Q1

- **False**
  Amazon.com isn’t located in branch office, based on the configuration in SDP, datagram will be either discarded or sent in plain.
- **True**
  since datagram should be protected (destination is branch office), and the SA is between two routers (Tunnel mode), the header must change.
- **True**
  same as previous
- **False**
  IPSec seq number will always increase regardless of the content of datagram. And the packet will be resent.

Q2

The Anti-Relay window alone can’t defend against this attack. The combination of sequence number and Authentication MAC (ICV) can verify the sender of datagram so IPSec can decide to drop the datagram or not.

Q3

Transport adjacency: Refers to applying more than one security protocol to the same IP packet, without invoking tunneling. This approach to combining AH and ESP allows for only one level of combination; further nesting yields no added benefit since the processing is performed at one IPSec instance: the (ultimate) destination.

Iterated tunneling: Refers to the application of multiple layers of security protocols affected through IP tunneling. This approach allows for multiple levels of nesting, since each tunnel can originate or terminate at a different IPSec site along the path.

Q4

GSM provides:

- Subscriber authentication
- Confidentiality of communications and signaling over the wireless interface
- Protection of the subscriber’s identity from eavesdroppers on the wireless interface

GSM lacks and flaws:

- protection on the wired part of the network (neither for privacy nor for confidentiality)
- The visited network has access to all data (except the secret key of the end user)
- No authentication of base station (fake base station attacks)
- Vulnerable to SIM Card cloning

Q5

- Authentication is one-way only (AP is not authenticated to STA and STA is at risk to associate to a rogue AP)

- A static key is used, which means that every connected device on the network has access to all of the confidential message contents.

- The attacker can manipulate messages despite the ICV mechanism and encryption, because CRC is a linear with respect to XOR

- Misuse of RC4 and the small 24-bit space of IV results in easy and fast breaking of key and encryption.