Cryptographic and Security Implementations
Mid-Semester Assignment 2021
Total Marks: 50

Instructor: Dr. Sabyasachi Karati

Indian Statistical Institute Kolkata, India

Q1. Let A and B be two multi-precision numbers represented with n digits in base r. Write an algorithm `compare`(A,B) which outputs as given below:

$$\texttt{compare}(A, B) = \begin{cases} 1, \text{ if } A < B \\ 0, \text{ if } A = B \\ -1, \text{ if } A > B \end{cases}$$

[Marks. 10]

Q2. Toom's multiplication can be adapted to work for unbalanced operands which is when the sizes of the operands vary considerably. Let A and B be two multi-precision numbers represented in base r as given below:

$$A = a_2 r^2 + a_1 r + a_0, \text{ and}$$
$$B = b_1 r + b_0.$$

Describe how you can compute the product AB in this case using a Toom-like algorithm. [Marks. 10]

Q3. Let A and B be two integers of 127 bits. Write a C-program which contains the following functions:

(a) `convertC2I`(`char` $* A$): converts a multi-precision integer in base 2^8 to a multi-precision integer in base 2^{26}.
(b) `add`(`int` $* C$, `int` $* A$, `int` $* B$): computes $C = A + B$. The output C must be in base $r = 2^{26}$.
(c) `mult`(`int` $* C$, `int` $* A$, `int` $* B$): computes $C = A \times B$. Compute the multiplication using Karatsuba method. The output C must be in base $r = 2^{26}$.
(d) `convertI2C`(`int` $* A$): converts a multi-precision integer in base 2^{26} to a multi-precision integer in base 2^8.

In the `main()` function of the C-program,

(a) generate A and B randomly as a string of characters.
(b) Convert A and B in base 2^{26} using the function `convertC2I`.
(c) Call function `add` to compute the addition.
(d) Call function `mult` to compute the multiplication.
(e) Convert the outputs of `add` and `mult` into a base 2^8 multi-precision integer using the function `convertI2C`.
(f) Print the final outputs.

[Marks. 5+8+12+5=30]