The first midterm will cover all of the material we've done during the first two weeks. Much of it is contained in your textbook, but most of it is. (Sometimes it's in a different form, such as those topics I covered in class using slightly less advanced terminology.) Roughly speaking, the major points are:

Basic Definitions : You should be familiar with the terms we've been using, such as: key, plaintext, ciphertext, cipheralphabet, substitution cipher, transposition cipher, monoalphabetic, polyalphabetic, etc. Also be familiar with the three types of attack: ciphertext only, ciphertext with known plaintext, and ciphertext with chosen plaintext.

Monoalphabetic Ciphers Know the examples that we've covered: shift, affine, and shuffle (or "simple substitution") ciphers. You should know how to encode/decode them and how to attack them, how much text is needed for an attack, etc.

Polyalphabetic Ciphers You should know why these provide more security than monoalphabetic ciphers. You should be familiar with the Vigenere cipher, how to use it, and how it might be broken. (Not including Friedman's attack.)

Transposition Ciphers Know the examples we discussed, such as the Box Cipher (or "Block Interleaver"). Note that the textbook doesn't cover the important variation of a Box Cipher with a Keyword. How do you recognize when a transposition cipher has been used instead of a substitution cipher?

Functions and Set Notation While I may not ask questions specifically about these topics, other questions will be related or will use this notation. You should be comfortable with our function notation and injective/surjective. Also be familiar with with Garrett's function notation for Encoding and Decoding.

Permutations Be familiar with permutations, cycle notation, and how to multiply permutations together.

Counting and Probability Know how to count. The types of problems we've worked on are a good general guide for the level of difficulty you should be comfortable with. Also know the basic definitions for probability, including conditional probability, independent events, and expected values.

Other topics...? This list should be fairly complete, but isn't intended to be exhaustive. Unless I've specifically told you something isn't on the test, you shouldn't assume so. (For example, modular arithmetic and multiplicative inverses aren't specifically listed above, but they'll be included because they are used in the definitions of some of our ciphers.)

You can have your Viginere table and half of an 8.5x11 sheet of paper with *handwritten* notes on one side. Calculators are allowed.

1. Describe how to break an affine cipher using a chosen-plaintext attack.

2. For some affine cipher, $E_{(a,b)}(\text{`}d') = \text{`}L'$ and $E_{(a,b)}(\text{`}g') = \text{`}U'$. Find the key (a, b) or explain why it is not possible. If it *is* possible, explain why the process you used might break down in certain cases, and describe what else you could do to break the cipher.

3. The following three ciphertexts are all encrypted versions of the *same* plaintext. I've also given you the frequencies of the most common letters in each ciphertext. Determine what type of cipher was used in each case, and explain your reasoning.

```
    WDQEUZDZRIVGDYAEDUIWXDURCPLASGDRALQCUDHAPDSILLWVMDQYDI
ZZCVZWAVZADIDSIUCDORWSRDSCPZIWVLYDFPCUCVZUDUAQCDHCIZEPCUDAHDWV
ZCPCUZDWRIXDANUCPJCXDUAQCDVCOUFIFCPDSAQQCVZDIZDZRCDZWQCDNEZDWD
OIUCTSCCXWVMLYDFPCASSEFWCXDNYDZRIZDLWZZLCDIHHIWPDAHDZRCDJIZWSI
VDSIQCAUIVXDWVDQYDIVTWCZYDZADANLWMCDZRCDFAFCDWDLAUZDZAESRDOWZR
DUCJCPILWVZCPCUZWVMDCVMLWURDSIUCUDZRWUDIPZWSLCDYAEDUIYDSAVZIWV
                    UDILLZRCDFENLWSDHISZU
```

(D: 15%, C: 10%, Z: 9%, slowly decreasing to 1% and less)

```
    IAOXWYFAPJXVLLCJPJSBXUIECQLPENDMUSUNCKRBFOSRDECIWWKXZB
VWISZPWWDZLNNRQJWSQCYZFYCFTWENTSGIZCQFSCJJRLIHUWDDAUWUIXFVNISY
FRFTIKRBBVTWMASFTYIIFZWVOKZRKHFRHXLUSLKLEOVCEYFAPNJEUZSORLLSCU
MXQDXDGHHNTNTHJADRCRSLHBYYPYWYTICWDQOABUOKMSTPYIRHZUJECYVBVLGF
TGKJWPAFOCTQAGTHOWYMXJGWCEZVHXLWUTSOJYWSJJFBXHZMQVXEZVCLRKIVHW
PJWOYMQIGMTFTHWYOUOIOYSYWHXQUTMZIWRGITBDVYOJTNJJAHNHQPRVIIJXGM
                    SACOPYNLHYEMXVQOVRUMMTYJLD
```

(W: 6%, Y: 5%, C: 4%, everything else between 2-4%)

```
    NCSPPEINSYSINHOITTZNNMALTYFOEATHZHZEESTYTZLZCSCIZZEHME
OGNEATSASOOTZTIGHEAEINLATEZCEESZSECEZEAUSCKOSEAMBNAIOIZTUAAXRT
WZHTUBWFHESUFRNIBZRESMHZLIEAUYZZLLZTOSETCZNLYSREYZDRVTZIEDPCBZ
MLZAPEIOTIRIZZZSEZLLZPOCFIEEETZEMFTEZZZZPEATZZORGULVSAHAOYUSIH
CWACTERPYTRENZDRIZTZOSILZICENYEIZOOSIZISAIEEZTZRCGTWAZDMECNOTH
PCEVBSINFZOMCAAOZZITMTOZSZTHDZNSZUTNHAIZZGZNZNNATDTZITLZTATAFK
                    ZALHOSLXECRAHZROMLZZE
```

(Z: 15%, E: 10%, T: 9%, slowly decreasing to 1% and less)

If you want a challenge, you could try to find the plaintext; don't attack the last one, though.