The second midterm will cover all the material since the first exam; that period begins with Friedman's Incidence of Coincidence attack, continues on through our elementary properties of the Integers and Primes, and finishes with RSA, DES, and the public key exchange.

You can expect a similar format; some *very* short answer questions (true/false, multiple choice, etc.), some short answer questions, and perhaps a longer question which will require a bit more detail. Calculators are ok to check your work, but I'll want to see the individual steps when using—for example—the Euclidean Algorithm. A page of notes will be allowed.

Here's a rough guide of topics to study:

Friedman's Attack You should know the expected number of pairs when comparing various kinds of text. You should be familiar with the process that we used to attack a cipher in the computer lab: first comparing a text with (shifted versions of) itself to determine the keylength; then slicing the text into cipheralphabets according to that length; and finally, comparing shifted versions of those alphabets to determine the key itself.

Integers Basically, you should know those parts of chapter 7 that we covered; this means pretty much all of chapter 7, except that you don't have to know the nitty-gritty details of all of the proofs, or of propositions that we didn't mention in class. You should be familiar with divisibility, the Euclidean Algorithm, unique factorization, finding multiplicative inverses mod n, etc. You should also know what equivalence relations are.

This is as good a place as any to mention the specific properties needed to implement RSA and ensure it's security: how to find large primes (using our simple test, anyway); roughly how many prime numbers there are between 1 and a given number N; which tasks are easy in modular arithmetic and which are hard (as far as multiplying, exponentiation, root-finding, factoring, etc.).

You should also know Euler's Theorem, and the baby version that we called Fermat's Little Theorem. Fast Modular Exponentiation will show up, too.

RSA Be able to explain how the RSA system works, and why it's secure (using the tools above). "Knowing how it works" includes knowing what an antisymmetric cipher is and how it's even possible.

Key Exchange You should know the Diffie-Hellman Key Exchange process that we discussed in class.

DES You should have a good feel for the general overview of how DES works. I will not ask you to write down the specific permutations or S-Boxes, but you ought to know what an S-Box *does*. You should also know the basic terms here (such as *Feistal Network* or *Cipher*).

Practice Problems On the quizzes on Paul Garrett's crypto page, the following problems could be useful to look at. (I can help you print these out in the lab, and can post answers Thursday night if desired.) Quiz 5: Problems 1–3. Quiz 6: Problem 1 (2–4 are good problems and are worth doing, but they're probably harder than anything I'd put on the exam). Quiz 7: Problems 1–3. Quiz 8: Problem 3.