Anish Banerjee, Shankh Gupta
COL759: Cryptography

Problem Set - 1
August 2023

Problem 1: CPA with Very Weak Ciphertext Integrity

Solution:

Problem 2 : Encryption Scheme with Threshold Decryption

Solution:

Problem 3 : One-time secure MACs, and Upgrading One-Time MACs to Many-Time MACs

Solution:

Problem 4 : CCA Security v/s Authenticated Encryption

Solution:

Problem 5: Modular Arithmetic and Basic Group Theory

Solution:

(a) Since a and p are coprime, by the Extended Euclid's Agorithm:

$$ab + py = \gcd(a, p) = 1$$

Taking modulo p on both sides:

$$ab \mod p = 1$$

Where $b \in \mathbb{Z}_p$ (If not then by the division algorithm $b = qp + b', b' < p$. So, we can replace b with b')

Now suppose there exist $b, b' \in \mathbb{Z}_p$ such that

$$ab = 1 \mod p \qquad\qquad ab' = 1 \mod p$$

Then by definition of mod, $p|a(b - b')$. So $b - b' = 0$ since a and $b - b'$ will be coprime to p. Hence b is unique.

(b) Consider $h(y) = y^2 + y$ and $n = 6$. For 3 values of y viz. $2, 3, 5$, we have $h(y) = 0 \mod 6$. Thus

$$|\{y \in \mathbb{Z}_6 : y^2 + y = 0 \mod 6\}| = 3 > 2$$

(c) Let $a \in \mathbb{Z}_p$ and $r = \mathsf{ord}(a)$. Then $a^r = 1 \mod p$. By Fermat's Little Theorem:

$$a^{p-1} = 1 \mod p$$

Suppose by the division algorithm, $p - 1 = rq + s$, $s < r$. Since $a^{p-1} = 1 \mod p$ and $a^r = 1 \mod p$,

$$a^{p-1-rq} = 1 \mod p$$

and hence $a^s = 1 \mod p$. But since $s < r$, it must be 0.