**Q1:**

**Q1.1:**

The attack is composed by two phases. Trudy can impersonate Alice to Bob.

This is a reflection attack.

When Alice send (A,a), Trudy impersonate her and send it to Bob. Then Bob will repond with (B,b,HMAC(X,a)) using the secret shared key. Now Bob Wait for the respond of the challgenge. Obviously Trudy cannot compute it so it starts a new connection challenging Bob with its own challenge (A,b), Now Bob will respond with (B,n, HMAC(X,b)). Now Trudy has the respond to the first challenge and can conclude it.

**Q1.2:**

This can be solved using for example different decided keys or challenges (e.g. even challenges in a), or personal nonces, timestamps or lifetime of challenges.

**Q2:**

**Q2.1:**

**V**

**Q2.2:**

**V**

**Q2.3:**

Basically a block cipher when using operation modes

**Q3:**

**Q3.1:**

A Cryptocraphic Hash Function is an Hash function particularly strong wrt the security requirements and in addition:

1. Arbitrarly input length.
2. Fixed output Length.
3. Efficiency.

**Q3.2:**

The principal problem of hashing is collision. Collision can always be found with brute force. Birthday paradox is a statistic paradox that says that two find two people birth in the same day we just need 23 people (sqrt(365)) to achieve 50% of possibilities instead of 365/2. In cryptographic, to ensure security we need to make it “impossible” to reach 50% of possibility in a reasonable time. According to today computational power and time, we need to use output of 2^160, so an attacker has to compute 2^80 possibility in order to achieve 50% of possibility.

SHA-1 is affected.SHA-3 not (large and variable output).

**Q3.3:**

If x is <= 2^256 it will be not modified.

**Q4:**

**Q4.1:**

Iptables -A INPUT -j DROP

Iptables -A OUTPUT -j DROP

Iptables -A FORWARD -j DROP

**Q4.2:**

Iptables -A INPUT -s 152.100.0.0/16 -d 192.168.0.16/28 -j DROP

Iptables -A OUTPUT -s 152.100.0.0/16 -d 192.168.0.16/28 -j DROP

Iptables -A INPUT -s 192.168.0.16/28 -d 152.100.0.0/16 -j DROP

Iptables -A OUTPUT -s 192.168.0.16/28 -d 152.100.0.0/16 -j DROP

**Q4.3:**

This sintax says: drop all the packets leaving the network using either tcp or udp protocol if the source device connects to a port in the range 0:1023.

Normally ports in that range are paired with server, e.g.: HTTP, SMTP etc. so we don’t want that our server communicates with the external internet.

**Q5:**

Principal differences are on the level and the transparency.

IPSec gives security to IP packets in a transparent way wrt to application. Anyway, it is weak against spoofing etc. TLS is a protocol between transport and application. It is application-specific and applying it you must change some code. TLS is more used in real-world application.