Air Force Institute of Technology
Department of Electrical and Computer Engineering
Data Security(CSCE 544)
Homework #5
Due Date: **20-May-2019**

1 [10 points] Given the following RSA public-key: pk ={e,n} ={5, 29623244235986089658629749102364587250074379396847895501789 74023998496502140571365918899417655751929}

1.1 [8 points] Determine the prime numbers p and q:

The two prime numbers are shown below, factored using msieve:

```
p50 factor: 47720170418078602591676381343885005276759196131213
p50 factor: 62076987522164082179415623963823156278081468066333
```

1.2 [2 points] Compute Euler's Totient function $\phi(n)$:

The totient function is shown below:

$\phi(n) = 2962324423598608965862974910236458725007437939684679753021033781313725410135263657757344576991554384$

2 [30 points] Given prime numbers $p = 315349$ and $q = 259907$ and $e = 5$:

2.1 [7 Points] Construct public key pk={e,n}

Using $n = p \cdot q$, this gives the following public key:

$$pk = (5, 81961412543)$$

2.2 [7 Points] Determine Euler's totient function $\phi(n)$:

Using $\phi(n) = (p-1) \cdot (q-1)$, this gives the following:

$$\phi(n) = 81960837288$$

2.3 [7 Points] Determine the private-key={d,n}:

Using $e \cdot d = 1 \mod \phi(n)$, gives the following key:

$$private\,key = (49176502373,\ 81961412543)$$

2.4 [9 Points] Compute the cipher text for EACH of the following ASCII (8-bits) characters: `‘‘The US Army will never control the ground under the sky, if the US Air Force does not control the sky over the ground.’’ -- Col Gene Cirillo, USAF (Ret).`

The ciphertext is shown below:

```
[8153726976, 8153726976, 4182119424, 12166529024, 10510100501, 33554432, 4437053125,
    3939040643, 33554432, 1160290625, 19254145824, 15386239549, 25937424601,
   33554432, 23863536599, 12762815625, 14693280768, 14693280768, 33554432,
   16105100000, 10510100501, 22877577568, 10510100501, 19254145824, 33554432,
   9509900499, 16850581551, 16105100000, 21003416576, 19254145824, 16850581551,
   14693280768, 33554432, 21003416576, 12166529024, 10510100501, 33554432,
   11592740743, 19254145824, 16850581551, 21924480357, 16105100000, 10000000000,
   33554432, 21924480357, 16105100000, 10000000000, 10510100501, 19254145824,
   33554432, 21003416576, 12166529024, 10510100501, 33554432, 20113571875,
   14025517307, 25937424601, 164916224, 33554432, 12762815625, 11040808032,
   33554432, 21003416576, 12166529024, 10510100501, 33554432, 4437053125,
   3939040643, 33554432, 1160290625, 12762815625, 19254145824, 33554432,
   1680700000, 16850581551, 19254145824, 9509900499, 10510100501, 33554432,
   10000000000, 16850581551, 10510100501, 20113571875, 33554432, 16105100000,
   16850581551, 21003416576, 33554432, 9509900499, 16850581551, 16105100000,
   21003416576, 19254145824, 16850581551, 14693280768, 33554432, 21003416576,
   12166529024, 10510100501, 33554432, 20113571875, 14025517307, 25937424601,
   33554432, 16850581551, 22877577568, 10510100501, 19254145824, 33554432,
   21003416576, 12166529024, 10510100501, 33554432, 11592740743, 19254145824,
   16850581551, 21924480357, 16105100000, 10000000000, 205962976, 90224199,
   90224199, 33554432, 184528125, 184528125, 33554432, 1350125107, 16850581551,
   14693280768, 33554432, 1804229351, 10510100501, 16105100000, 10510100501,
   33554432, 1350125107, 12762815625, 19254145824, 12762815625, 14693280768,
   14693280768, 16850581551, 164916224, 33554432, 4437053125, 3939040643,
   1160290625, 1680700000, 33554432, 102400000, 3707398432, 10510100501,
   21003416576, 115856201, 205962976]
```

Ciphertext.txt

3 [30 points] Given the following prime numbers, list all numbers α that can be used as generators in a cyclic group $\mathbb{Z}_p^*$

1. 41

   $\alpha \in$ [6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35]

2. 43

   $\alpha \in$ [3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34]

3. 71

   $\alpha \in$ [7, 11, 13, 21, 22, 28, 31, 33, 35, 42, 44, 47, 52, 53, 55, 56, 59, 61, 62, 63, 65, 67, 68, 69]

4. 73

   $\alpha \in$ [5, 11, 13, 14, 15, 20, 26, 28, 29, 31, 33, 34, 39, 40, 42, 44, 45, 47, 53, 58, 59, 60, 62, 68]

5. 541

   $\alpha \in$ [2, 10, 13, 14, 18, 24, 30, 37, 40, 51, 54, 55, 59, 62, 65, 67, 68, 72, 73, 77, 83, 86, 87, 91, 94, 96, 98, 99, 107, 113, 114, 116, 117, 126, 127, 128, 131, 132, 138, 150, 152, 153, 156, 158, 163, 176, 181, 183, 184, 195, 197, 199, 206, 208, 210, 213, 218, 220, 223, 224, 244, 248, 250, 257, 258, 259, 260, 261, 263, 267, 269, 270, 271, 272, 274, 278, 280, 281, 282, 283, 284, 291, 293, 297, 317, 318, 321, 323, 328, 331, 333, 335, 342, 344, 346, 357, 358, 360, 365, 378, 383, 385, 388, 389, 391, 403, 409, 410, 413, 414, 415, 424, 425, 427, 428, 434, 442, 443, 445, 447, 450, 454, 455, 458, 464, 468, 469, 473, 474, 476, 479, 482, 486, 487, 490, 501, 504, 511, 517, 523, 527, 528, 531, 539]

4 [30 points] Alice and Bob publicly agree to use a modulus $p = 1999$ and a generator $\alpha = 1994$. Alice chooses a secret integer $a = 1997$, and Bob chooses a secret integer $b = 2001$. Compute the shared secret integer s using the Diffie-Hellman Key Exchange algorithm.

The secret integer s is 1983.

5 [50 points] Alice and Bob publicly agree to use a modulus $p = 2999$ and a generator $\alpha = 161$. Alice sends secret integer $a = 2341$ to Bob, and Bob sends secret integer $b = 192$. Compute the shared secret integer s using the Diffie-Hellman Key Exchange algorithm.

The secret integer s is 2377. The code for Problems 4 and 5 is shown in the attached Python scripts.