Brandon Brown

CS 298 – 71

Dr. Yantorno

Crypto & Diffie – Hellman Assignment 1

**Crypto Assignment**

Gpg key - <https://github.com/Hockey1801.gpg>

Ssh key - <https://github.com/Hockey1801.keys>

Repo / Commits - [Hockey1801/Hockey: favorite sport (github.com)](https://github.com/Hockey1801/Hockey)

**Diffie – Hellman Key Exchange Assignment**

**Step 1 - 2**

Bob and Alice agree on a prime number of 97 and a generator of 4. **974**

Bob’s private number: 4

Alice’s private number: 8

Bob: 44 = 256/ 97 = 2, with a remainder of 62.

Alice: 48 = 65,536/ 97 = 675, with a remainder of 61.

Bob: 618 = 191,707,312,997,281 / 97 = 1,976,364,051,518, with a remainder of 35.

Alice: 624 = 12,960,000 / 97 = 133,608, with a remainder of 24.

**Step 3 - 5**

136 =

64(5) = 3,656,158,440,062,976/ 13 = 281,242,956,927,921, with a remainder of 3.

117 =

73(6) = 1,628,413,597,910,449/ 11 = 148,037,599,810,040, with a remainder of 9.