Cryptography I, homework sheet 11

Due: 07 January 2011, 10:45

If you have too much time over Christmas: everybody is interested in results (attacks and implementations) on the remaining SHA-3 candidates and some offer prices.

The first exercise speaks of a Feistel cipher. The definitions in the text are sufficient to solve the exercise but it helps to think of L as the left part of the ciphertext and of R as the right part. Per round a function is applied to the right half and the result added to the left half; then the positions swap. So the bits in R get overwritten only in the second round. This is a typical feature of a Feistel cipher. Usually many more than 2 rounds are used. An important example of a Feistel cipher is DES ... which is still around even though AES is the official standard.

The following exercises are courtesy of DJB so that I could enjoy Indocrypt. Thanks!

1. In a 2-round Feistel cipher, the key is used to create secret functions f and g. The plaintext is a pair (L, R). The ciphertext is (T, U), where $T = L + f(R)$ and $U = R + g(T)$.

   (a) Exhibit a fast chosen-plaintext attack that determines $f(A)$ given A.

   (b) Exhibit a fast chosen-plaintext attack that determines $g(B)$ given B.

   (c) Exhibit a fast chosen-plaintext attack that determines a plaintext (L, R) given a ciphertext (T, U).

2. Majordomo is a program that manages Internet mailing lists. If you send a message to `majordomo@foodplus.com` saying `subscribe recipes`, Majordomo will add you to the `recipes` mailing list, and you will receive several interesting recipes by e-mail every day.

   It is easy to forge mail. You can subscribe a victim, let's say `God@heaven.af.mil`, to the `recipes` mailing list, and thousands more mailing lists, by sending fake subscription requests to Majordomo. `God@heaven.af.mil` will then be flooded with mail.

   Majordomo 1.94, released in October 1996, attempts to protect subscribers as follows. After it receives your subscription request, it sends you a confirmation number. To complete your subscription, you must send a second request containing the confirmation number.

   Majordomo 1.94 generates confirmation numbers as follows. There is a function h that changes strings to numbers. The `recipes` mailing list has a secret string k. The confirmation number for an address a is $h(ka)$. For example, if the secret string is `ossifrage`, and the address is `God@heaven.af.mil`, the confirmation number is $h($`ossifrageGod@heaven.af.mil`$)$.

   The function h produces a 32-bit result, computed as follows. Start with 0. Add the first byte of the string. Rotate left 4 bits. Add the next byte of the string. Rotate left 4 bits. Continue adding and rotating until the end of the string.

   Explain how to subscribe `God@heaven.af.mil` to the `recipes` mailing list despite this protection, and explain what Majordomo 1.94 should have done.