COMP364: Quiz #1
March 15^{th}, 2001
10:30-11:45am

1. Explain, in not more than 60 English words, the meanings of "authentication" and "non-repudiation" in the area of computer and communication security.

2. What major assumption(s) must be satisfied for a cipher-text only brute force attack of a secret key algorithm to be successful.

3. (a) How many different keys are there for an affine cipher with $N = 30$?

   (b) In crypt-analysing an affine cipher, we arrive at two equations

   $$4a + b = 8 \bmod 126$$
   $$10a + b = 6 \bmod 126$$

   Note that $N = 126$ in this case. Find all the possible solutions to the two equations. Show your steps.

4. (a) On the average, how many DES keys map a given plaintext to a given ciphertext?

   (b) On the average, how many plaintexts are mapped by a given DES key to a given ciphertext?

5. A symmetric block cipher, B, does its encryption as follows:

   for i = 1 **to** 16 **do**
   $RE_i = LE_{i-1} \oplus P_i$;
   $LE_i = F(RE_{i-1}) \oplus RE_{i-1}$;
   $LE_{17} = RE_{16} \oplus P_{18}$;
   $RE_{17} = LE_{16} \oplus P_{17}$;

   where RE_i and LE_i are the right and left half (each 32 bits) of the output of the i^{th} round, respectively. $F()$ is a function that takes a 32-bit input and produces a 32-bit output. $\oplus$ is the bitwise exclusive or function. Also, P_i, $1 \leq i \leq 18$, can be thought of as the i^{th} per round key (32 bits) generated from the secret key. (RE_0 and LE_0 are from the plaintext directly. RE_{17} and LE_{17} together is the ciphertext.)

   Write down the decryption function in terms of F and $P_i's$. Use RD_i and RD_i to denote the right and left half of the output of the i^{th} round of the decryptor.

   Verify that your decryption function properly inverses the encryption function.

6. Use examples to show a security weakness of each of

   (a) the Electronic Code Book (ECB), and

   (b) the Cipher Block Chaining (CBC)

   modes of operation. (One example for each mode.) Assume the block cipher being used is DES.