Problem Set 3

Due on Tuesday, February 23, 2010.


**Problem 1: Simplified DES**
Textbook, problem 4-1.

**Problem 2: DES Complementation Property**
Textbook, problem 4-4.

**Problem 3: Triple DES**
Textbook, problem 4-6.

**Problem 4: Modified Feistel Network**
Textbook, problem 4-8.

**Problem 5: Extended CFB Mode**
Textbook, problem 4-9. (Note: “CFB mode” as used in this problem is what we called “Extended CFB mode” in the lectures.)

**Problem 6: Fast exponentiation algorithm**

A recursive algorithm for modular exponentiation was presented in class (Lecture 8, slide 17).

```c
/* computes m^e mod n recursively */
int modexp( int m, int e, int n) {
    int r;
    if ( e == 0 ) return 1;  /* m^0 = 1 */
    r = modexp(m*m % n, e/2, n);  /* r = (m^2)^(e/2) mod n */
    if ( (e&1) == 1 ) r = r*m % n;  /* handle case of odd e */
    return r;
}
```
Here is a different recursive algorithm to do the same thing.

```c
/* alternate method to compute m^e mod n recursively */
int modexp2( int m, int e, int n) {
    int r;
    if ( e == 0 ) return 1;
    if ( e&1 ) return m*modexp2(m, e-1, n) % n;
    r = modexp2(m, e/2, n);
    return r*r % n;
}
```

Both algorithms operate by computing $m^k \pmod n$ for various integers $k$.

(a) Explain why `modexp2` is correct.

(b) For each algorithm, list the powers of $m$ that are multiplied together during the course of the algorithm when computing $m^{23} \pmod n$. For example, if an algorithm computes $m^5$ by computing $m^2 = m \ast m$, $m^3 = m^2 \ast m$, $m^5 = m^3 \ast m^2$, you would list the exponent pairs $(1, 1), (2, 1), (3, 2)$.

(c) Some of the multiplications performed by these algorithms are redundant. Which ones in part (b) are redundant?

(d) Rewrite `modexp2` to make exactly the same useful multiplications but avoid making the redundant ones.