VE475 Midterm Big RC

Written by yc

VE203 Recap

Personal recommended reading: Chap6 and Chap15 of an old book called `Discrete Math-Elementary and Beyond`. I've read the whole book and find it might help.

Personal recommended practice material (Unfortunately only Chinese version available): `XiaoCongShu Number Theory`

Part A review

Reference: Lecture Slides

The questions in the slides and simple questions in homework!!! Super important for part A, theses might be the only points I can get in the exam.

My style is to list some keywords or questions, if you are not familiar or cannot answer some of these questions, go back to slides and review relevant contents. If I am allowed to bring cheating paper, I will bring answers to these questions.

CH1

Important concept

Five attacks: cipher-text only, KPA, CPA, CCA, CPCA

What is `Kerckchoff`'s principle?

Frequency analysis => hill cipher (block cipher)

Useful in proof: Bezout's identity

essence of EEA => calculate coefficient of Bezout

Public key (PKC) => solve $\mathcal{O}(n^2)$ problem

level of secure = 2^{128}

double-encryption => MITM (what is the time and space complexity)

Five complexity classes: P, NP, NP-complete, co-NP, co-NP complete

graph isomorphism && Hamilton circuit = simple circuit that pass thru every node exactly once

Problem you might meet:

How to calculate the inverse of a mod b? => Use EEA

Calculate the inverse of matrix => $M^{-1} = adj(M)/det(M)$

The graph on p118 appears in VE477 exam [doge]

CH2

Important concept:

ECB, CBC (decrypt parallel, encrypt cannot), CTR (parallel)

BBS generator:

Useful in the WHOLE semester! Fermat Little ($a^{p-1} \equiv 1 \mod p$)

=> Proposition on how to find square root mod p

=> QR(quadratic residuosity) as hard as factorization

How to attack Feistel network? IMPORTANT(key is to cancel out two F(something))

two rounds CPA => same right, different left and XOR the LHS of the result

two rounds KPA => birthday attack

three rounds CPCA => mentioned in lecture (non-trivial construction)

What is detail process of AES? for detail explanation, check lecture or wiki or AES paper

Decryption of AES (review homework)

Problem you might meet:

How to apply Chinese Remainder Theorem? p18 find x such that $x^2 \equiv 71 \mod 77$

Given a polynomial, decide whether it is irreducible over a finite field

How is S-box constructed?

Calculate round key for AES

CH3

Important concept:

Group, Ring, Field

Why $0 \neq 1$ in field?

What is order and generator?

Lagrange's theorem

Euler's theorem (Little Fermat Theory is a special case)

How to find generator?

Finding order is as difficult as factorization

What is RSA?

Modular exponentiation algo

How to generate prime? => Generate random integers until one of them is prime

What is the density of prime?

p52 A list of factorization Algo. (detail of Pollard's Rho, can be modified for DLP)

3072 is secure for RSA.

What is the difference between CCH and CDH? (open problem)

`Diffie-Hellman` for key exchange and `Elgamal`

Problem you might meet:

How to calculate Euler's totient function $\varphi(n)$?

How to calculate $2^{639613} \mod 5353$? Do not trust the method mentioned in slides p21 (first factorize 5353 => apply Euler => apply CRT)

Calculation of Legendre symbol (used for prime), Jacobi symbol (only -1 side can be trusted => `Solovay-Strassen` Algo), Millar-Rabin Algo.

CH4

Important concept:

Three resistant for hash function and their relation

What is `Merkle-Damgard` construction?

Part B Review

(I guess it will focus on proof and construction)

Try to understand proofs in slides, review homework questions carefully.

Some exercise for you to `practice`:

It is TOTALLY OK if you cannot solve these problems, JUST for practice and fun!

Ex1.(EASY, practice module calculation) Is there exists natural numbers a, b, c, such that a^2bc+2, ab^2c+2, abc^2+2 are all perfect squares?

Ex2.(MEDIUM, practice Euler) Find out all positive number a, such that for any integer $n \geq 5$, we have $(2^n-n^2)|(a^n-n^a)$.

Ex3.(HARD, practice construction) k is a given odd number and $k > 3$, prove that there exists infinite positive odd number n, such that there exists two positive integer d_1 and d_2 that satisfy $d_1 | \frac{n^2+1}{2}$, $d_2 | \frac{n^2+1}{2}$, and $d_1 + d_2 = n + k$.

EX4.(HARD, practice prime) Find out all positive $m, n \geq 2$, such that (1)$m + 1 \equiv 3 \mod 4$ is a prime, and (2) there exists prime p and natural number a such that $\frac{m^{2^n-1}-1}{m-1} = m^n + p^a$

Q&A Time