VE475 Final Big RC

Written by yc

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.

Ch5

This is the focus, maybe it is easier to have a question of 50 marks on this topic

What is five attacks on signature

How does RSA & Elgamal(two attacks and misuse same k) & DSA signature work? (Do not forget to use Euler & CRT learnt before midterm to make life easier)

difference between DSA & Elgamal

blind signature = signature + verification + disavowal

How does RSA & Chaum-Vam Antwerpen works?

Ch6

Important concept:

Problem you might meet:

How to force all children cooperate?

How to force some of them cooperate? (t, w)-threshold m children out of w

Blakley=>polynomial=>key is of degree n => n+1 points to decide

Shamir=>plane intersect(special case of Blakley)

Ch7

key generation/distribution + encryption/decryption + tracing

m-resilient = find at least one out of m

Chor-Fiat-Naor=>take advantage of binary representation

hamming distance & distance

representation problem as hard as DLP

Boneh-Franklin (how to handle key revocation)

Ch8

Best should be Pollard-rho only

How to draw and compute graphically on elliptic curves?

$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ or $y^2 = x^3 + bx + c$

How to compute numerically on elliptic curves? (see slides)

Hasse's Theory

ECDLP key size? 256 compared to 3072 for DLP

Tripartite key exchange => pairing=>bilinear

Ch9

inner product & outer product

probability = c_i^2

review matrix calculation($H\ F_a\ D$) quantum search $\mathcal{O}(n^{1/3})$ negate + flip over mean

reference: https://www.youtube.com/watch?v=951pds5_5YM

quantum bit commitment

Ch10

Give some example of side attack. => Werewolf kill, use side attack to decide who is wolf.

Montgomery's ladder to avoid power difference => GMP Library

reverse engineering => run gdb and type `objdump -t` to obtain symbol table and type `objdump -d` to get the assembly code => pls refer to the BombLab and AttackLab of CMU online course 15213.

Part B Review

(I guess it will focus on proof and construction)

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

If you are interested in problem 2 in Part B of Mid, this link might help

http://hyperelliptic.org/tanja/teaching/CCI11/online-ff.pdf

No need to panic. Read the problem carefully, take advantage of hints. Subproblems have strong link and will gradually lead you to success.

Marks in simple questions are easy to get.

Q&A Time