

Practice problems

Do the assigned reading!

Problem 1. Check that 2 is generator of group \mathbb{Z}_{11}^* . Find the discrete log of 7 to base 2 in group \mathbb{Z}_{11}^* .

Problem 2. Consider a "toy" example of the RSA encryption (public) key: ($N = 53 \cdot 59, e = 7$). Find the decryption key.

Problem 3. Explain why adding two numbers a and b modulo n takes linear time (in $|n|$), if $a, b \in \mathbb{Z}_n$.

Problem 4. The Orange Jackets win with probability 0.8 when it is raining and with probability 0.6 when it is dry. It rains 30% of the time. What is the probability that it is raining, given a win of the Orange Jackets?

Problem 5. Show how to efficiently find the RSA secret key d if you know N , which is a product of two primes, e the public exponent and $\phi(N) = |\mathbb{Z}_n^*|$.

Problem 6. Let p and q be primes and $N=pq$. What is the probability that a randomly chosen positive integer less than N is not divisible by either p or q ? How is it relevant for RSA encryption?