1. Write a “hello world” web server in Java. Regardless of the page requested, the server should respond with an HTML page displaying just the words “Hello World”. Handle each client in a separate thread (30 pts, use back of page).

```java
// ANSWER
import java.io.*;
import java.net.*;

public class HelloServer extends Thread {
    private Socket socket;

    // Wait for clients
    public static void main(String args[]) throws Exception {
        ServerSocket ss = new ServerSocket(80);
        while (true)
            new HelloServer(ss.accept());
    }

    // Create client handler
    HelloServer(Socket s) {
        socket = s;
        start();
    }

    // Handle client in a separate thread: ignore input, then write "Hello World"
    // using a minimal HTTP/1.1 header and HTML
    public void run() {
        try {
            PrintWriter out = new PrintWriter(
                new OutputStreamWriter(socket.getOutputStream(), "latin1"));
            out.print("HTTP/1.1 200 OK\r\n"
                + "Content-Type: text/html\r\n"
                + "\r\n"
                + "<html><head></head><body>Hello World</body></html>\r\n");
            out.close();
        } catch (Exception x) {} 
    }
}
```

2. Circle True or False (2 pts each).

**ANSWERS**
- F The UDP port number provides secure authentication of the sender.
- F If the receiver detects a TCP checksum error, then it returns a packet requesting a resend.
- T ICMP is used to deliver error messages.
- T TCP uses random initial sequence numbers to make address spoofing difficult.
- F PPP is an application level protocol.

3. Short answer (3 pts each).

**ANSWERS**
- What TCP/IP packet header field is used to tell the sender to slow down? **Window size**
- What field distinguishes TCP from UDP? **Protocol**
- What field prevents infinite router loops? **TTL**
- What field is used to reassemble a TCP stream in the right order? **Sequence number**
- What field is used to identify IP fragments belonging to the same packet? **ID**
What protocol resolves host names to IP addresses? ___ DNS
What protocol resolves IP addresses to Ethernet addresses? ___ ARP
What protocol gives a computer its IP address at boot time? ___ DHCP
What type of server connects cell phones to Web servers? ___ WAP
Which two block cipher modes effectively create stream ciphers? ___ OFB, CTR

Give two examples of block ciphers. ___ AES, DES, etc.
Give two examples of hash functions. ___ SHA-1, MD5, etc.
Give two examples of digital signature functions. ___ DSA, ElGamal, RSA
What are the elements of $\mathbb{Z}_4$? ___ 0, 1, 2, 3
What are the generators of $\mathbb{Z}_5^*$? ___ 2 and 3

Consider RSA with $p = 11$, $q = 5$, $e = 3$, $d = 7$.
What is the public key? ___ $n = 55$, $e = 3$
What is the digital signature of message $m = 2$? ___ $2^7 \mod 55 = 18$

4. Suppose computers A, B, and C are connected by a switched Ethernet. C has been compromised by an attacker who wants to sniff traffic between A and B without being detected. Describe the steps in an attack to do this (9 pts).

**ANSWER:** Use ARP spoofing to launch a man-in-the-middle attack.
1. Send ARP reply to A with B’s IP address and C’s Ethernet address.
2. Send ARP reply to B with A’s IP address and C’s Ethernet address.
3. Forward packets from A addressed by IP to B (but delivered to C) to B.
4. Forward packets from B addressed by IP to A (but delivered to C) to A.