Cibersecurity: Applied Cryptography 2024-25

Secret sharing exercises

December 5, 2024 to be done in the classroom: December 6, 2024

All secrets are ASCII strings encoded as a big integer (one byte per character). For example, "AB" represents the number $65 \times 256 + 66$.

First exercise

A secret shared by four entities and requiring all entities to reveal it was generated using the xor technique. The four parts of the secret are stored in the files `ex1_s1.txt` to `ex1_s4.txt`. Recover the secret.

Second exercise

A secret shared by four entities and requiring all entities to reveal it was generated using the modular addition technique. The four parts of the secret are stored in the files `ex2_s1.txt` to `ex2_s4.txt`. The modulus is a large power of two. Recover the secret.

Third exercise

A secret shared by four entities and requiring all entities to reveal it was generated using the modular multiplication technique. The four parts of the secret are stored in the files `ex3_s1.txt` to `ex3_s4.txt`. The modulus is a large power of two. Recover the secret.

Fourth exercise

A secret shared by five entities and requiring at least three of them to reveal it was generated using the Shamir technique. The five parts of the secret are stored in the files `ex4_s1.txt` to `ex4_s5.txt`. In each file is stored x, $p(x)$ and the modulus. Recover the secret using only three of the files.

Fifth exercise

Write your own code to generate the secret shares for Shamir's technique.