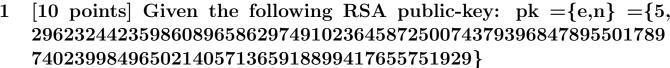
Air Force Institute of Technology Department of Electrical and Computer Engineering Data Security(CSCE 544)

Homework #5 Due Date: 20-May-2019

May 13, 2019 Micah Hayden Page 1 of 2



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

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

- [30 points] Given prime numbers p = 315349 and q = 259907 and e = 5: 2
- [7 Points] Construct public key pk={e,n}
- [7 Points] Determine Euler's totient function $\phi(n)$:
- 2.3[7 Points] Determine the private-key= $\{d,n\}$:
- [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).

[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
- 2. 43
- 3. 71
- 4. 73
- 5. 541

Air Force Institute of Technology Department of Electrical and Computer Engineering Data Security(CSCE 544)

Homework #5
Due Date: **20-May-2019**

May 13, 2019 Micah Hayden Page 2 of 2

3 [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.

4 [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.