

Applied Cryptography exam expectations. May 17, 6:30pm, usual room. Office hours during finals week: Monday 4:30 - 5:30, Tuesday 12:20 - 1:20, Wednesday 12:20 - 1:20.

DO bring a calculator - you will need one. Bring blank sheets. The exam heavily emphasizes the newer material.

You do **NOT** need to know anything about the Vigen'ere cipher or the cryptanalysis of a monalphabetic substitution cipher (that was to get you started on your project).

Old material

Be able to do a running time analysis, like in your homework. I would remind you how long it takes to add, subtract, multiply and divide. Know what O - notation means.

Understand quantum cryptography with or without eavesdropping. You need not memorize which polarization corresponds to which bit.

Be able to use the RC4 pseudo random bit generator if I give you the algorithm.

For MD5, you should be able to do problems like your homework - the only thing you need to memorize is what the notation means.

Be able to answer homework-like questions on timestamping. You need not memorize exactly which strings of documents that get hashed and/or signed.

Be familiar with how KERBEROS works. You need not memorize all the things sent back and forth. But you should have a general idea about what they are and why they are sent.

New material

If I give you a public key ring for PGP, and a diagram, you should be able to say who will trust the authenticity of which keys.

For key management, there is nothing to memorize. Know how salting works.

Be able to do a homework-like problem using the Lagrange Interpolating Polynomial Scheme for secret sharing. I am aware that you have limited ability to do linear algebra modulo a large prime.

Understand how Pollard's ρ -algorithm helps factor, solve the FFDLP and solve the ECDLP if I give you the appropriate random map.

Know how a meet-in-the-middle attack works.

Know how digital cash works.

Know how Scantegrity II works and why it was designed as it was.