Mid Semester Examination: Cryptography and Network Security (Course No: CS60041)

Time: 2 hours
Marks: $10 \times 8 = 80$ marks

Attempt All Questions

1. Alice and Bob wish to resolve a dispute over telephone. We can encode the possibilities of the dispute by a binary value. For this they engage a protocol:
   (a) **Alice** $\rightarrow$ **Bob**: Alice picks up randomly an x, which is a 200 bit number and computes the function $f(x)$. Alice sends $f(x)$ to Bob.
   (b) **Bob** $\rightarrow$ **Alice**: Bob tells Alice whether x was even or odd.
   (c) **Alice** $\rightarrow$ **Bob**: Alice then sends x to Bob, so that Bob can verify whether his guess was correct.

   If Bob's guess was right, Bob wins. Otherwise Alice has the dispute solved in her own way. They decide upon the following function, $f : X \rightarrow Y$, where X is a random variable denoting a 200 bit sequence and Y is a random variable denoting a 100 bit sequence.
   The function f is defined as follows:

   $f(x) = ($ the most significant 100 bits of $x) \vee$ (the least significant 100 bits of x), $\forall x \in X$

   Here $\vee$ denotes bitwise OR.
   Answer the following questions in this regard:
   (a) Design a suitable strategy for Bob to guess the parity of x.
   (b) If Alice is honest, what is the probability of Bob to be successful in guessing whether x is even or odd correctly?
   (c) What is Alice's probability of cheating Bob?
   (d) Give a brief reasoning as to whether you would suggest Alice and Bob to use the function f.

   (2+3+3+2=10 marks)

2. Let $n = pq$ with p and q being distinct large prime numbers of roughly equal size. Suppose, we know that for any $a < n$ and $gcd(a, n) = 1$ we have $a^{p+q} = a^{n+1} \text{mod}(n)$. Prove that n can be factored in $O(n^{1/4})$ steps with a high probability.
   Note: Detailed proof is not required. A sketch of the proof would suffice.

3. Consider a cryptosystem, with P, K, C denoting the Plaintext, Key and Ciphertext respectively. Prove that for any cryptosystem, $H(K|C) \geq H(P|C)$, that is given the Ciphertext, the attacker's ambiguity of the Key is atleast as large as the uncertainty of the Plaintext.
(**Hint:** Express $H(P|C)$ in terms of $H(P, K, C)$)

4. Show that the unicity distance of the Hill Cipher over $\mathbb{Z}_{26}$ (with an $m \times m$ encryption matrix) is less than m/R_L, where R_L is the redundancy of the language.

5. Suppose S_1 is the *Shift Cipher* (with equiprobable keys) and S_2 is the *Shift Cipher* where keys are chosen with respect to some probability distribution $P_{\mathcal{K}}$ (which not be equiprobable). Prove that $S_1 \times S_2 = S_1$.

6. Let $DES(x, K)$ represent the encryption of plaintext x with key K using the DES cryptosystem. Suppose $DES(x, K)$ and $y' = DES(c(x), c(K))$, where $c(.)$ denotes the bitwise complement of its argument. Prove that $y' = c(y)$.
That is if we complement the plaintext and the key in DES, then the ciphertext also gets complemented.
Note: This can be proved by the high level description of DES, the actual structure of S-Boxes or other component functions are irrelevant to this result.

7. (a) Consider an SPN (Substitution Permutation) cipher on input x, with number of rounds being indictated by N_r. Prove that if the last round has a permutation layer then it does not increase the strength of the cipher.
   (b) Consider an invertible Substitution operating on m bits, where m is an integer. Prove that it is a permutation from $\{0,1\}^m$ to $\{0,1\}^m$.

(6+4=10 marks)

8. Suppose that X_1, X_2 and X_3 are independent discrete random variables defined on the set $\{0, 1\}$. Let ϵ_i denote the bias of X_i, for $i = 1, 2, 3$. Prove that if $X_1 \oplus X_2$ is independent of $X_2 \oplus X_3$, then either $\epsilon_1, \epsilon_3 = 0$ or $\epsilon_2 = \pm 1/2$.