Introduction to Cryptography

Homework 1

Due by November 26, 2008.

1. (Shannon's theorem)
   Consider an encryption scheme where the size of the plaintext space *(P)* is equal to the size of the ciphertext space *(C)*, and is also equal to the size of the key space *(K)*. (Namely $|P|=|C|=|K|$.) Then the encryption scheme provides perfect secrecy *if and only if* the following two conditions hold:
   - Every key is chosen with equal probability ($1/|K|$).
   - For every message m in P and every possible ciphertext c in C, there exists a single key k in K, such that $E_k(m)=c$.

   Prove *one* of the two directions of the theorem (namely, either the "if" direction or the "only if" direction.).

2. Let m and n be positive integers. Partition the plaintext to segments of nm letters each. Write down each plaintext segment by rows in an n-by-m matrix. The ciphertext is created by going over the columns of the matrix. For example, if n = 3; m = 4 the plaintext "cryptography" will lead to the following matrix

   c r y p
   t o g r
   a p h y

   and the ciphertext will be "ctaropyghpry".
   a. Decipher the ciphertext (generated in the abovementioned way, not necessarily with the same m and n) "gdoooeivntnneenetmderhewcaenaetatysebins".
   b. Describe an effective method for deciphering long enough ciphertexts, encrypted by applying a monoalphabetic substitution cipher first, followed by a permutation cipher as described in the question above. Limit your answer to no more than 8 lines.

3. An Internet radio station wishes to broadcast streamed music to its paying subscribers. Non-subscribers should not be able to listen in. When a person subscribes she is given a software player with a number of secret keys embedded in it. The station encrypts the broadcast using a symmetric cryptosystem (private key) with a 128-bit key, K. The secret keys in the player of each paying customer can be used to compute K and enable legitimate subscribers to tune in. When the set of paying customers changes, the station will encrypt future broadcasts using a different key K' which corresponds to the new set of customers.
   Suppose the total number of potential subscribers is less than $n = 10^5$. Let R1,R2,...,Rn be n random independent keys, 128 bits each . The player shipped to subscriber number u contains all the keys except for Ru (i.e. each player contains 99999 keys).
   a. Suppose that the station wants to encrypt the broadcast so that all users except for user 1 can decrypt it. How can the station do that?

b. Let S be the set of currently subscribed users (S might be smaller than 99999). Show that the station can construct a key K, used to encrypt the broadcast, so that every subscriber in S can derive K (from the Ri's in her player), while any single subscriber outside of S cannot derive K. You may assume that the set S is known to everyone (e.g. it is a plain part of the broadcast) . Briefly explain why your construction satisfies the required properties.
c. Is your construction collusion resistant? That is, can two or more users who are not in S combine their knowledge of keys in order to decrypt the transmission. (Assume that each users knows the set of keys in his or her decoder, and that the users can build a new decoder. The only thing that they cannot do is guess the value of keys that they don't have.)
d. (Bonus question) Design a similar system which is secure even against two illegitimate users who try use the union of the keys in the decoders of both of them. The system should have at most n(n-1)/2 keys.