Massachusetts Institute of Technology
6.857: Network and Computer Security
Professor Ron Rivest

Handout 4
February 27, 2012
Due: March 9, 2012

Problem Set 2

This problem set is due on *Friday, March 9* by **11:59 PM**, and should be turned in through email to *6857-staff*. Please note that no late submissions will be accepted.

You are to work on this problem set with your assigned group of three or four people. You should have received an email with your group assignment for this problem set. (Note that your group will be *different* than your group for pset 1.) If not, please email `6.857-tas@mit.edu`. Be sure that all group members can explain the solutions. See Handout 1 (*Course Information*) for our policy on collaboration.

Homework must be submitted electronically! Each problem answer must appear on a separate page. Mark the top of each page with your group member names, the course number (6.857), the problem set number and question, and the date. We have provided templates for LaTeX and Microsoft Word on the course website (see the *Resources* page).

Grading: All problems are worth 10 points.

With the authors' permission, we will distribute our favorite solution to each problem as the "official" solution—this is your chance to become famous! If you do not wish for your homework to be used as an official solution, or if you wish that it only be used anonymously, please note this in your profile on the homework submission website.

Problem 2-1. Reciprocal Block Ciphers

A symmetric-key encryption scheme is a *reciprocal cipher* if encryption and decryption are the same operation—that is if $E(K, x) = D(K, x)$ for any key K and any message or ciphertext x. Mathematically, encryption is an *involution*— it is its own self-inverse, so that:

$$x = E(K, E(K, x))$$

for all keys K and all inputs x. Some famous ciphers are reciprocal, such as the one-time pad and the Enigma cipher used by the Germans in World War II.

A *reciprocal block cipher* is just that: a block cipher that is also a reciprocal cipher, with the plaintext input block and the ciphertext output block having the same length. (The key length may be different.)

You have just been hired as a new research staff by TerraCrypt Software to begin investigations on reciprocal block ciphers, as the CTO thinks this is likely to become a hot research area yielding sales advantages for TerraCrypt. You begin your research with the following questions, and report your findings.

(a) Give a careful definition of an *ideal reciprocal block cipher* (IRBC), analogous to the definition of an ideal block cipher.

The idea of course, is that a proposed construction for an RBC should be considered a good one if an adversary can't effectively distinguish between an IRBC and the construction, given black box access to both.

(b) The CTO suggests the following construction; argue that the following is *not* a good construction (it can be distinguished from an IRBC):

$$E(K, x) = (\mathrm{AES}(K, \mathrm{right}(x)), \mathrm{AES}^{-1}(K, \mathrm{left}(x))$$

where E is the proposed construction, K is a 128-bit key, x is a 256-bit input value, AES() denotes AES encryption, $\mathrm{AES}^{-1}()$ denotes AES decryption, $\mathrm{left}(x)$ denotes the left (first) half of x, $\mathrm{right}(x)$ denotes the right (second) half of x, and $E(K, x)$ denotes the encryption (or equivalently, decryption) of x using the key K.

(c) Since RBC's have only one operation, they seem simpler to work with than the usual encryption methods, which have to define two operations (encryption and decryption) and keep track of which one is appropriate to use at each point.

Suggest some reasons (if you can think of any) to tell your CTO why RBC's might not be as good as the usual approach to symmetric-key cryptography. (If you can't think of any, just say so.)

(d) Try to come up with a plausible construction for a good RBC. Argue that your proposal is indeed self-inverse. You may use AES as a primitive operation if you like. The goal would be to come up with a proposal such that your design is effectively indistinguishable from an IRBC if AES is indistinguishable from an IBC. However, your CTO isn't interested at this time in proofs of this property, so you don't need to provide one. (If you have any informal hand-waving on this point, he would appreciate seeing that, though.) Efficiency is not a top priority for your design, although extreme inefficiency should be avoided. (Hint for one possible approach: DES.)

(e) If you try to define a mode of operation yielding a reciprocal encryption scheme taking variable-length inputs that is IND-CCA secure (modified appropriately for reciprocal ciphers) you immediately run into a problem—what is it?

Problem 2-2. Variable-input-length ciphers

In class we saw a proposal by Desai for a variable-input length block cipher (the "UFE" proposal) based on a block cipher (from CRYPTO 2000).

A very similar proposal was published by Bellare and Rogaway at about the same time, titled "On the Construction of Variable-Input-Length Ciphers" (from FSE 1999).

Both of these papers are posted on the class web site (handouts 5 and 6).

(The papers don't reference each other, although the authors (Bellare and Desai) are from the same institution and have clearly worked closely together. Here we are interested in the technical content of these papers, however, and not their history.)

(a) Compare and contrast the constructions given in these two papers. What is similar, and what is different?

(b) Compare and contrast the security results proved about these two methods. Are they proving the same security properties, or different ones?

(c) If you needed a variable-input-length cipher for an application, and had to choose one of these two constructions, which would you use? Why? (This is a technical question; we're not asking about the possible patent status of these methods, or their implementations in available software packages, if any.)

Problem 2-3. The web page `http://www.sans.org/top25-software-errors/#cat3` lists the "TOP 25 Most Dangerous Software Errors".

Of the 25 vulnerabilities given, identify those that either directly relate to cryptography, or that can be mitigated at least in part by the use of cryptography. Explain your reasoning.