Algorithms in the Real World (15-853), Fall 04
Assignment #2

Please answer all of the questions. Due Oct. 25.

Problem 1: Chaining (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: Number Theory basics (15pt)

A. For what values of n is $\phi(n)$ odd?

B. Show that if $d|m$ (i.e. d divides m), then $\phi(d)|\phi(m)$.

C. A group $(G_1, *)$ is isomorphic to a group $(G_2, +)$ if there exists a one-to-one and onto function $f : G_1 \rightarrow G_2$, such that for every $a, b \in G_1$, $f(a * b) = f(a) + f(b)$.

Show that the multiplicative group Z^*_{17} is isomorphic to the additive group Z_{16}. Note that you **don't** need to do this using brute force by filling in a 16×16 table.

Problem 3: Coin flipping over the phone (10pt)
Consider the following problem. Alice and Bob are talking on the phone and want to decide whether they should go to the opera or the fight. Unable to arrive at a decision, they decide to flip a coin. However, they do not trust each other. Help Alice and Bob determine the outcome of a fair coin flip (heads with probability 0.5), without having to meet in person. Prove that the outcome is random even if one of the two is dishonest, while the other is honest. (Hint: Use bit-commitment.)

Problem 4: Diffie-Hellman (10pt)
Extend the Diffie-Hellman scheme to enable three parties to share a single secret.

Problem 5: RSA (10pt each)
The following two questions exhibit what are called a protocol failures. They shows how one can break a cryptosystem if the cryptosystem is used carelessly.
You can solve either one of the two questions or both.

A. 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 Alice and Bob send the same secret plaintext message m to Joe one encrypted with e_1 and the other with e_2. Suppose that Eve is eavesdropping on the conversation and gets the two encrypted messages. Show how she can use these to reconstruct the original message m. Hint, for any positive integers a and b, the extended Euclid's algorithm finds integers r and s such that $ra + sb = \gcd(a, b)$.

B. This problem shows why it is unsafe to use a very small public key in RSA. Suppose Alice, Bob and Carol have the following RSA public keys—$(3, N_A)$, $(3, N_B)$, and $(3, N_C)$ respectively. Joe sends the message m to each one of them, encrypted using their respective public keys. Suppose that Eve is eavesdropping on the conversation and gets the three encrypted messages. Show how she can use these to reconstruct the original message m.

Problem 6: El-Gamal (15pt)
We give an example of the ELGamal Cryptosystem implemented in 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 below. Suppose Bob uses the polynomial x as the generator (g in the notes) and uses 11 as the random power (x in the notes, and a in the slides). 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. Also writing a program will help you understand how to implement the Galois Field operations.

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

Problem 7: Square roots (10pt)
When p and q are distinct odd primes, $n = pq$, points in Z_n^* have either zero or four square roots. A quarter of the points have four square roots; the rest have no square root. The four square roots will look like a; $n-a$, b, and $n-b$. Suppose Harry designs an efficient algorithm S that, on input of a square x, finds some square root of x. You don't know which. Use S to make an efficient (probabilistic) algorithm F that factors n. (Hint: try to find two square roots of a number, a and b, which are not of the form $a = \pm b \pmod{n}$. Show how, if you do this, you can factor n.)