Cryptography and Cryptanalysis – E1427

Fall 2024

Project Outline

0. Introduction:

   The purpose of this project is to implement RSA Public Key Algorithm on an 8051 Microcontroller. The project include both encryption and decryption. The 8051 board should be connected to a laptop using any serial interface. The interface program from PC side is a Hyperterminal or similar application. Prime candidates for P and Q are input from PC to the 8051 for primality check and subsequent steps. 8051 program should apply Fermat Primality test at security level of 5. Public and private keys are then calculated by 8051, while the plain text is also input by Hyperterminal. Ciphertext is then calculated and the output is sent back to Hyperterminal.

1- General Guidelines:

   a. Each project group contains 5 students working on one 8051 board and a laptop
   b. For the sake of simplicity, restrict the length of p, q to 4 bytes.
   c. Use short encryption code as short as possible.
   d. Use Extended Euclidean Algorithm to get private key from public key.
   e. Plain text and ciphertext are transferred from//to laptop as an ASCII code.
   f. Project is due on Thu, Jany. 16’th. Project discussion date will be communicated later.

2- Deliverables:

   a. Complete 8051 c-code.
   b. Working circuit including interface to laptop.
   c. Report on program structure, modules, and testing steps and results.