Ciphers and number theory: revision notes

Here is a list of the main topics which were covered in the course, and an indication of the kinds of procedures you should be able to carry out. This list is not necessarily exhaustive, as anything covered in class could be examinable, but concentrates on the main areas in the module.

Chapter 1

- know the definitions of Caesar, keyword, and general monoalphabetic substitution ciphers, and how to encrypt and decrypt using them.
- understand the use of the terminology cipher, plaintext, and ciphertext.
- know the definition of a permutation cipher.
- know the definition of the railfence cipher, and how to encrypt and decrypt using this.
- understand the basic ideas behind frequency analysis, and be able to explain how it can be used to attack a monoalphabetic substitution.
- know the definition of a polyalphabetic substitution
- know the definition of the Vigenère and Playfair ciphers, and how to encrypt and decrypt using them.

Chapter 2

- know the definition of a divisor, and of the notation $r = a \bmod b$ and $r \equiv a \bmod b$.
- know the definition of the GCD of two integers (and of two integers being coprime) and know how to calculate the GCD using the Euclidean Algorithm.
- know the statement of Bezout's identity, and be able to calculate it using the Extended Euclidean Algorithm.
- know the definition of $\mathbb{Z}_n$, and be able to carry out addition, subtraction, and multiplication in this.
- be able to calculate the remainder of a^b on division by n.
- know the definition of the inverse of an element y in $\mathbb{Z}_n$, and be able to state a condition that y and n must satisfy for the inverse to exist.
- be able to calculate inverses to elements in $\mathbb{Z}_n$ using Bezout's identity.
- know how to write a message as a series of blocks in $\mathbb{Z}_n$.
- know the definition of an affine cipher, be able to verify when a function gives such a cipher, and be able to encrypt and decrypt with it.

Chapter 3

- know the definition of the Euler ϕ-function and of a reduced residue system.
- be able to transform one reduced residue system into another.
- be able to state Euler's theorem and Fermat's little theorem.
- be able to state the Chinese Remainder Theorem, and use it to solve simultaneous congruences.
- know the definition of a multiplicative function.
- know the general formula for calculating $\phi(n)$ given a prime factorisation of n.
- know how to carry out fast exponentiation.

Chapter 4

- be able to explain the basic idea behind public key cryptography (including the notion of public and private keys).
- be able to describe and implement the RSA algorithm.
- know the definition of a primitive root and of the discrete logarithm.
- be able to describe and implement Diffie-Helman key exchange and ElGamal encryption.
- be able to explain how to use the CRT to speed up decryption in RSA.

Chapter 5

- know the definition of prime and of composite numbers.
- know how to show that there are infinitely many primes.
- be able to state the fundamental theorem of arithmetic.
- know the method of trial division.
- be able to state and apply Fermat's test.
- know the definition of pseudoprimes and of Carmichael numbers.
- be able to state Wilson's theorem and its converse, and the associated primality test.
- be able to state and apply the Miller-Rabin test to a given base.
- know the definition of strong pseudoprimes, and that there is no strong analogue of Carmichael numbers.
- be able to explain how the Miller-Rabin test gives a probabilistic primality test.