Cryptography and Communication Security	**Final**
CSG 252 Fall 2006	**Due: Friday 12/08/2006**

Note on integrity: For the final, you are not allowed to discuss problems with fellow students. All written work must be entirely your own, and cannot be from any other course.

Questions

(1) We can represent the DES encryption function as a function $DES_{k_1,\ldots,k_{16}}(x)$ taking a 64-bits plaintext x and applying the 16 rounds of DES encryption, where subkey k_i is used at round i. (The DES key generation process takes a 64 bits key K and produces that sequence of 16 subkeys, $k_1, \ldots, k_{16}$.)

Prove that for any sequence of subkeys $k_1, \ldots, k_{16}$, $DES_{k_{16},\ldots,k_1}(DES_{k_1,\ldots,k_{16}}(x)) = x$; in other words, to decrypt a DES-encrypted ciphertext, it suffices to apply the DES encryption algorithm, but feeding it the round subkeys in the reverse order.

(2) Consider the following variant of the Diffie-Hellman key agreement protocol. As in the Diffie-Hellman protocol, let p be a sufficiently large prime such that it is intractable to compute discrete logarithms in $\mathbb{Z}_p^*$. Let α be an element of $\mathbb{Z}_p^*$ of order n. Both p and α are publicly known. Alice has a secret key x_A and a public key $y_A = \alpha^{x_A}$. Bob has a secret key x_B and a public key α^{x_B}. Alice and Bob establish a secret shared key by executing the following protocol:

1. Alice chooses a at random, $0 \leq a \leq p-2$, sets $c = \alpha^a$, and sends c to Bob.
2. Bob chooses b at random, $0 \leq b \leq p-2$, sets $d = \alpha^b$, and sends d to Alice.
3. Alice computes the shared key $k = d^{x_A} y_B^a = \alpha^{bx_A + ax_B}$.
4. Bob computes the shared key $k = c^{x_B} y_A^b = \alpha^{ax_B + bx_A}$.

Does this protocol provide entity authentication, that is, does the protocol ensure that when Alice completes her interaction, she is guaranteed to have been exchanging messages with Bob, and vice versa, and in particular, that they both share a key with each other, as opposed to sharing one with an adversary? (Recall that the standard Diffie-Hellman protocol does not satisfy entity authentication, because there was a man-in-the-middle attack that let an adversary fool Alice and Bob into each sharing a key with him.) Discuss the security of the protocol.

(3) Let $P = \{P_1, P_2, P_3, P_4, P_5, P_6\}$. Set up a secret sharing scheme, such that exactly the groups $\{P_1, P_2\}$, $\{Q \subseteq P \mid |Q| \geq 3, P_1 \in Q\}$ and $\{Q \subseteq P \mid |Q| \geq 4, P_2 \in Q\}$ are able to reconstruct the secret, where $|Q|$ is the number of elements in the set Q.

(You may want to refer to Stinson 13.2.)

(4) Alice and Bob have fallen in love, and Bob wishes to mail Alice a ring. Unfortunately, they live in such an awful place that whenever something is sent through the mail it is stolen unless it is enclosed in a padlocked box. Alice and Bob have plenty of padlocks, but none to which the other has a key.

How can Bob get the ring safely into Alice's hand (by using the postal system, of course)?