Comprehensive Exam: Cryptology
Fall 2014

1. Give the list of application of the Chinese Remainder Theorem.

2. Give a proof of the Euler theorem.

3. Compute Euler Totient of:

a) 4
b) 7
c) 10
d) 20
e) 25
f) 30
g) 50
h) 75

4.
i) What is **the name** of the weakest theorem (Fermat, Euler or RSA) that can compute:

a) $4^{2014} \bmod 10$
b) $3^{2011} \bmod 11$
c) $3^{2011} \bmod 10$
d) $4^{2011} \bmod 10$
e) $3^{2014} \bmod 11$
f) $3^{2014} \bmod 10$

ii) What is **the result** of:

a) $4^{2014} \bmod 10$
b) $3^{2011} \bmod 11$
c) $3^{2011} \bmod 10$
d) $4^{2011} \bmod 10$
e) $3^{2014} \bmod 11$
f) $3^{2014} \bmod 10$

5. Using RSA n=143 (p=11 q=13), and assuming X = 5, and Y =7, let M=5.

a) Show each step of encrypting M when e is the first valid number greater or equal with X. (What is e?).

b) Show each step for the fast decryption for the ciphertext 10 with the same keys as above.

6. There are six possible ElGamal digital signature schemes inferable from the equation ***"ux+vk=w mod p-1".***

a) give one signature generation step (that obtains <a,b> for message H(M))
.

b) give one signature verification step (for signature <a,b>)
.