Crypto and SecDev Example Paper

1. Calculate 1 / 8 mod 11 (the inverse of 8) by hand using the equation subtracting algorithm. Use your result to calculate 5 / 8 mod 11. [8 marks]

2. It is proposed that a modern mechanical rotor machine would make a useful encryption machine since it does not rely on computer technology, which can be compromised. How many rotors would be needed for secure encryption? Justify your answer. [6 marks]

3. An isolated civilisation has developed a written language based on an alphabet with just 4 letters: α, β, γ and δ. Their written documents are very long. The letters do not occur with equal frequency: α occurs 3/8 of the time ; β and γ 1/4 of the time each and δ 1/8 of the time. The probability of any two letter combination occurring is however just the product of the probability of each letter occurring independently and there are no special digrams or trigrams. Calculate the redundancy of his language. You do not need to calculate an exact number but can leave terms like $\log_2(3)$ in your answer. [12 marks]

4. How is polynomial arithmetic similar and how does it differ from using integers mod n? In what way is it better? When must integers mod n be used rather than polynomial arithmetic? [6 marks]

What is the difference between `a+b` and `a-b` when `a` and `b` are both integers `mod 2`? [3 marks]

Convert 1916_2 and 1170_2 to polynomials, add them up, and convert the answer back to bit strings. [3 marks]

5. Describe the RSA public key encryption system and show how it works when prime numbers 5 and 7 are used to construct the modulus n = 35. Choose an encryption parameter e and calculate the corresponding decryption parameter d. Use these values to encrypt the plaintext value 17 and decrypt the resulting cipher text to recover the plaintext. [10 marks]

6. What is the difference between a peer-to-peer network and a centralised network? What things are harder to do with a peer-to-peer network? [3 marks]

   Why do digital coins have a unique ID while pound coins do not? Is this similar to the unique ID on bank notes? [3 marks]

   What is a crypto-coin ledger and why is it important? [3 marks]

   How can you get change when you spend your crypto-coin? [3 marks]