Midterm

March 16, 2016, 3:35–4:50 PM

There are six problems each worth five points for a total of 30 points. Show all your work, partial credit will be awarded. Space is provided on the test for your work; if you use a blue book for additional workspace, sign it and return it with the test. No notes, no collaboration.

Name: ____________________

Problem	Credit
1	
2	
3	
4	
5	
6	
Total	

1. *Merkle Trees*

   Let $h(x, y)$ be a hash function.

   Let T_k be a binary tree with k leaves. Each node n of T_k, except the leaf nodes, has a right and a left child, $r(n)$ and $l(n)$. Leaf nodes have no children. Each node n has a value $v(n)$. The root of T_k is R.

   Assign k values $x_1, \ldots, x_k$ to the k leaf nodes $n_1, \ldots, n_k$ as $v(n_i) \leftarrow x_i$.

   For each internal node n assign to that node the hash value calculated with the left and right child values as input:

   $$v(n) \leftarrow h(v(l(n)), v(r(n))).$$

   This scheme is collision resistant if only with negligible probability can an adversary A find distinct sequences of values $\langle x_1, \ldots, x_k \rangle$ and $\langle x'_1, \ldots, x'_k \rangle$ that when assigned to the leaves of T_k result in a collision of the value at the root, $v(R) = v(R')$.

   Show that this scheme is collision resistant if and only if h is a collision resistant hash function.

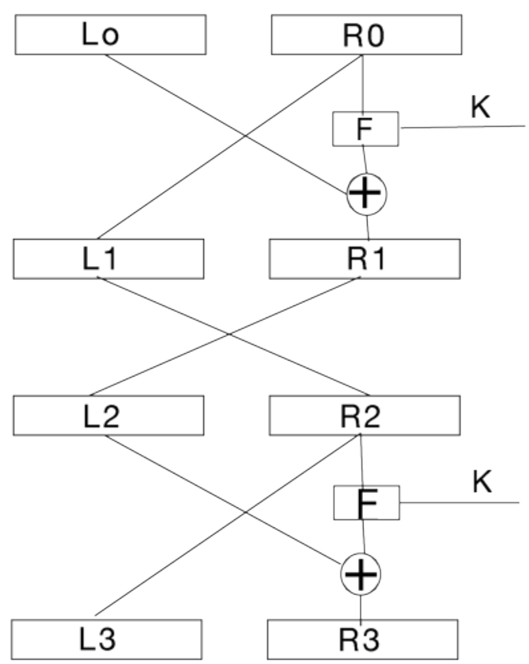
2. *Feistal Networks*

   A useful property of a Feistal network is that the same network encrypts and decrypts just by reversing the order that the subkeys are applied. (A technical details is that between the encryption output and the decryption input the left and right halves of the ciphertext have to be swapped.)

   This can be shown by working stage by stage. The illustration below is the last Feistal stage of the encryption, followed by the swap, followed by the first Feistal stage of the decryption.

   Show that this diagram reduces to a swap:

$$\begin{aligned} R_3 &= L_0 \\ L_3 &= R_0 \end{aligned}$$



3. *Malleability*

   Let the plaintext be the sequence of bytes $m_1, \ldots, m_n$. Let the check sum of the bytes be the byte result of exclusive or of all the bytes $\sigma = \oplus_i m_i$. Given a key k, G_k is a pseudorandom number generator that generates a sequence of bytes $G_k(i)$ for $i = 1, 2, \ldots$.

   The encryption of the message with check sum is,

   $$E_k(m_1, \ldots, m_n) = c_1, \ldots, c_{n+1}$$

   where $c_i = m_i \oplus G_k(i)$ for $i = 1, \ldots, n$ and $c_{n+1} = \sigma \oplus G_k(n+1)$.

   Given the encryption of $m_1, \ldots, m_n$ show how to get the encryption of $m_1, \ldots, m'_j, \ldots, m_n$, where m'_j is the complement of m_j.

   Note: In answering this problem you are cracking the WEP protocol that was standard WiFi encryption scheme from 1997 to 2003.

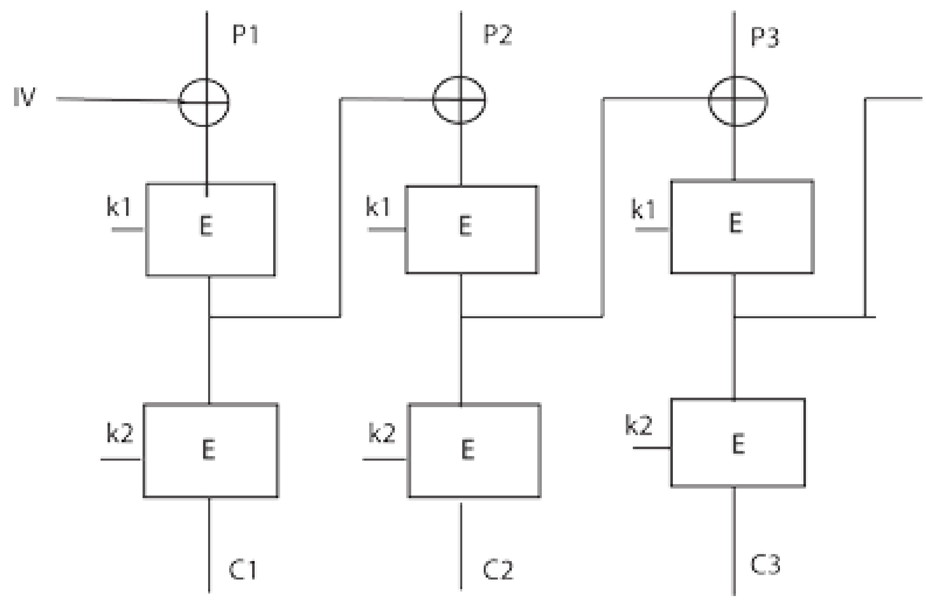
4. *Multiple Modes of Operation*

   In order to double key length, Prof R is considering cascading two k-bit encryptions. He believes this will mean that the brute force attack requires $O(2^{2k})$ trial keys given a known plaintext-ciphertext pair.

   He decides to use CBC in the first stage of encryption, followed by ECB in the second stage. In the diagram, E is a k bit block cipher, with k bit keys. Keys k_1, and k_2 are chosen independently.

   I think Prof R has made a blunder.

   Show a chosen-plaintext attack to reduce the time for a brute force attack to $O(2^k)$, profiting from the structure of CBC over ECB.



5. *Perfect Secrecy*

   Consider an encryption that encrypts the message $m \in \{0, 1\}$ by exclusive or with a key chosen independently at random $k \in \{0, 1\}$ with the probability $Pr(k = 0) = 2/3$ and $Pr(k = 1) = 1/3$.

   The input has known distribution $Pr(m = 0) = 3/4$ and $Pr(m = 1) = 1/4$.

   (a) What is the probability that the ciphertext is 0.

   (b) What is the probability that the ciphertext is 1.

   (c) What is the probability that the message is 0 given that the ciphertext is 0.

   (d) What is the probability that the message is 1 given that the ciphertext is 1.

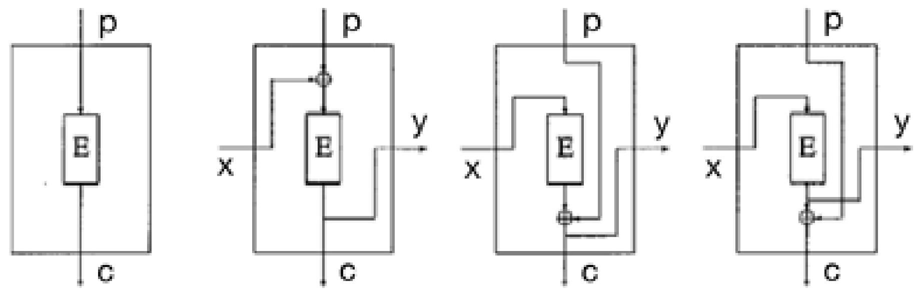
   (e) How should the eavesdropper guess the message from the ciphertext?

   (f) And what is the eavesdropper's probability of successfully guessing the message?

   (g) Is this a secretly perfect encryption.

6. *Modes of Operation*

   Recall the modes of operation:



   Label the modes correctly as CBC, OFB, ECB and CFB and for each mode give decryption formulas in terms of p, c, x and y.

   Example: ECB decryption is $p = E^{-1}(c)$.