Understanding Cryptography Homework No. 4 Due Date:

1. Prove that every positive integer is uniquely expressible in the form:
$$2^{j_0} + 2^{j_1} + \cdots + 2^{j_m}$$
Where $m \geq 0$ and $0 \leq j_0 < j_1 < \cdots < j_m$.

2. If a and $b > 2$ are any positive integers, prove that $2^a + 1$ is not divisible by $2^b - 1$.

3. Prove that any prime of the form $3k + 1$ is of the form $6k + 1$.

4. If p is a prime, prove that $(p-1)! + 1 = 0 \mod p$.

5. Prove the following according to the Euler Function:
   a) If p is a prime and a is a positive integer, then $\varphi(p^a) = p^{a-1}(p-1)$.
   b) If $gcd(m,n) = d$, then $\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$.
   c) If $a|b$, then $\varphi(a)|\varphi(b)$.

6. Find the greatest common divisor of your student number and that of your best friend using the Euclidian algorithm.

7. Assume a fast public-key library such as OpenSSL that can decrypt data at a rate of 100 Kbit/sec using the RSA algorithm on a modern PC. On the same machine, AES can decrypt at a rate of 17 Mbit/sec. Assume we want to decrypt a movie stored on a DVD. The movie requires 1 GByte of storage. How long does decryption take with either algorithm?
As said in Ch. 6, symmetric ciphers have a much better computational performance than asymmetric ones. So why do we use asymmetric cryptography?