Top of Form

Homework

1. **Prepare for Mathematical Induction Test. Forum with practice questions will be open today**

Please present a proof validity of these statements by Mathematical Induction

1. 9n-3n is divisible by 6 for any n >0

Basis n = 1

91 – 31 = 6 is divisible by 6

n = k

9k – 3k is divisible by 6

n = k+1

9k+1 – 3k+1 is divisible by 6

= 9k.9 – 3k.3

= (6+3)9k – 3k.3

= 6.9k + 3.9k – 3.3k

= 6.9k + 3(9k – 3k)

Since 9k – 3k is divisible by 6

So 9k+1 – 3k+1 is divisible by 6

1. 10n-2n is divisible by 4 for any n

Basis n = 1

101 – 21 = 8 is divisible by 4

n = k

10k – 2k is divisible by 4

n = k+1

10k+1 – 2k+1 is divisible by 4

= 10k.10 – 2k.2

= (8+2)10k – 2k.2

=8.10k +2.10k – 2k.2

= 8.10k + 2(10k – 2k)

Since 10k – 2k is divisible by 4

So 10k+1 – 2k+1 is divisible by 4

1. 9n-1 is divisible by 4 for any n >0

Basis n = 1

91 – 1 = 8 is divisible by 4

n = k

9k – 1 is divisible by 4

n = k+1

9k+1 – 1 is divisible by 4

= 9k.9 – 1

= 9(9k -1) +8

Since 9k – 1 is divisible by 4

So 9k+1 – 1 is also divisible by 4

1. 1+2+…+ n = n(n+1)/2 for any n >0

We assume n = k

1+2+...+k = k(k+1)/2

n = k+1

1+2+..

.+k+(k+1) = ((k+1)(k+1+1))/2

1. 2+4+6+… +2n= n(n+1) for any n >0
2. 1+5+9+…+(4n-3) = n(2n-1) for any n >0

Here are 4.0 questions mentioned before. Please work on them already, if you want 4.0. If you almost have a proof and just little piece is missing, you may send me your thoughts. If I think that you are on the right track, I'll help you with a hint.

1. Please show that an algorithm with complexity n^2 is more efficient than an algorithm with complexity 2^n. In other words, starting from some n, n^2 < 2^n

2.  Please show that an algorithm with complexity 2^n is more efficient than an algorithm with complexity n!. In other words, starting from some n,  2^n < n!

1. **Diffie-Hellman**

**Design a protocol for four people: Alice, Bob, Carol and Peter**

**Prove Correctness of the algorithm**

Diffie-Hellman key exchange protocol can be easily extended to work with four people. In this example Alice, Bob, Carol and Peter together genereate a secter key:

Round 1

1. Alice chooses a randomly large number p and sends Bob

P= gp mod n

2. Bob chooses a randomly large number q and sends Carol

Q= gq mod n

3. Carol chooses a randomly large number r and sends Peter

R= gr mod n

4. Peter chooses a randomly large number s and sends to Alice.

S= gs mod n

Round 2

5. Alice sends Bob

P’ = Sp mod n

6. Bob sends Carol

Q’ = Pq mod n

7. Carol sends Peter

R’ = Qr mod n

8. Peter sends Alice

S’ = Rs mode n

Round 3

9. Alice sends Bob

P” = S’p mod n

10. Bob sends Carol

Q” = P’q mod n

11. Carol sends Peter

R” = Q’r mod n

12. Peter sends Alice

S” = R’s mod n

Round 4

13. Alice computes

K = S”p mod n

14. Bob computes

K’ = P”q mod n

15. Carol computes

K” = Q”r mod n

16. Peter computes

K”’ = R”s mod n

Note K, K’, K” and K”’ are equal gpqrs mod n.

Example:

The general one-way function is 7k mod 11.

Step 1.

* Alice chooses a number, say 3, and keeps it secret. We label her number P
* Bob chooses a number, say 6, and keep it secret. We label his number Q
* Carol chooses a number, say 5, and keep it secret. We label her number R
* Peter chooses a number, say 3, and keep it secret. We label his number S

Step 2

* Alice puts 3 into the one-way function and works out the result of 73 mod 11=2. Let us call the result of this calculation P.
* Bob puts 6 into the one-way function and works out the result of 76 mod 11 = 4. Let us call the result of this calculation Q.
* Carol puts 4 into the one-way function and works out the result of 75 mod 11= 10. Let us call the result of this calculation R.
* Peter puts 5 into the one-way function and works out the result of 73 mod 11 = 2. Let us call the result of this calculation S.

Step 3

* Alice puts 3 into the one-way function and works out the result of 23 mod 11=8. Let us call the result of this calculation P’.
* Bob puts 6 into the one-way function and works out the result of 26 mod 11 = 9. Let us call the result of this calculation Q’.
* Carol puts 4 into the one-way function and works out the result of 45 mod 11= 1. Let us call the result of this calculation R’.
* Peter puts 5 into the one-way function and works out the result of 103 mod 11 = 10. Let us call the result of this calculation S’.

Step 4

* Alice puts 3 into the one-way function and works out the result of 103mod 11 = 10. Let us call the result of this calculation P”.
* Bob puts 6 into the one-way function and works out the result of 86 mod 11 = 3. Let us call the result of this calculation Q”.
* Carol puts 4 into the one-way function and works out the result of 95 mod 11 = 1. Let us call the result of this calculation R”.
* Peter puts 5 into the one-way function and works out the result of 13 mod 11 = 1. Let us call the result of this calculation S”.

Step 5

* Alice computes K = 13 mod 11 = 1
* Bob computes K’ = 106mod 11 = 1
* Carol computes K” = 35 mod 11 = 1
* Peter computes K”’ = 13 mod 11 = 1

Obviously, K= K’= K” = K”’

Bottom of Form