Algorithms in the Real World
Assignment #4 Due Date: 6 Nov 00

Problem 1: (10pt) Cipher Block Chaining (CBC) was described in class and the notes. Assume that CBC is being used with DES for transmitting a stream of blocks. If there is a one-bit error in transmitting a ciphertext block, how many bit-errors might this cause in the decrypted output (across all blocks)?

Problem 2: (10pt) Assume we have a 3×3-bit s-box used in a block cipher. For each of the following three substitutions explain what is wrong, or might be bad about this s-box.

Input	out_1	out_2	out_3
0	2	0	4
1	5	4	3
2	3	1	7
3	7	5	2
4	0	2	5
5	4	6	0
6	3	3	6
7	1	7	1

Problem 3: (20) This problem exhibits what is called a protocol failure. It shows how one can decrypt a message without figuring out the key when a cryptosystem is used carelessly. Joe Hacker decides that he wants to have two public-private key pairs to be used with RSA—he feels that two is more prestigious than one. In his infinite wisdom, he decides to use a common value for $n = pq$ and selects two separate encryption exponents e_1 and e_2, giving two distinct decryption keys d_1 and d_2. He makes e_1, e_2 and n public. You can assume that e_1 and e_2 are relatively prime.
Assume two people send the same plaintext message m to Joe one encoded with e_1 and the other with e_2. Describe how Mallory can easily determine m if he intercepts these two messages. Hint, for any positive integers a and b, the extended Euclidean algorithm finds integers r and s such that $ra + sb = \gcd(a, b)$.

Problem 4: (20) We give an example of the ELGamal Cryptosystem implemented in $\text{GF}(3^3)$ using x^3+2x^2+1 as the irreducible polynomial. We can associate the 26 letters of the alphabet with the 26 nonzero field elements, and thus encrypt ordinary text. The associations are given on the next page. Suppose Bob uses the polynomial x as the generator (g in the notes) and uses 11 as the random power (x in the notes). Show how Bob will decrypt the following string of ciphertext:

```
(K,H)(P,X)(N,K)(H,R)(T,F)(V,Y)(E,H)(F,A)(T,W)(J,D)(U,J)
```

I would advise writing a small program for this. Although it might be quicker to do by hand, it would be quite tedious. Note that part of the problem is generalizing ElGamal from Z_p (as in the notes) to $\text{GF}(3^3)$.

A	1
B	2
C	x
D	$1+x$
E	$2+x$
F	$2x$
G	$1+2x$
H	$2+2x$
I	x^2
J	$1+x^2$
K	$2+x^2$
L	$x+x^2$
M	$1+x+x^2$
N	$2+x+x^2$
O	$2x+x^2$
P	$1+2x+x^2$
Q	$2+2x+x^2$
R	$2x^2$
S	$1+2x^2$
T	$2+2x^2$
U	$x+2x^2$
V	$1+x+2x^2$
W	$2+x+2x^2$
X	$2x+2x^2$
Y	$1+2x+2x^2$
Z	$2+2x+2x^2$