AAD Problem Set - 5

November 2025

Randomized Algorithms

Problem 1

How does one generate safe prime pairs, that is, primes p and q such that $p = 2q + 1$? One way is to choose a random number q and test that it is prime (e.g., using Miller–Rabin). If it is prime, proceed to test that $p := 2q + 1$ is prime as well (again, using Miller–Rabin). This works, but it invokes the primality testing algorithm twice. We'd like to show that safe prime pairs can be generated at the cost of a single primality test.

Prove that if q is a prime, then $p := 2q + 1$ is a prime if and only if

$$2^{p-1} \equiv 1 \pmod{p}.$$

Use this to devise a faster way of generating safe prime pairs using a single primality test.

Problem 2

Suppose you use the Fermat primality test by choosing a random integer $a \in \{2, \ldots, n-2\}$ and checking whether

$$a^{n-1} \equiv 1 \pmod{n}.$$

a. Prove that if n is prime, this test always passes (use Fermat's Little Theorem).

b. Show that if $\gcd(a, n) > 1$, then $\gcd(a, n)$ gives a nontrivial factor of n.

c. Define what a *Carmichael number* is, and prove that every Carmichael number passes the Fermat test for all a coprime to n.

d. Give an example (e.g. 561) and discuss why Carmichael numbers limit the reliability of the Fermat test.

Negligibility and One Way Functions

Problem 3

Give a simple example of a function f such that:

- Given y, it is easy to find $x \in f^{-1}(y)$ if such an x exists.
- Given $f(x)$, it is hard to find x: for any algorithm A, it holds that

$$\Pr[A(1^n, f(U_n)) = U_n] = \mathrm{negl}(n).$$

Is your function a one-way function?

Problem 4

Define negligible functions.

Is the following equivalent to the definition of a negligible function? Explain why it is different, or prove it is the same.

$$f \text{ is negligible if } f(x) = \frac{1}{g(x)}$$

where

$$g(x) = c \cdot e^{\mathrm{poly}(x)}, \quad c \in \mathbb{R}^+.$$

Problem 5

Are the following functions negligible?

a. $f(x) = \dfrac{1}{x!}$

b. $f(x) = \dfrac{x^2}{x}$

c. $f(x) = \dfrac{1}{(\log x)!}$

d. $f(x) = \dfrac{1}{(\log \log x)!}$

e. $f(x) = 2^{-n^{1000}}$

Problem 6

Prove that if one-way functions exist, then there exists a one-way function f such that $|f(x)| = |x|$ for all x, i.e., the length of the output of f is always equal to the length of its input, where $|x|$ denotes the length (number of bits) of the string x.

Problem 7

Prove that if one-way functions exist, then there exists a one-way function f and a constant n_0 such that $f(x)$ can be computed in $|x|^2$ time for all x of length at least n_0.

Problem 8

Show that there is no one-way function where every bit of the output depends on only two bits of the input. [*Hint*: Use the fact that $2SAT$ is in P.]

Problem 9

Let a *puzzle generator* be a polynomial-time algorithm that maps a random string r to a pair (φ_r, x_r), where φ_r is a 3SAT instance and x_r is a satisfying assignment for φ_r, such that for all polynomial-time algorithms A,

$$\Pr_r \left[A \text{ finds a satisfying assignment for } \varphi_r \right]$$

is negligible (less than any inverse polynomial in n).

Show that puzzle generators exist if and only if one-way functions exist.

Rivest–Shamir–Adleman(RSA) public-key cryptosystem

Problem 10

State and prove Fermat's Little Theorem.

Problem 11

Let $N = pq$ be a product of two distinct primes p and q. Suppose you are given N and the inverse of 3 modulo $\varphi(N)$. That is, you are given N and $d \equiv 3^{-1} \pmod{\varphi(N)}$, but you are not told what $\varphi(N)$ is.

Using this information, show a fast way to find the prime factors of N.

Problem 12

Given a product of two primes, $N = pq$, show that if an eavesdropper can efficiently determine $(p-1)(q-1)$ (the order of the multiplicative group mod N), then she can also efficiently determine p and q themselves.

Problem 13

Let N_1, N_2, and N_3 be distinct RSA moduli, such that

$$\gcd(3, \varphi(N_1)) = \gcd(3, \varphi(N_2)) = \gcd(3, \varphi(N_3)) = 1.$$

Let $e = 3$. Show that, given three vanilla RSA ciphertexts of a number $m < \min(N_1, N_2, N_3)$ under public keys (N_1, e), (N_2, e), and (N_3, e) respectively, one can quickly find the underlying message m. You must accomplish this without factoring any of N_1, N_2, or N_3.

Problem 14

Recall that, having chosen primes p and q such that $p-1$ and $q-1$ are not divisible by 3, a key step in RSA is to find an integer k such that $3k \equiv 1 mod (p-1)(q-1)$. Give a simple procedure to find such a k given p and q.

Problem 15

A multiplicatively homomorphic encryption scheme is one where, given ciphertexts of two messages M_1 and M_2 (under the same public key), one can easily find a ciphertext that encrypts their product, namely $M_1 \cdot M_2$.

Show that the vanilla RSA scheme is multiplicatively homomorphic.

Distributed Algorithms

Problem 16

Theorem: In a synchronous distributed system consisting of n processes, of which at most f may be Byzantine faulty, the achievability of deterministic Byzantine Agreement (BA) depends on the communication model as follows:

1. **Without signatures (unauthenticated messages):** BA is achievable if and only if $n > 3f$.

2. **With signatures (authenticated messages):** BA is achievable if and only if $n > f$.

Prove the above theorem.

Problem 17

State the authenticated byzantine agreement protocol and show how byzantine protocol can be reduced to broadcast problem.

Quantum Algorithms

Problem 18

Show that CNOT clones the states $|0\rangle$ and $|1\rangle$. Explain why cloning two specific known states does not violate the no-cloning theorem. Also describe the largest set of states that can be cloned simultaneously.

Problem 19

A student claims: "*To copy a qubit, just measure it bro and re-prepare it.*"

To prove that measurement cannot be used to clone quantum states, show that measuring an arbitrary state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

does not reveal α and β. Compare with classical copying, where measurement always reveals the state.

Problem 20

BB84 uses the states

$$|0\rangle, \quad |1\rangle, \quad |+\rangle, \quad |-\rangle.$$

(a) Assume cloning is possible. Describe how an eavesdropper could break BB84.

(b) Explain why the security of BB84 relies on the impossibility of cloning non-orthogonal states.

(c) Show that cloning both $|0\rangle$ and $|+\rangle$ leads to a contradiction.

Problem 21

Explain the BB84 protocol for Quantum Key Distribution. How do Alice and Bob figure out if an eavesdropper is trying to listen to the channel or not?

Problem 22

State and prove Shor's Algorithm (proof-sketch) and discuss its implications on public key cryptography.