

Applied Cryptography exam expectations. May 8, 2008. Bannan 241

Do not bring a calculator (you won't need one). Bring blank sheets. You are welcome to stay the entire 105 minutes. Most of you will not need that much time for the exam.

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).

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 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.

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.

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