INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR
Department of Mathematics
**Mid-Semester Examination, September, 2012**
MA61027 / MA51115 : Cryptography and Network Security
Duration: 2 Hours
Total Marks 30

**Instructions: Answer all questions (1-7).**

1. (a) Describe the Rijndael S-box.

   (b) How are block ciphers different than stream cipher? [3+2]

2. Describe ECB and CBC mode of operations. What are the advantages and disadvantages of ECB mode over CBC mode? [3]

3. (a) Describe RSA cryptosystem.

   (b) Prove that decryption in the RSA Public-key Cipher actually recovers $m$. In other words, prove that computing $c^d$ yields $m$ as the least positive residue modulo $N$.

   (c) If a plaintext is encrypted twice with the RSA system using two public RSA keys $(n, e)$ and $(n, f)$ and if $\gcd(e, f)=1$, then the plaintext $m$ can be recovered from the two ciphertexts $c_e = m^e \bmod n$ and $c_f = m^f \bmod n$. How? [3+2+2]

4. Compute the Jacobi symbol $\left(\frac{25}{408}\right)$. [2]

5. Given the superincreasing sequence $X = (2, 3, 6, 12, 24, 48, 96, 200)$. Encrypt the plaintext 10010110 using easy Knapsack cipher. Explain why it is not secure. To make it strong, choose $m = 453$ and $k = 61$, then generate the sequence $kX \bmod 453$. What is the public key in this strong knapsack? Use this public key encrypt the plaintext 10010110. Use the private key $(453, 61)$ to decrypt the message. [5]

6. Describe Diffie-Hellman Key exchange technique. [3]

7. Here is a variation of the El Gamal Signature scheme. The key is constructed in a similar manner as before: Alice chooses a generator $\alpha$ of $Z_p{}^\star$ and a random integer $a$, $0 \leq a \leq p-2$, such that $gcd(a, p-1) = 1$, and computes $\alpha^a \bmod p$. Alice's public key is $(p, \alpha, \alpha^a \bmod p)$ and her private key is $a$. Let $m \in Z_p{}^\star$ be a message to be signed. Alice computes the signature $(\gamma, \delta)$ on message $m$, where

$$\gamma = \alpha^k \mod p$$

and

$$\delta = (m - k\gamma)a^{-1} \mod (p-1)$$

The only difference from the original El Gamal Signature Scheme is the computation of $\delta$. Answer the following questions concerning this modified scheme:

a). Describe how a signature $(\gamma, \delta)$ on a message $m$ would be verified using Alice's public key.

b). Describe computational advantage of the modified scheme over the original scheme. [5]

———END———