Midterm Topics

4440 and 5440 students cover the same material, but 5440 students may find slightly more emphasis on their midterm on definitions, proofs and logical deductions instead of algorithms and computations.

With the exception of the application to Radar, everything we've done follows the textbook. We have covered:

1. Chapter 1: all
2. Chapter 2: 2.1, 2.2, 2.3, 2.4, 2.7, 2.8, 2.9, 2.10, 2.12
3. Chapter 3: 3.1, 3.2, 3.3, 3.4, 3.5, 3.6
4. Chapter 4: 4.1, 4.2, 4.4, 4.5 but only an overview
5. Chapter 5: 5.1, 5.2 but only an overview
6. Chapter 6: 6.1

Ciphers

For each of these, you should be able to encipher or decipher a short message by hand, if given a key. For all of these, you should be able to describe the size of the keyspace in terms of factorials, exponents, etc. (not the full decimal expansions!).

1. Caesar cipher (key = shift)
2. Scytale (key = size of tube to wrap it around; perhaps somewhat impractical on a midterm)
3. Substitution cipher (key = arbitrary permutation of the alphabet)
4. Vigenere cipher (key = word)
5. Affine cipher (key = α and β)

6. Hill cipher (key = $n \times n$ matrix)
7. One-time pad (key = sequence of elements of $\mathbb{Z}/26\mathbb{Z}$ if using alphabet, or $\mathbb{Z}/2\mathbb{Z}$ if using bit strings)
8. Enigma (key = a full set of rotors and reflectors... this is unlikely on your exam but know the way it works)
9. RSA (use of public key and private key)
10. Three-pass protocol (both parties have their own secret key)

Number Theory Topics

For each of these, you should know the appropriate definitions, and be able to do standard computations by hand efficiently.

1. Modular arithmetic
2. Divisibility
3. GCD (gcd and magic box algorithms)
4. Solving $ax + by = d$ (when is it solvable? how do you solve it? how do you get one solution or all solutions?)
5. Finding an inverse modulo n (when is it possible? how to do it?)
6. Efficient arithmetic modulo n (reducing frequently; successive squaring)
7. Chinese Remainder Theorem (the statement, and the ability to find the solution that it guarantees)
8. Fermat's Theorem (statement and its use to compute exponents)
9. Know the proof of Fermat's Theorem! It's a great proof and I may ask you to prove it on an exam.
10. Euler's Theorem (statement and its use to compute exponents)
11. I could ask you to give small novel proofs using the basic definitions (similar to the problem on your first homework using the definition of divisibility).

Cryptanalysis

1. The method of frequency analysis as used against a Caesar cipher or substitution cipher
2. Cryptanalysis of the vigenere cipher (the key mathematical observations and how they are used)
3. Cryptanalysis of affine and hill, as done on your homework.
4. Basic outline of cryptanalysis of Enigma (the main important fact about permutations and its usage)
5. RSA: Be able to factor n if you know $\phi(n)$, and be able to compute $\phi(n)$ if you know the factorisation of n.
6. RSA: Be able to use the previous bullet to decipher a message you don't have the private key for, if you know $\phi(n)$ or the factorisation of n.

Computer Science topics

1. Pseudorandom number generators (know what it is, what a seed is)
2. Know the complexity, i.e. time taken, by the extended gcd algorithm and by successive squaring
3. DES and Rijndael (know the basic large-scale structure but leave out the details)
4. Modes of operation for block ciphers: electronic codebook and cipher block chaining (you can ignore the others)
5. Basics of how passwords are handled by a server
6. The use of chinese remainder theorem to make computations efficient on a computer; the use of chinese remainder theorem in radar.

Miscellaneous

These words should hold meaning for you. I may refer to them on the exam.

1. enciphering, deciphering, plaintext, ciphertext, key

2. block cipher
3. symmetric key cryptography
4. public key cryptography
5. Alice, Bob, Eve, Oscar, Mallory
6. keyspace
7. man-in-the-middle attack