**CISC 250**

**Assignment 4**

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

**Asymmetric encryption** utilizes a pair of keys- a public key and a private key. If you encrypt data with the public key, only the holder of the corresponding private key can decrypt the data, hence ensuring confidentiality. An asymmetric encryption algorithms typically involve exponential operations, they are not lightweight in terms of performance. So asymmetric algorithms are often used to secure key exchanges rather than used for bulk data encryption.

**Symmetric encryption** means that the encryption and decryption operations utilize the same key. For two communicating parties using symmetric encryption for secure communication, the key represents a shared secret between the two. Symmetric encryption is typically more efficient than asymmetric encryption, and is often used for bulk data encryption.

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(1G):**

**AMPS (advanced mobile phone system): introduced in North America in Oct. 1983, only supports calls //still didn’t find the data rate supported for this one**

**2nd Generation(2G):**

**GSM (Global System for Mobile Communications): introduced in Finland in 1991, supports voice calls and data transfer speeds up to 9.6 kbps, and short message service, uses SIM card**

**IS-95(Interim Standard 95): first CDMA based 2G digital cellular standard, and cdmaOne is the brands 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(3G):**

**UMTS (Universal Mobile Telecommunication System) UMTS Terrestrial Radio Access supports several different terrestrial air interfaces. Multiple Access in UTRA can be supported by UTRA-FDD or UTRA-TDD. WCDMA(Wideband Code Division Multiple access) is the 3G mobile cellular system that uses the UTRA-FDD mode. It has seamless mobility for voice and packet data applications. It has simultaneous voice and data support, and interworks with existing GSM networks.**

**CDMA2000: standardized by 3GPP2. CDMA2000 1Xev-DO(Evolution-Data Optimized) enables 2.4Mbps data rate.**

**4th Generation(4G):**

**LTE-A (LTE-Advanced): considered as a 4G technology based on the ITU-R IMT-Advanced process. The peak data rate can be 3Gbps downlink and 1.5Gps uplink. LTE-A incorporate higher order MIMO and allows multiple carries 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**: anything from a broom closet with communication hardware mounted in the wall to giant rooms with raised floors full racks of equipment and cable trays connecting them. It usually houses equipment of higher complexity than TC. The design aspects of the equipment room are specified in the EIA/TIA 569 standard

**Backbone Cabling**: is cabling between TC, equipment rooms and building entrance facilities. The most commonly used cablings are multi-mode fibers.

**Telecommunications Closet**: It’s a closet or cabinet to house. It’s the terminations for the other end horizontal cabling, the cross connect device, patch cords, and electronic switch equipment for the network of that floor.

**Horizontal Cabling**: from the information outlet in the work area to the horizontal cross-connect in the telecommunication closet. It is in start topology, and has a length limit of 90m.

Work Area: from the information outlet to the station equipment. It is relatively simple, and has station equipment, patch cables 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:**

frequency range: 2.4/5 GHz radio spectrum, up to 300 feet range

maximum data rate: up to 600 Mbps, but typically around 100 Mbps

pros: cheaper, the covering range is wider

cons: the speed is quite low comparing to 802.11ac

**802.11ac:**

frequency range: operates at 5GHz radio spectrum only

maximum data rate: at least 1 Gbps

pros: faster

cons: more expensive, the covering range may not be as wide as 802.11n

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?**
2. **The media access control method used in in the 802.11 wireless LAN is CSMA/CA+ACK.**
3. **The media access control method used in Ethernet is CSMA/CD. The reason why the media access control method used in Ethernet cannot be used in wireless LAN is that wireless transceivers can’t send and receive on the same channel at the same time, so they can’t detect collisions. It mainly has a carrier sense to listen to the media to see if it is free, and use the collision avoidance which is to minimize chances of collision by starting a random back off time, when medium is free and prior to transmission. Since it cannot detect the collision, it will wait a little longer before starting sending information.**
4. **List and briefly describe at least two ways to provide security for wireless LAN (e.g., WPA).**

**WPA: WPA strengthened WEP by including authentication using 802.1X framework or a passphrase, creating a key hierarchy out of the master key, doubling the size of the initialization vector used during encryption and including a more robust data integrity algorithm.**

**WPA2: uses the same authentication process, 4-way handshake and key hierarchy as WPA, the difference is that in WPA2 sessions, the TKIP is replaced with the advance encryption standard(AES) CCMP protocol.**