Cryptography & Encryption:6G7Z1011: Lab Questions

Keith Yates

March 8, 2019

Cryptography & Encryption:6G7Z1011 : Digital Signatures, and Introduction to Collision Algorithms

1 Cryptography & Encryption:6G7Z1011 : Digital Signatures, and Introduction to Collision Algorithms

2 Problems & Supplementary Material:Problems

2.1 problem:iterative solution

⌜We present an iterative way of solving (certain types of equations). Suppose we wished to solve $x^3 - x - 1 = 0$ on $[1, 2]$. The fixed point iteration requires

$$f : [1, 2] \to [1, 2], x \mapsto f(x) = (1 + x)^{1/3} \tag{1}$$

The idea being if $x = f(x)$ we have a fixed point. Write a Java method that takes a starting point x_1 and finds the solution to $x^3 - x - 1 = 0$ to four decimal places. To commence let $x_1 = 1.1$
⌟

2.2 problem:Digital Signatures

⌜Code the RSA Digital Signature algorithm in JAVA.

1. Sam picks two primes $p = 1223$ and $q = 1987$; check they are prime. Evaluate

$$N = p.q = 1223.1987 = 2430101. \tag{2}$$

2. Sam picks a verification exponent $v = 948047$ check

$$\gcd(v, (p - 1)(q - 1)) = 1 \tag{3}$$

3. Sam's signing key is the s that solves

$$sv = 1 \mod (p - 1)(q - 1); \tag{4}$$

find s (you should get $s = 1051235$.)

4. Suppose the document is $D = 1070777$ then the signed document is

$$S = D^s \tag{5}$$

Sam makes S (the signed document), D (the actual document) and v (the verification exponent) and N available.

5. Victor has access to N, v, S and D, Sam evaluates

$$S^v \mod N, \tag{6}$$

and it should equal D.

⌟

2.3 problem:Probability and Combinatorics

⌜

1. How many different seven letter words can be formed from the symbols A, B and C?
2. Using the seven letters A, A, A, A, B, B, B how many different words of length seven can be formed?
3. A fair coin is flipped six times, find the probability that:
   1. The result is six heads.
   2. Exactly one head occurs.
   3. There are the same number of heads as there are tails.
   4. A *n-sequence* is when the same result (head or tail) turns up n-times so HHHTHT contains a 3-sequence of heads. What is the probabilty that no sequence of length 2 or greater occurs in the six flips?

⌟

2.4 problem:

⌜Continue with your assignment. ⌟