CS 127/CSCI E-127: Introduction to Cryptography

Problem Set 7

Assigned: Oct. 25, 2013 Due: Nov. 1, 2013 (5:00 PM)

Justify all of your answers. See the syllabus for collaboration and lateness policies. Submit solutions by email to kevin@seas (and please put the string "CS127PS7" somewhere in your subject line).

Problem 1. (Modes of Operation) Recall that block ciphers (like AES or DES) are used for encryption via various *modes of operation*. Suppose we know that the block cipher F_k used in each of these constructions is actually a pseudorandom permutation. Which of the following modes of operations are secure under chosen-plaintext attack? Justify your answers (e.g. by giving a security reduction or by exhibiting an adversary).

a) In Output Feedback (OFB) Mode the initial value IV (denoted z_0 in the lecture notes) is transmitted in the clear, but chosen at random. Could IV instead by chosen deterministically (e.g., set to 0^ℓ)?

b) Consider a stateful variant of OFB Mode, again in which the initial value is deterministically set to $\text{IV} = 0^\ell$. However, after encrypting each message $m = m_1 \dots m_t$ as $c = c_1 \dots c_t$, where $c_i = m_i \oplus z_i$, $z_{i+1} = F_k(z_i)$, and $z_0 = \text{IV}$, we remember the last output value z_t. We encrypt the next message using $\text{IV} = z_t$.

c) Consider a Cipher Block Chaining (CBC) variant in which a random initial value $c_0 = \text{IV}$ is chosen (and sent in the clear) but instead of computing each ciphertext block as $c_{i+1} = F_k(c_i \oplus m_{i+1})$, the encryption rule is $c_{i+1} = c_i \oplus F_k(m_{i+1})$.

Problem 2. (Attacks on AES) In this problem, you will show that AES with a very small number of rounds or linear S-boxes is insecure. The high-level structure of AES as described in class should suffice for this problem; in particular, the solution does not require an understanding of arithmetic over finite fields. You may find it helpful to read the attacks on round-reduced substitution-permutation networks in KL2e §6.2.1.

a) Show that 1-round AES is not (a concrete-security version of) a family of pseudorandom permutations.

b) Show that 2-round AES is not a family of pseudorandom permutations. (Hint: show how to construct two inputs for which the outputs disagree at most one column.)

c) Show that AES (with an arbitrary number of rounds) using linear S-boxes is not a family of pseudorandom permutations. An S-box is linear if $S(x \oplus y) = S(x) \oplus S(y)$ for every x, y. Note that the column substitutions (denoted C in lecture) are already linear.

d) Extra credit: Show that 3-round AES is not a family of pseudorandom permutations. (Hint: A distinguishing advantage of $\approx 1/2^8$ should be considered "nonnegligible".)

Problem 3. (Factoring vs. Block Ciphers)

a) The General Number Field Sieve algorithm is (asymptotically) the fastest algorithm known for integer factorization. Heuristically, factoring an integer N with it takes time proportional to:

$$L(N) = \exp\left(c \cdot (\ln N)^{\frac{1}{3}} \cdot (\ln \ln N)^{\frac{2}{3}}\right),$$

where $c \sim 1.526$.

In 1999, a 512-bit integer was factored using 292 PCs averaging 400 MHz, each investing an average CPU time of 45 days. In 2009, a 768-bit RSA number was factored. According to their report[1], the amount of computation would have taken at least fifteen hundred years on a single core 2.2 GHz processer.

Assuming you control 500 cores running at 3GHz, estimate how long it would take to factor a 1024-bit integer. How about a 2048-bit integer?

b) For some block ciphers such as AES, there are no known cryptanalytic attacks that do much better than a brute-force search of the key space. Using the table of AES encryption speeds below, about how long would it take 500 parallel processors to break a 128-bit key? What about 192 and 256-bit keys?

c) What other criteria would you take into account when deciding how long to make your composite numbers or block-cipher keys for cryptography? With your answers to parts a) and b) in mind, and assuming computing power continues to grow exponentially, in what years do you think 1024-bit RSA and 128-bit AES should be phased out?

d) The following table shows estimates of encryption speeds with various security parameters[2]:

	encryption speed (kbps)
aes-128 cbc	95838.21
aes-192 cbc	76750.85
aes-256 cbc	60353.19
rsa 512 bits	589
rsa 1024 bits	374.5
rsa 2048 bits	53.9
rsa 4096 bits	29.9

Suppose HBO wants to secretly deliver the entire next season of Game of Thrones to you for review (let's assume it's 10GB worth of data). What encryption scheme and key size would you recommend that they use? Discuss the pros and cons.

[1] http://eprint.iacr.org/2010/006.pdf

[2] If you are using linux/mac, you can do this test on your own machine by typing `$openssl speed aes rsa`.