Tutorial 4 Solutions

1. *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?*

   What is the difference between `a+b` *and* `a-b` *when* `a` *and* `b` *are both integers* `mod 2`*?*

   Convert 1010_2 *and* 110_2 *to polynomials, add them up, and convert the answer back to bit strings.*

   Polynomial arithmetic has the concept of a prime polynomial. All polynomials except 0 will have an inverse if their arithmetic is mod a prime (irreducible) polynomial. Polynomial arithmetic where the coefficients are integers mod 2 is more convenient than integers mod n because bitstrings can be converted directly into polynomials. Prime numbers are not powers of 2, and so bit strings need to be converted to integers before integers mod n, where n is not a power of 2, are used.

   Assignment Project Exam Help

   A+b and a-b are both the same because + and – are both xor.

   https://powcoder.com

   $x^3 + x$, and $x^2 + x$. Adding them gives $x^3 + x^2 + 2x + 1$, but $2x = 0$, so the addition gives $x^3 + x^2$. This corresponds to 1100_2.

2. *Describe how the Rijndael AES encryption algorithm uses polynomial arithmetic. What is the advantage of using this arithmetic over the use of S-boxes in DES?*

   Add WeChat powcoder

   8-bit polynomial arithmetic is used to transform single data bytes in the SubBytes stage. Polynomials of degree 4 where the coefficients are 8-bit polynomials are used in the MixColumns stage. These polynomials are reduced mod $X^4 + 1$, which is not irreducible.

3. *An organisation has decided that its secrets are too valuable to entrust to just one person, and has decided that three people will be needed to access the secret information. Devise a scheme that will allow the head of the organisation to issue passwords to three people in such a way that all three passwords are needed simultaneously. Give a numerical example of the operation of your scheme when the secret is the number 42. You may assume that each secret is a 6 bit number.*

   Pick two random bitstrings r1 and r2 and hand out r1, s ⊕ r2, r1 ⊕ r2 as the three keys (⊕ is the exclusive or operator). The secret can be recovered by exclusive oring the three keys. The numerical example converts 42 to a bitstring 101010, choosing two random bitstrings, such as 110011 and 011101 and performing the above calculations to generate the keys 110011, 110111, 101110. Combining these three results in 1 ⊕ 1 ⊕ 1 = 1 for the first bit, and so on, recovering 101010.

© 2017 Ron Poet

4. *One drawback of the previous scheme is that all three persons are needed to operate it. All secrets would be lost if one person were to have an accident. Devise an alternative scheme where three people are still needed to access the information, but five people have parts of the key. Any three people will be sufficient. A numerical example is not needed!*

   A Lagrangian interpolation scheme would work for this case. The basic curve is $y = a x^2 + b x + s \pmod n$, where a and b are random and n large enough. 5 values of x are chosen at random, and the resulting values of y (together with x) handed out as keys. Any three of the (x, y) pairs can be used to recover the polynomial and hence find s.

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

© 2017 Ron Poet