**Cryptography Assignment - 1**

**Pramod Aravind Byakod**

**1. Treat your OUID number as a decimal integer.**

**1) Find its representation in base 26 (A = 0, B=1, ..., Z = 25)**

|  |  |  |  |
| --- | --- | --- | --- |
| Divider | Dividend | Quotient | Reminder |
| 26 | 113436879 |  |  |
|  |  | 4362956 | 23 |
|  |  | 167806 | 0 |
|  |  | 6454 | 2 |
|  |  | 248 | 6 |
|  |  | 9 | 14 |

A=0 B=1 C=2 D=3 E=4 F=5 G=6 H=7 I=8 J=9 K=10 L=11 M=12 N=13 O=14 P=15 Q=16 R=17 S=18 T=19 U=20 V=21 W=22 X=23 Y=24 Z=25

**(113436879)10 = 9 14 6 2 0 23 -> (JOGCAX)26**

**2) Multiply the result of 1) by DALLAS, and output the product in base 26**

(DALLAS)26 = S\*260 + A\*261 + L\*262 + L\*263 + A\*264 + D\*265

= 18\*260 + 0\*261 + 11\*262 + 11\*263 + 0\*264 + 3\*265

= (35844918)10

(DALLAS)26 \* (JOGCAX)26  = (35844918)10 \* (113436879)10

= (4066135625930922)10

|  |  |  |  |
| --- | --- | --- | --- |
| Divider | Dividend | Quotient | Reminder |
| 26 | 4066135625930922 |  |  |
|  |  | 156389831766573 | 24 |
|  |  | 6014993529483 | 15 |
|  |  | 231345904980 | 3 |
|  |  | 8897919422 | 8 |
|  |  | 342227670 | 2 |
|  |  | 13162602 | 18 |
|  |  | 506253 | 24 |
|  |  | 19471 | 7 |
|  |  | 748 | 23 |
|  |  | 28 | 20 |
|  |  | 1 | 2 |

(4066135625930922)10 = 1 2 20 23 7 24 18 2 8 3 15 24

= (BCUXHYSCIDPY)26

**(DALLAS)26 \* (JOGCAX)26  = (BCUXHYSCIDPY)26**

**3) Divide the result of 2) by OKC, and find the remainder and quotient, all in base 26.**

(OKC)26 = C\*262 + K\*261 + O\*260

= 2\*262 + 10\*261 + 14\*260

= (9726)10

(BCUXHYSCIDPY)26 / (OKC)26 = (4066135625930922)10 / (9726)10

= (418068643422)10

|  |  |  |  |
| --- | --- | --- | --- |
| Divider | Dividend | Quotient | Reminder |
| 26 | 418068643422 |  |  |
|  |  | 16079563208 | 14 |
|  |  | 618444738 | 20 |
|  |  | 23786336 | 2 |
|  |  | 914859 | 2 |
|  |  | 35186 | 23 |
|  |  | 1353 | 8 |
|  |  | 52 | 1 |
|  |  | 2 | 0 |

(418068643422)10 = 2 0 1 8 23 2 2 20 14

= (CABIXCCUO)26

**(BCUXHYSCIDPY)26 / (OKC)26 = (CABIXCCUO)26**

**2. Read a few articles online about the Great Internet Mersenne Prime Search (GIMPS). Argue that if n is a composite integer,**

**then 2^n - 1 is also a composite integer.**

**Method 1**

Let n be composite.

Then there exist a and b, both greater than 1, such that n=ab.

Note that 2n−1 = 2ab−1

= (2a)b−1

Let x=2a

Note that x−1 divides xb−1, for xb −1= (x−1) (xb-1 +xb-2+…………+1).

We still need to check that 2a −1 is a proper divisor of 2n−1.

Below is the proof

Let m=2a−1.

Then 2a=1 (mod m)

It follows that (2a)b = 1 (mod m), so m divides (2a)b−1.

Hence proved that if n is a composite integer, so is 2n-1.

Lets look at another way of proving this.

**Method 2**

Suppose n is composite.

Then n = ab for some integers a, b ≥ 2.

Since 2a ≡ 1 mod (2a − 1), we have 2n = (2a )b ≡ 1b = 1 mod (2a − 1).

Thus, 2n − 1 is divisible by 2a − 1, and since 1 < a < n.

The integer 2a − 1 is a proper divisor of 2n − 1 (i.e., strictly greater than 1 and less than n). Hence 2n − 1 is composite.