Cryptography

Lab 4 – 13 V

Problem 1 (10 points) Implement Rabin encryption and decryption for $n = pq$, where $p = q = 1 \bmod 4$. Prepare your implementation for multi-core processors *i.e.,* CRT and computing square roots should be performed concurrently for p and q.

Problem 2 (10 points) (1) Implement RSA for $n = p_1 \cdots p_k$. Implement both standard decryption and decryption with CRT. Compare efficiency (at least for $k = 2, 3, 4$) between different values of k (for the same modulus size) between the standard version and one using CRT. Prepare your implementation for multi-core processors *i.e.,* CRT for p_i and p_j should be executed concurrently (up to the number of native threads supported by a system).

(2) Compare efficiency of RSA against AES (pick key sizes to make comparison meaningful). Here, you need to treat RSA as a block cipher which then is used with *e.g.,* CBC mode. Try to encrypt 1, 10, 1000, 1 000 000 messages.