

姓名 \_\_\_\_\_  
学籍番号 \_\_\_\_\_  
学部 \_\_\_\_\_  
クラス \_\_\_\_\_  
科目番号 \_\_\_\_\_  
担当教員 \_\_\_\_\_

大連理工大学

科目名: コンピュータネットワーク 問題種類: A 試験形式: 閉巻  
所属学部: 国際情報ソフトウェア学部 試験の実施日: \_\_\_\_\_ 年 \_\_\_\_\_ 月 \_\_\_\_\_ 日  
問題用紙合計ページ数 6

	一	二	三	四	五						合計
配点	20	20	30	20	20						100
得点											

得点	
----	--

一、インターネットの発展の歴史に関する以下の説明文について、空欄(1)～(10)に入る適切な用語を以下の語群(a)～(s)から選択し、その記号を解答欄に記入せよ。

インターネットの起源は、軍事的攻撃を受けても維持できる( 1 )の通信網の必要性から米国防総省の研究機関( 2 )によって研究、開発が進められた( 3 )方式のコンピュータネットワーク( 4 )である。( 4 )は1969年に構築されてから年々接続拠点を増やし、1978年には実験が正式に完了し、実験ネットワークから運用ネットワークへ移行した。( 4 )は、さらに成長を続け、1980年代後半から全米科学財団(NSF: National Science Foundation)の資金援助を受けた( 5 )に継承され、1990年に正式に解散した。

その一方で、1990年代に入り商用インターネット接続が登場し、一般の人でも( 6 )でインターネットにアクセスできるようになった。1991年には、( 7 )という研究機関により、ネットワーク全体を( 8 )により相互参照することで1つの文書データベースとして取り扱う( 9 )が開発された。イリノイ大学のNational Center for Supercomputing Applicationsにより開発されたブラウザである( 10 )によって、( 7 )は世界中に爆発的に普及することになった。

語群:  
(a) ARPA, (b) ARPANET, (c) CERN, (d) JUNET, (e) Mosaic, (f) Netscape, (g) NSFNET, (h) OSI, (i) TCP/IP, (j) WWW, (k) 回線交換, (l) シンボリックリンク, (m) ダイアルアップ, (n) 集中型, (o) ハイパーリンク, (p) パケット交換, (q) 分散型,

(1)	(2)	(3)	(4)	(5)
(6)	(7)	(8)	(9)	(10)

得点	
----	--

二、インターネットを支える技術に関する以下の説明文に該当する用語を語群から選択して解答欄に記入せよ。

- (1) ネットワーク上の全てのコンピュータに対して行われる通信のこと。
- (2) イーサネットの伝送メディアとして使われるケーブルの1つであり、2本1組の、より対線4組で構成されており、LANケーブルとして最も多く使用されている。
- (3) 子機同士が直接通信を行う無線LANの通信モードの1つ。
- (4) LAN上に他のコンピュータから送信されたパケットがあるか確認せず、送信の準備ができたなら、すぐにパケットを送信する方式。
- (5) システムや特権ユーザのプロセスのみが使うことができる0～1023のポート番号であり、ネットワーク全体で広く提供されているサービスの通信プロセスに割り当てられている。
- (6) 通信を開始する際に行うコネクションを確立する処理のことであり、送信側と受信側の間で3ステップにより行われる処理のこと。
- (7) WWWのアプリケーション層が使用するプロトコルであり、WWWサーバとクライアントの間の通信に用いられる。このプロトコルは、トランスポート層はTCPを用いており、基本的にはポート番号80が使用されている。
- (8) 電子メールの送信のために使用されるプロトコルであり、クライアントからサーバに対してメッセージを送信する場合や、サーバ間でメッセージを中継する場合に用いられる。
- (9) 暗号化と復号に別個の鍵を使い、復号鍵をネット上に送信すること無く暗号化できるようにした暗号方式。
- (10) 複数の異なるデジタル信号を時間的に配列して、一つの伝送路で伝送を行うことができるようにする方式。

#### 語群

・1-persistent CSMA ・ALOHA ・HTML ・HTTP ・ICANN ・IEEE802.11n ・IETF ・IPアドレス ・IRTF ・ISO ・MACアドレス ・POP ・RFC ・TCP ・UDP ・URL ・アドホックモード・インフラストラクチャモード ・周波数分割多重方式 ・エニーキャスト ・キャリアセンス ・コネクション ・時分割多重方式 ・コネクション指向 ・コミュニケーション ・UTP ケーブル ・ピアツーピア ・3ウェイハンドシェイク (three-way handshaking) ・ウェルノウンポート(well-known ports) ・ブロードキャスト ・マルチキャスト ・メディアアクセス制御 ・ユニキャスト ・リピータ ・ルーティング ・公開鍵暗号方式

#### 解答欄

(1)	(2)	(3)	(4)	(5)
(6)	(7)	(8)	(9)	(10)

得点	
----	--

三、ネットワーク層のプロトコルである IP について，以下の問いに答えよ．

問 1. あるネットワークに接続しているコンピュータに，IP アドレスが「123. 33. 44. 56」，サブネットマスクが「255. 255. 255. 192」と設定されている．このとき，以下の問題に答えよ．なお，計算の途中経過も書くこと．

(1) このネットワークのネットワークアドレスを 10 進数で表記せよ．

解答

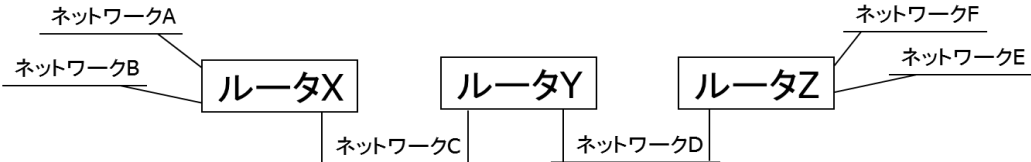
(2) IP アドレスが「112. 33. 44. 65」，サブネットマスクが「255. 255. 255. 192」と設定されているコンピュータは，このネットワークに接続できるか答えよ．

解答

(3) このネットワークに接続できるホストの最大数を求めよ．

解答

問 2. 下図のような接続関係にあるルータ X, Y, Z 内に保持されるルーティングテーブルが距離ベクトルアルゴリズムにより更新されているものとする．時刻 t=0 から 2 までの状態遷移を下表の空欄に記載せよ．ただし，必要のない空欄は／を引いて削除せよ．

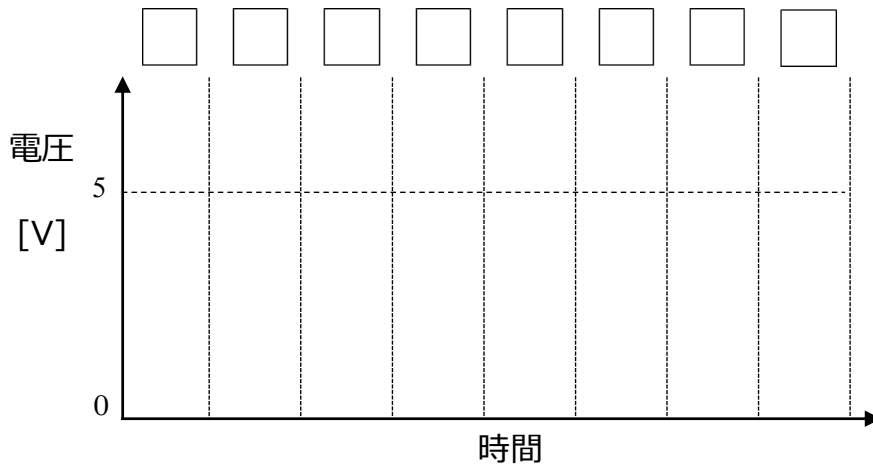


	ルータ X のルーティング テーブル			ルータ Y のルーティング テーブル			ルータ Z のルーティング テーブル		
	ネットワー ク名	ルータ名	距離 (ホップカウント)	ネットワー ク名	ルータ名	距離 (ホップカウント)	ネットワー ク名	ルータ名	距離 (ホップカウント)
t=0 初期状態	A	X	0						
	B	X	0						
	C	X	0						
t=1									
t=2									

得	
点	

四、符号化，誤り制御に関する以下の問いに答えよ．

問 1. 送信データ 116 を 2 進数に変換して□に記入した上でマンチェスタ符号により電圧の変化を符号化して図示せよ．ただし，0 は 5V から 0V，1 は 0V から 5V の変化で表し，下位ビットから順に送信するものとする．



問 2. 送信者は受信者との間で，偶数パリティによるシングルパリティチェックにより誤り検出を行っている．このとき，以下の問いに答えよ．

(1) 送信者が(1, 1, 0, 1, 1, 0, 1)というビット列を送信するとき，ビット列後尾に付加されるパリティビットは何になるか答えよ．

解答

(2) (1)の受信者が，パリティビットを含む(1, 1, 0, 0, 1, 1, 0, 0)というビット列を受信したとき，このビット列が誤りであると判定されるか，理由とともに答えよ．

解答

理由

得点	
----	--

五、ネットワークセキュリティにおける基本技術について、以下の問いに答えよ。

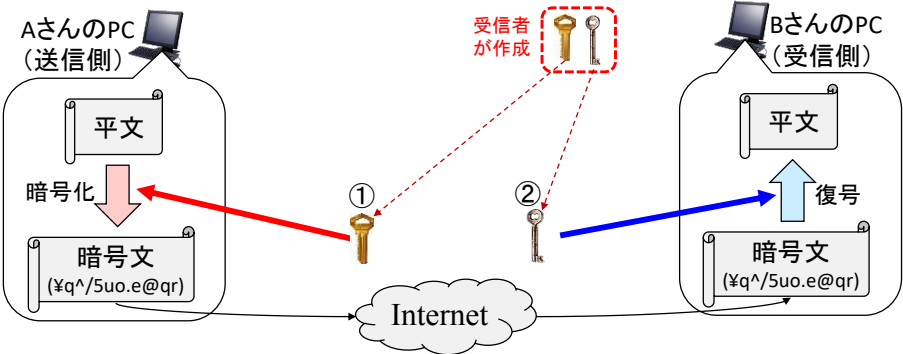
- 問 1. 暗号方式について、以下の文章のうち正しいものには○，間違っているものには×の記号を解答欄に記入せよ。
- (1) 共通鍵暗号方式は，鍵の送信が必要であるためセキュリティ上問題があり現在は全く使われていない。
  - (2) 公開鍵暗号方式の 1 つである RSA 暗号は，素数の掛け算と素因数分解の計算コストの大きな差を利用して実現されている。
  - (3) 計算時間が十分にあれば一方方向ハッシュ関数の入力データを算出することができる。
  - (4) 換字式暗号は文字の出現頻度から解読可能な場合がある。

解答欄

(1)	(2)	(3)	(4)

問 2. 問 1(2) の暗号方式の 1 つである RSA について，以下の問いに答えよ。

- (1) 送信側・受信側が使用する鍵の名称(図中の①，②)を答えよ。



解答欄

①	②
---	---

- (2) ②の鍵として 2 つの素数(229, 71)が使用されているとき，①の鍵として使用される数値を求めよ。なお，計算の途中経過も書くこと。

解答