情報理論及演習 2003 年 7 月 7 日分 略解

1. 以下について説明しなさい (10 点 ×6 問).

   (a) SMTP

   Simple Mail Transfer Protocol の略. TCP/IP の上位プロトコルで, 電子メールを送信するためのプロトコル. 電子メールソフトがメールサーバにメールを送るときや, メールサーバ間のメールのやり取りに使われる.

   (b) POP

   Post Office Protocol の略. メールサーバーから電子メールを受信するためのプロトコル.

   (c) WWW

   World Wide Web の略. URL を使用し, Internet に参加している世界中の WWW サーバのどの Web ページにもジャンプすることができるドキュメントシステム.

   (d) URL

   Uniform Resource Locator の略. インターネット上の Web ページの所在地を表記する方法. アクセス方式, ドメイン名, パス名を並べて表記する. 例えば, http://www.xxx.ac.jp など.

   (e) HTML

   Hyper Text Markup Language の略. Web ページを記述する書式のこと. 単語, 文章, 画像にリンクを持たせ, クリックすることで関連項目を表示できるのが最大の特徴.

   (f) DNS

   Domain Name System の略. DNS サーバは, ホスト名と IP アドレスの対応関係を記述したデータベースを管理しており, クライアントからの要求に応じて, ホスト名からその IP アドレスを参照できるようにする. これによりユーザーは, 憶えにくく, 分かりにくい IP アドレスではなく, ホストの名前を指定してネットワークにアクセスできるようになる.

2. 電子メールはどのように配送されるかを，テキスト pp.330 – 331 を参考にしてまとめなさい (10 点).

   クライアント (送信者) が SMTP サーバーに接続要求を行い，データを送信する．次に，SMTP サーバーは DNS を用い，データの送信経路を決定する．データは，この送信経路 (インターネット上のルーター) を通り，受信者の STMP サーバーに送信される．さらに，受信者の STMP サーバーは，データを POP サーバーに送り，一時保管する．受信者は，メールを読みたい時に，POP サーバーに接続要求し，メールを受信する.

3. インターネットにおいて，オーディオファイル，映像ファイルを伝送するための技術にストリーミングと呼ばれる技術がある．どのような技術か説明しなさい (10 点).

   サーバがネットワークを使用してデータを配信する場合に, クライアントが全データをダウンロードしてからではなく, 順次データを再生することを可能にする技術.

4. 公開鍵暗号方式とは何か (10 点)．秘密鍵暗号方式とは何か (10 点).

   ・公開鍵暗号方式

   暗号システムにおいて, 「暗号化鍵」と「復号化鍵」という 2 つのキーをペアで使い, しかもそのうちの「暗号化鍵」は公開してもかまわないという暗号系. 復号化鍵は発信者が管理して秘密にしておく.

   通信文を送信する場合は, 暗号化鍵を使って通信文を暗号化し, 受信した側では復号化鍵を使って元に戻す. ２つの鍵はある数学的な関係に基づいて決められているので, 片方の鍵が分かればもう一方を求めるのは不可能ではないが, (計算量の点から) 現実的ではない.

   公開鍵暗号システムは, 従来の秘密鍵暗号システムに比べて, (1) 暗号化鍵は秘匿する必要がないので, 暗号化鍵の配布が容易, (2) 暗号文を復号化するには, 各ユーザーが個々に持っている復号化鍵さえあればよいので, 復号化鍵を配布する必要がない, (3) デジタル署名による認証機能を持つ, という利点がある.

   ・秘密鍵暗号方式

   暗号文の送信側と受信側が, 共有する 1 つの鍵 (秘密鍵) で暗号化と解読を行なう形式. 難解な鍵を作成して強固なセキュリティを確保できる半面, 秘密鍵を知られると暗号がたちまち見破られるという欠点がある.