Introduction to Cryptography, 2024 Spring

Homework 4: On-site Test

Time: 5:30pm-9:30pm, 4/19/2024 (Friday)

Problem:

The problem is to use the RSA encryption function as the key stream generator to generate a binary key stream as follows:

(i) Let $\mathrm{pk} = (\mathrm{n}, \mathrm{e})$

(ii) Set seed $\mathrm{X}_0,\ where\ 1 \leq \mathrm{X}_0 < n$

(iii) Compute $\mathrm{X}_{i+1} = \mathrm{E}(\mathrm{pk}, \mathrm{X}_\mathrm{i}) = \mathrm{X}_\mathrm{i}^{e} \bmod n$, for i ≥ 0

(iv) The j-th bit B_j of the key stream is last-bit(X_j), j ≥ 1

You program read in a line:

L n e $\mathbf{X_0}$

such as,

64 9D001E6473DFACF9 10001 F569AB

where

(i) L is the modulus length in Dec

(ii) n is the modulus in Hex

(iii) e is the exponent in Hex

(iv) X_0 is the seed in Hex

Your program outputs the key stream $B_1 \mathrm{B}_2 \ldots \mathrm{B}_{32}$ of 32 bits long in Binary, such as,

11110110011011000101000011011111