Class Test: Cryptography and Network Security (Course No: CS60041)

Date: 10/9/08
Time: 1.5 hours
Marks: $3 + 5 + 10 + 5 + 15 + 2 = 40$ marks

DES (Data Encryption Standard) although an elegantly designed cipher has become old. Its $n = 56$ bit key is being challenged by the present day computation power. As an alternative, it was thought of applying DES twice, i.e in creating a product cipher $DES' = DES \times DES$. If the key space of DES was $K = \{0,1\}^n$, the key size of the product cipher is expected to be $K_1 \times K_2 = (K_1, K_2)$, where $K_1, K_2 \in K$. The plaintext of the cipher is denoted by $P = \{0,1\}^m$ and the cipher is endomorphic (the plaintext and the ciphertext are the same set).

In regard to this composed cipher answer the following questions:

1. What is the property in the DES construction which helps to increase the key length by performing such composition? (Another way of asking the question is: why is DES not idempotent?)

2. Using the DES cipher an attacker obtains l pairs of plaintexts and ciphertexts: $(p_1, c_1), \ldots, (p_l, c_l)$. The key is say (K_1, K_2) but unknown to the attacker (obviously, else why will he/she be an attacker).
   Prove that for all $1 \leq i \leq l$, $DES_{K_1}(p_i) = DES^{-1}_{K_2}(c_i)\ \forall i$, where $1 \leq i \leq l$.

3. Prove that of all the possible keys (K_1, K_2), the expected number of keys for which $DES_{K_1}(p_i) = DES^{-1}_{K_2}(c_i)\ \forall i$, where $1 \leq i \leq l$, is about 2^{2n-lm}.

4. Suppose $l \geq 2n/m$, what can you say to the attacker to help him in developing an attack against the composed cipher DES'?

5. The attacker starts building up two lists: L_1 and L_2. Each entry in the list L_1 and L_2 has l tuples of elements of P followed by an element from K. The lists are filled with all possible keys.
   The lists are now sorted in a lexicographic manner on the l tuples. The attacker now does a linear search to find out the common l tuples in the lists.
   Explain how does the attacker maintain the list and how does this approach help him to find out the correct key? Show that the amount of memory required by the attacker is $2^{n+1}(ml + n)$ bits and number of encryptions and/or decryptions required to identify the key is $l2^{n+1}$.

   (Hint: Use the distinguisher: for the correct key $DES_{K_1}(p_i) = DES^{-1}_{K_2}(c_i)\ \forall i$)

6. Into what class does the above kind of attack fall?