Coursework 6G7Z1011 Cryptography and Encryption

Keith Yates

February 15, 2019

Abstract

Answer all questions. The deadline is stated on moodle; submission is via moodle: a zip file containing a pdf file (named in the format surname-idnumber.pdf;for example, yates-01900300.pdf) and any java files that you used to solve the problems.

0.0.1 ✑:

Answer all questions, each question carries 25 marks, a large proportion of the question can be answered by referring to the slides and using the problems and examples found there. If you answer a problem using Java code then comment the code.

1 Mathematical Tools

1. Define the terms: group, ring, field, normal subgroup, abelian group, and provide examples of each. Determine, by hand the addition and multiplication tables for the rings $\mathbb{F}_{3^2}$ and $\mathbb{Z}_9$. [8]
2. Consider a function $f : X \to Y$, explain what is meant by the terms: injective, inverse and trapdoor. Discuss the relevance of these concepts to cryptography. [8]
3. Consider the specific primes $P = \{7, 11, 13, 17\}$, for each $p \in P$ determine the generators of $\mathbb{F}_p^*$ (recall $\mathbb{F}_p^*$ is the group of size $p - 1$ formed by removing 0 from $\mathbb{F}_p$) [9]

2 Private Key Encryption

1. Many private key encryption algorithms use *permutations* of bits, *confusion* and *diffusion*; define the terms in italics. [6]
2. Discuss (no need for coding) the principles behind the DES algorithm and comment on how secure it is. What variants of the algorithm exist, and how do they improve on DES? [6]
3. Denote by S_n the permutation group on n objects. Explain what is meant by the terms transposition and generating set, and give examples of both in the case of S_5. [6]
4. Write a Java program that takes two arguments a string A and a filename B, the string A is a permutation of the letters a to z, for example A=‘qwertyuiopasdfghjklzxcvbnm’ is such a permutation. The program opens file B and encrypts the plain text within it by permuting the characters according to the key A, for example with the key A then a ↦ q, b ↦ w, c ↦ e, so abc ↦ qwe. The encrypted data is written to a file with the same name as B but with a .encrypt extension. [7]

3 Public Key Encryption

1. What fundamental problem did public key encryption solve that private key encryption could not? [4]
2. Bob and Alice wish to use private key encryption to communicate; explain the basic steps that allow then to established a shared secret (that is a private shared key) over an insecure channel. Illustrate by using representative data values; to keep things simple use small primes in your discussion. [6]
3. Find the solutions (by written calculation no java) to the following problems:
   (a) The remainder when 24^{1947} is divided by 17.

   (b) Let p be a prime number $p > 2$, is it true that for all a that

   $$a^p = a \mod p?$$

   Prove or find a counter-example.

   (c) Let p be a prime number. Let $a^p = b^p \mod p$ then does this imply $a = b \mod p$? Prove or find a counter-example.

   [15]

4 RSA

1. Briefly describe how the RSA algorithm works. [5]
2. The strength of the RSA encryption protocol depends on the difficulty of factorizing a large number into its prime components. Describe one algorithm used in cryptographic factorization theory. [5]
3. Use Pollard's $p - 1$ method and a written calculation to determine a factor of $n = 2813$. [5]
4. Let x be an odd integer is it always true that $x^2 = 1 \mod 8$? [5]
5. Denote by $\pi(n)$ the number of prime numbers between 1 and n. Plot the graph $\frac{\pi(n)}{n}$ how does the function decay for large n and what does its distribution tell you about the frequency of the prime numbers? [5]