Syllabus for CS111 Quiz 2

- Number theory :
  - Primes, composite numbers, factorization. Examples:
    - Give a factorization of 223.
    - Explain how to obtain the factorization of ab from factorizations of a and b.
  - Common divisors and multiples, relation to factorization. Example:
    - Prove or disprove: there are positive integers a, b such that $ab + 2a + b + 2$ is prime.
  - Greatest common divisor, computing $\gcd(a, b)$ using Euclid's algorithm. Examples:
    - State Euclid's algorithm.
    - Use Euclid's algorithm to compute $\gcd(723, 990)$.
  - $\gcd(a, b)$ as a linear combination of a, b. Using Euclid's algorithm to compute α and β satisfying $\alpha a + \beta b = \gcd(a, b)$.
  - Modular arithmetic: computing sum, difference, multiplication, or powers modulo a number. Example:
    - Compute 7^{547549} rem 11 using exponentiation by squaring.
  - Inverses modulo a prime. Using linear combinations to compute inverses.
  - Fermat's little theorem. Using the theorem to compute powers and inverses. Examples:
    - Give a complete statement of Fermat's theorem.
    - Compute 7^{547549} rem 11 using Fermat's theorem.
  - Fermat's primality test.
  - Solving linear congruences. Example:
    - Find x such that $7x \equiv 5 \pmod{19}$.
- The RSA :
  - Explain the principle of public-key cryptosystems.
  - Explain the RSA (initialization, encryption, decryption); should be able to present the algorithms as well.
  - Explain how to "break" the RSA.
  - Providing correct values of RSA, verifying correctness of given values. Examples:

    * Suppose that Bob chooses $p = 5$, $q = 11$. Show some correct values of e (public exponent) and d (secret exponent). Give three correct pairs.
    * Bob uses $P = (143, 19)$ as his public key and $S = 21$ as his secret key. Is Bob's system correct?
    * Suppose Bob chooses $p = 7$, $q = 13$, $e = 11$. Determine d. If Alice wants to send $M = 10$ to Bob, what is the ciphertext?
- Examples:
    * If Bob by mistake publishes its secret key S_B as its public key, and if Alice sends Bob a message encrypting it with S_B, can Bob decrypt this message?
    * Bob can use two pairs of public and secret keys, say P_1, S_1 and P_2, S_2. To encrypt a message to Bob, Alice first encrypts it with P_1 and then with P_2. How can Bob decrypt the received ciphertext? Justify correctness of this scheme.