ICS 268 Midterm
October 24, 2001

NAME: ***Student ID:***

PROBLEM 1

Let **E(k,M)** be a block cipher with **k** being a 56-bit key (like DES). Suppose Alice sends the ciphertext **C1=E(k1,M1)** to Bob and ciphertext **C2=E(k2,M2)** to Charlie. Eve intercepts both ciphertexts. Assume that she also knows **X=M1 ⊕ M2**.

Eve wants to discover both **k1** and **k2**. Assume that **M1** and **M2** are both sufficiently long, so that -- given **C1, C2** and **X** -- the pair of keys **(k1,k2)** is uniquely determined. If Eve tries all possible pairs of keys (all $\mathbf{2^{112}}$ of them) she can find **k1** and **k2**. (She can do this by iterating through all **k1', k2'** until **D(k1',C1) ⊕ D(k2,C2) = X** is found.)

Show that -- given **C1, C2** and **X** – Eve can find **(k1,k2)** by doing only $\mathbf{2^{57}}$ decryption operations. You may use as much memory as you need.

1) Decrypt C1 with all possible k1', create table T1.
2) Decrypt C2 with all possible k2', create table T2.
3) Compose T3 = T1 xor T2
4) Search for X in T3

(1) + (2) cost $\mathbf{2^{57}}$ decryptions

PROBLEM 2

Let **E(k1,k2,M)** be an encryption algorithm defined as follows:

- Let **p** be a 128-bit prime
- **(k1,k2)** are each in $\mathbf{Z_p}$ **and k1<>0**
- **M** is in **Zp**
- **E(k1,k2,M) = C=k1 * M + k2 (mod p)**

Show that, given two random plaintext/ciphertext pairs **(M1,C1)** and **(M2,C2)**, it is possible to easily recover **k1** and **k2** with high probability.

C1-C2=k1(M1+M2)
K1=(C1-C2) / (M1+M2)
K2=C1-K1*M1

PROBLEM 3

A set G and *operator* @ satisfy:

- for all x,y in G, x @ y is in G
- there is an *identity* element e such that, for all x, in G, e@x = x and x@e=x
- G is *finite*
- For all x,y,z in G, if x@y = x@z , then y = z
- For all x,y,z in G, (x@y)@z = x@(y@z)

Is (G,@) is a group? Prove your answer…

(G,@) is a group only if for each x in G, there exists an inverse.
Let's suppose that there exists an element x in G that doesn't have an inverse. Consider a set of elements: x@y where y is free. Clearly, this set contains exactly n distinct elements where n=|G|. Suppose it has less than n elements. Then, for some y1,y2 it holds that x@y1=x@y2 which implies that y1=y2, a contradiction. Therefore, the set must contain exactly n elements. Consequently, one of those elements must be e, the identity element. Thus, x must have an inverse. QED

PROBLEM 4

Suppose that Alice encrypts, using RSA, the same message m for three different recipients: Bob, Charlie and Diana. All of them have the same public key of e=3 but each has a unique modulus: n_1, n_2 and n_3

Eve (who knows e, n_1, n_2 and n_3) observes all three ciphertexts:

$$C_1=m^3 \bmod n_1$$
$$C_2=m^3 \bmod n_2$$
$$C_3=m^3 \bmod n_3$$

Show how Eve can compute m **without** factoring any moduli or computing any private keys.

We have the system of equations where we would like to solve for x:

$C_1 = x^3 \pmod{n1}$
$C_2 = x^3 \pmod{n2}$
$C_3 = x^3 \pmod{n3}$

A fair assumption is that n_1, n_2, and n_3 are pair-wise relative prime. So x^3 has unique solution (mod $n_1n_2n_3$) according to the CRT. Let's call the solution a. Then we have:

$$a = x^3 \pmod{n_1n_2n_3}$$

Since n_3,n_1,n_2 are believed to be fairly large, we are certain that $x < n1$, $x < n2$, and $x < n3$. But this means that $x^3 < n_1n_2n_3$. So we may proceed and solve this equation as usual, i.e. without considering the modulus. Recall that a cubic equation is easily solved in polynomial time.

PROBLEM 5

a) (5) It is often necessary to use compression to conserve bandwidth and reduce overhead in communication. If encryption and compression are used on the data, does it make more sense to encrypt the data and compress it, or to compress it first and then encrypt it? Explain.

b) (5) In his famous book, "The Road Ahead" Bill Gates writes that the security of RSA is based on "the difficulty of factoring large prime numbers". Is Bill's statement proven true? Conjectured? Not true? Explain.

c) (10) Recall one way to produce one-time signatures:

m is an n-bit message

$SK = x$

$PK = y$

$y = f^{2^n}(x)$

$Signature: m, f^{2^n - m}(x)$

Suppose n=8, so that $y = f^{256}(x)$

What is the one-time signature for m_1=00110111?

Is it safe to use the same PK twice if we want to later sign another message m_2=00110011?

a) compress, then encrypt
b) can not factor prime numbers, wrong!
c) $m, f^{201}(x)$ can not reveal m_2 since $m_1 > m_2$