Assignment 2 Winter 2011

Due on March 8th in the class. Sorry - you need to do some calculations!

1. In RSA, public key of Bob is 31, where $n = 3599$. What is his private key?

2. What is $5^{600} \mod 1234$? In general how quickly (running time) you can compute $x^b \mod n$, where you can assume that x,b, and n are l-bit numbers.

3. Let $n = pq$, and p and q are distinct odd primes. Let $\lambda(n) = \frac{(p-1)(q-1)}{GCD(p-1,q-1)}$. Modify the RSA cryptosystem by requiring that $ab \equiv 1 \mod \lambda(n)$. Prove that encryption and decryption are still inverse operations. If $p = 37$, $q = 79$, and $b = 7$, compute a in this new system, as well as in the original RSA.

4. In RSA, for two plaintexts of Alice say x_1 and x_2, is it true that

$$e_K(x_1)e_K(x_2) \mod n = e_K(x_1x_2 \mod n).$$

   Bonus: Use the above property to show the following: Given a cipher text y, describe how to choose a ciphertext $y' \neq y$, such that if we know the plaintext x', such that $y' = e_K(x')$, then we can find the plaintext x, such that $y = e_K(x)$. This is called as the chosen ciphertext attack.

5. Show that for every a and n, where GCD(a, n)=1, $a^{\phi(n)} \equiv 1(\mod n)$.

6. Let $DES(x, K)$ represent the encryption of plaintext x with key K using DES. Let $y = DES(x, K)$. Let $y' = DES(c(x), c(K))$, where $c(.)$ represents the bitwise complement of its argument. Show that $y' = c(y)$. (You don't have to go too deep inside DES to answer this! - high level view should suffice).

7. Let $h_1 : \{0,1\}^{2m} \rightarrow \{0,1\}^m$ be a collision resistant hash function. Define $h_2 : \{0,1\}^{4m} \rightarrow \{0,1\}^m$ as follows:
   a) Let $x \in \{0,1\}^{4m}$ be $x = x_1||x_2$, where $x_1, x_2 \in \{0,1\}^{2m}$.
   b) Define $h_2(x) = h_1(h_1(x_1)||h_1(x_2))$.
   Prove that h_2 is collision resistant.
   Bonus: Can you generalize this to a function $h_i : \{0,1\}^{2^i m} \rightarrow \{0,1\}^m$, and show that it is collision resistant.