Answer All Questions

1. (20 pts)
   
   (a) Alice has selected the RSA public key \((n = 55; e = 23)\). Bob wants to encrypt
       the plaintext message 6 and send it to Alice.
       
       i. What is the corresponding ciphertext?
       ii. What is Alice's private key \(d\)?
       
       YOU MUST USE THE ALGORITHMS STUDIED IN CLASS FOR EXPONENTIATION AND FOR FINDING
       MULTIPLICATIVE INVERSES AND MUST SHOW ALL YOUR WORK.

   (b) With ECB mode of DES, if there is an error in a block of the transmitted ciphertext, only
       the corresponding plaintext block is affected. Is this also true for the
       CBC mode? If there is an error in the first cipher-text block, \(C_1\), how does this
       affect the reconstruction of plaintext blocks \(P_1, P_2\), etc.
2. (20 pts)

(a) Suppose that someone suggests the following way to confirm that the two of you are both in possession of the same key. You create a random bit string the length of the key, XOR it with the key and send the result over the channel. Your partner XORs the incoming block with the key (which should be the same as your key) and sends it back. You check, and if what you receive is your original random string, you have verified that your partner has the same secret key, yet neither of you has ever transmitted the key. Is there a flaw in this scheme?

(b) Many people believe that Digital Certificates and a Public Key Infrastructure (PKI) will solve the secure e-commerce problem to a large extent. Others however claim that this far from the truth. Give 5 of the strongest arguments that the critics of PKI provide when cautioning against the hype that currently abounds related to the advantages of PKI.
3. (20 pts)

(a) Given the security levels TOPSECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, say what type of access (read, write, or both) is allowed in the following situations. Assume discretionary access controls allow anyone access unless otherwise specified.

i. Paul, cleared for (TOPSECRET, A, C), wants to access a document classified (SECRET, B, C).

ii. Anna, cleared for (CONFIDENTIAL, C), wants to access a document classified (CONFIDENTIAL, B).

iii. Jesse, cleared for (SECRET, C), wants to access a document classified (CONFIDENTIAL, C).

iv. Sammi, cleared for (TOPSECRET, A, C), wants to access a document classified (CONFIDENTIAL, A).

v. Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, B).

(b) What is a salt value and how is it used by the UNIX password protection mechanism. Give two advantages of using a salt value?
4. (20 pts) Consider the following function:

```c
int foo(char a[]) {
    int x, y, z;
    char buf[10];

    ...

    strcpy(buf,a); //copies string stored in a to buf, without checking bounds
}
```

Suppose you know the following:

- integers are 4 bytes long
- addresses are 2 bytes long
- stack frames are organized so the stack grows down with the
  - stack pointer at the highest address (2 bytes),
  - followed by the return pointer (2 bytes),
  - followed by the parameters
  - followed by the local variables, in the order they're declared. (Note that a[] is an array parameter, so it occupies 2 bytes in the stack frame, corresponding to the address of a[0]).
- some malicious code is stored at the address, represented by the same 16 bits as the character string “cbd”.

(a) Draw a picture of the relevant parts of memory, labelling bytes with actual or relative addresses.

(b) Give a value for parameter a[] that will result in a stack-smashing attack that executes the malicious code stored at “cbd”

(c) Explain step by step what happens when you execute foo with this value of a[].
5. (20 pts)

(a) Database and/or Java Security.

(b) You can move the multi-level model question here if you wish and I can ask another OS question instead.