Problem Set #6

Due Thursday, November 3 @ 11:59 pm

1. Alice and Bob are using DHKE with $p = 48\ 947$, $\alpha = 7$. Determine the shared key k_{AB} in each case.

   (a) You are Alice and pick $a = 10\ 311$ and receive $B = 32\ 887$ from Bob

   (b) You are Alice and send $A = 40\ 391$ to Bob and receive $B = 16\ 903$ from Bob

   (c) You are Oscar and observe $A = 7671$ and $B = 9720$

2. For each value of p, explain why p is, or is not, a good choice to use with DHKE.
   If p is a good value to use, then find an appropriate α to use.
   Thoroughly explain why α is a good choice and how you found α.

   (a) $p = 15\ 488\ 093$

   (b) $p = 15\ 485\ 989$

   (c) $p = 2^{4096} - 2^{4032} - 1 + 2^{64}(\lfloor 2^{3966}\pi \rfloor + 240904)$

   FYI, the syntax to define p in Mathematica is:

   ```
   p = 2^4096 - 2^4032 - 1 + 2^64*(Floor[2^3966 Pi] + 240904)
   ```

   You should get a very large integer where $p = 1044 \cdots 3247$

3. Use a bifid cipher with key FIRESWAMP to decrypt the message

   ITOW HOFM FIYW GEGF MFFW OWWC IYKD BMHT SYGA DBMH TIYH

   Who sent the message?