao propósito de uso do certificado, ou à política sob a qual a chave pública pode ser usada.

Julgue os itens que se seguem acerca da arquitetura e do gerenciamento dos sistemas de detecção de intrusão (*intrusion detection systems* — IDS).

114 Na abordagem de detecção estatística de anomalias, definem-se regras de comportamento a serem observadas para decidir se determinado comportamento corresponde ao de um intruso.

115 A utilização de registros de auditoria como entrada para um sistema de detecção de intrusão pode-se dar com os registros nativos de sistemas e aplicações, ou com registros gerados com informações específicas da detecção de intrusão.

116 A medição do tempo decorrido desde o último *login* é um indicador significativo para a detecção de tentativas de quebra de uma conta de sistema operacional ociosa.

Acerca das normas nacionais e internacionais relativas à segurança da informação, bem como da gestão de riscos de sistemas de informação, julgue os itens seguintes.

117 Segundo a norma ISO 27002, a análise de riscos deve ser repetida periodicamente, de modo a levar em conta quaisquer modificações que tenham influenciado os resultados de análise de riscos feita anteriormente.

118 O interesse das pessoas, a educação e o treinamento quanto à segurança da informação constituem controles considerados, do ponto de vista legislativo, como essenciais para uma organização, segundo a norma ISO 27002.

119 A norma ISO 27001 adota o modelo *plan-do-check-act* (PDCA), que é aplicado para estruturar todos os processos dos sistemas de gestão de segurança da informação — *information security management system* (ISMS).

120 Dependendo de seu tamanho ou natureza, uma organização pode considerar um ou mais requisitos da norma ISO 27001 como não-aplicáveis e, ainda assim, continuar em conformidade com essa norma internacional.