**CISC 250**

**Suggested Solution to Assignment 4**

1. **Compare and contrast symmetric (private key) and asymmetric (public key) encryption.**

A symmetric (or private key) encryption algorithm is one in which the key used to encrypt a message is the same as the one used to decrypt it. Both parties to the transmission must possess the same key for encryption and decryption. The key must be kept secret, leading to a need for key management.

An asymmetric (public key) algorithm is one in which the key used to decrypt a message is different from the one used to encrypt it. There are two keys. One key (called the public key) is used to encrypt the message and a second, very different private key is used to decrypt the message. The net result is that if two parties wish to communicate with one another, there is no need to exchange keys beforehand. All public keys are published in a directory. Each knows the other’s public key from the listing in the public directory and can communicate encrypted information immediately. The key management problem is reduced to the on-site protection of the private key.

1. **List and briefly describe the 4 generations of cellular (mobile) networks. For each generation, list the names of the most commonly used standards (e.g., GSM), the data rate supported, etc.**

* 1st Generation – AMPS
  + Analog standard using FDMA (Frequency Division Multiple Access)
  + Only support voice calls, does not support data transfer
* 2nd Generation – GSM, IS-95 (cdmaOne)
  + Digital system
  + GSM
    - Dominant global standard
    - GSM uses TDMA & FDMA combined
    - GSM supports voice calls and data transfer speeds up to 9.6 kbps, and SMS (Short Message Service)
  + IS-95 (cdmaOne)
    - IS-95 (Interim Standard 95) is the first CDMA based 2G digital cellular standard
    - cdmaOne is the brand name for IS-95 that was developed by Qualcomm
    - IS-95 traffic channels support voice or data at bit rates of up to 14.4 kbps
* 3rd Generation – UMTS (WCDMA), CDMA2000
  + Universal Mobile Telecommunications System (UMTS)
    - Evolution of GSM
  + WCDMA (Wideband Code Division Multiple Access)
    - 3rd Generation (3G) mobile cellular system that uses the UTRA-FDD mode
    - 3GPP (3rd Generation Partnership Project) Release 99
      * Up to 2 Mbps data rate
    - Simultaneous voice and data support
    - Interworks with existing GSM networks
  + CDMA2000
    - Evolution of IS-95 cdmaOne standards
      * Uses CDMA & TDMA
    - CDMA2000 1xEV-DO (Evolution-Data Optimized) enables 2.4 Mbps data rate
* 4th Generation LTE-A
  + LTE-A (LTE-Advanced)
    - Peak Data Rate (Release 10)
      * Downlink: 3 Gbps
      * Uplink: 1.5 Gbps
    - LTE-A incorporates higher order MIMO (4×4 and beyond) and allows multiple carriers to be bonded into a single stream

1. **List and briefly describe the 6 sub-systems of structured cabling in commercial buildings.**

Entrance Facility: provides the point at which outside cabling interfaces with the intrabuilding backbone cabling. The physical requirements of the network interface are defined in the EIA/TIA-569 Standard.

Equipment Room: the room house racks of equipments of higher complexity than TC.

The design aspects of the equipment room are specified in the EIA/TIA 569 Standard.

Backbone Cabling: cabling between TC, equipment rooms, and building entrance facilities, including vertical connection between floors (risers), cables between an equipment room and building cable entrance facilities, and cables between buildings (inter-building in case of large system. The most commonly used cabling are multi-mode fibres.

Telecommunications Closet: a closet or cabinet to house: terminations for the other end horizontal cabling; cross connect device (patch panels); patch cords (or cross connect cords); electronic hub equipments for the network of that floor.

Horizontal Cabling: cabling from the information outlet in the work area to the horizontal cross-connect (HC) in the telecommunication closet (TC). It should be deployed in star topology and the length limit is 90 m.

Work Area: from the information outlet (or telecommunication outlet) to the station equipment. Components include station equipment, patch cables (or station cable, usually ~3m, cannot be > 10 m), and adapters.

1. **List two IEEE 802.11 wireless LAN specifications (e.g., 802.11ac) that the University of Delaware is currently using or used to use, and compare them in terms of frequency range, maximum data rate, and their pros and cons.**

|  |  |  |
| --- | --- | --- |
|  | **802.11n** | **802.11ac** |
| **Frequency Range** | 2.4 GHz/5 GHz | 5 GHz only |
| **Maximum Data Rate** | Up to 600 Mbps | At least 1 Gbps |
| **Pros** | Can cover larger area;  Back compatible with all previous types of WLAN;  Total 23 non-overlapping channels (11 in 40 MHz band) for easier deployment;  Relatively cheap | Highest speed;  Less interference;  Total 23 non-overlapping channels (11 in 40 MHz band) for easier deployment |
| **Cons** | More interference in the 2.4GHz band;  Slower speed;  High power consumption | More expensive;  Client hardware needs to be upgraded (not compatible with devices only working on 2.4GHz band) |

1. **Briefly explain: (a) the media access control method used in the 802.11 wireless LAN; (b) why the media access control method used in Ethernet cannot be used in wireless LAN?**

(a) The media access control used in 802.11 wireless LAN is CSMA/CA – Carrier Sense Multiple Access/Collision Avoidance plus ACK. Whenever a node needs to transmit, it senses the channel for traffic. If it senses traffic, it has to wait until there is no traffic sensed. However, even if it does not sense any traffic, it will have to start a random back off timer (wait for some random amount of time) prior to transmission to minimize chances of collision. Since wireless LAN adaptors cannot detect collisions, ACK is used to make sure that any collision occurred in the network is taken care of. That is: the receiver immediately sends back an ACK after receiving an 802.11 frame; if the sender does not receive the ACK within certain amount of time, it has to retransmit the frame using CSMA/CA.

(b) The media access control used in Ethernet is CSMA/CD. This method allows the node to immediately transmit once it senses that the channel is free (instead of waiting a random amount of time as with Collision Avoidance), because the node can detect collisions if there are any. This is not possible in wireless networks, because the station cannot have its receiver on while it is transmitting. Hence the collision has to be *avoided,* rather than being *detected.*

1. **List and briefly describe at least two ways to provide security for wireless LAN (e.g., WPA).**

MAC Address Filtering

In this method, there is a list of MAC addresses that are allowed to associate with an Access Point (AP). Any MAC address that is not in the list is not allowed to use the AP for communication. Therefore only known devices will get access to the network. However, this method is not scalable for large networks. If any wireless NIC is changed, the list has to be changed manually.

Wired Equivalent Privacy (WEP)

WEP uses RC4 streaming cipher to encrypt the data stream between a WLAN client and an AP. WEP uses either a 40-bit or a 104-bit key, and combines the key with a 24 bit Initialization Vector (IV) to get the seed for encryption. The key is shared between the WLAN client and the AP, and is usually entered as a string of 10 or 26 hex characters where each character corresponds to 4 bits. The encryption process is shown below.

Key + IV

(seed)

RC4

Input Stream

XOR

Encrypted Stream

Because WEP uses relatively short IV and the key is static, the key can be deciphered within a few minutes if encrypted stream is available. Also there is no check for payload integrity in WEP. Users may also have few choices of easy-to-remember key disadvantages of WEP

Wireless (Wi-Fi) Protected Access (WPA)

WPA also uses RC4 streaming cipher to encrypt the data stream. However, it uses a 128-bit key with 48-bit IV. The user can input the key as an 8-63 bit ASCII string. It can be used in two modes:

* Using an authentication server (e.g. RADIUS), which generates and distributes different keys to different users in a network
* Using Pre-shared key, where each user has the same *pass-phrase.*

WPA uses Temporal Key Integrity Protocol (TKIP) to dynamically change keys to avoid attacks. It also has provision for payload integrity as a CRC. But if both data and checksum are modified similarly, an attacker can tamper data even if the key is not known. Hence WPA uses Message Integrity Code (MIC) which includes a frame counter to prevent tampering. With MIC, TKIP and the increased IV size, WPA provides more effective security than WEP in wireless networks.