# Assignment 2

# Due at the beginning of next class (09/16/14)

**Instructions:**

* **Solve in this document**
* **Print and bring to class**

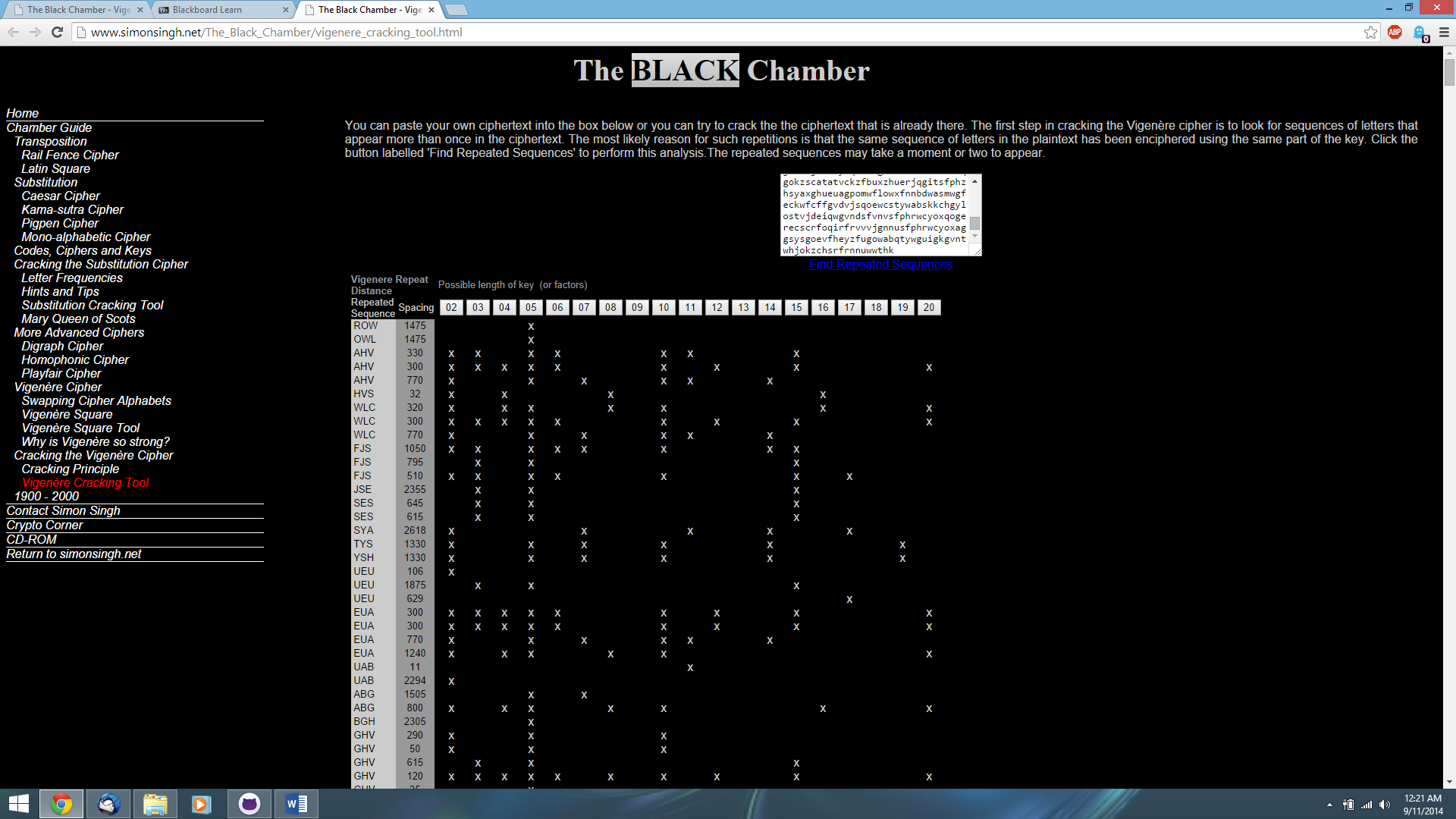
**Name: Michael Trotter**

**Q1. Cracking the Vigenere Cipher (20pts)**

The ciphertext is posted to the blackboard (same folder as the assignment) in a file called “ciphertext”

1. (5pts) Do a **Kasiski’s test on the cipher.** You can use this site:   
     
   <http://www.simonsingh.net/The_Black_Chamber/vigenere_cracking_tool.html>.

Add a screenshot (make it fit in the space below) of the some of the repeated sequences



Based on Kasiski’s test, what do you think the key period is? 5\_\_\_\_\_\_\_\_

1. (5pts) **Index of coincidence over each of the bins (or alphabets, which the term used in the slides)**

|  |  |
| --- | --- |
| Bins | IC |
| bin 1 | 0.0720893742547 |
| bin 2 | 0.0663089185966 |
| bin 3 | 0.0668612314065 |
| bin 4 | 0.0660704198833 |
| bin 5 | 0.0675767275466 |
| ….. |  |

1. (5pts) Find **the letter that has the highest frequency in each bin and use it to guess the key.**

|  |  |  |
| --- | --- | --- |
| Bins | Letter with highest freq. | Assuming this letter is “e” then  the key to decrypt this bin is |
| bin 1 | W (80) | Rotate left by 18 => Rotate right by 8 |
| bin 2 | S (72) | Rotate left by 14 => Rotate right by 12 |
| bin 3 | R (83) | Rotate left by 13 => Rotate right by 13 |
| bin 4 | E (70) | Rotate left by 0 => Rotate right by 0 |
| bin 5 | V (75) | Rotate left by 17 => Rotate right by 9 |
| … |  |  |

1. (5pts) What is the plaintext?

oneoftwobritishexplorershipsthatvanishedinthearcticmorethanonehundredandsixtyyearsagohasbeenfoundcanadasprimeministersaysstephenharpersaiditwasunclearwhichshiphadbeenfoundbutphotoevidenceconfirmeditwasoneofthemsirjohnfranklinledthetwoshipsandonehundredandtwentyninemenineighteenfortyfivetochartthenorthwestpassageinthecanadianarctictheexpeditionsdisappearanceshortlyafterbecameoneofthegreatmysteriesoftheageofvictorianexplorationthecanadiangovernmentbegansearchingforfranklinsshipsintwothousandandeightaspartofastrategytoassertcanadassovereigntyoverthenorthwestpassagewhichhasrecentlybecomeaccessibletoshippingbecauseofmeltingarcticiceexpeditionsonarimagesfromthewatersofvictoriastraitjustoffkingwilliamislandclearlyshowthewreckageofashipontheoceanflooriamdelightedtoannouncethatthisyearsvictoriastraitexpeditionhassolvedoneofcanadasgreatestmysterieswiththediscoveryofoneofthetwoshipsbelongingtothefranklinexpeditionprimeministerstephenharpersaidinastatementfindingthefirstvesselwillnodoubtprovidethemomentumorwindinoursailsnecessarytolocateitssistershipandfindoutevenmoreaboutwhathappenedtothefranklinexpeditionscrewthefindhasbeendescribedasthebiggestarchaeologicaldiscoverytheworldhasseensincetheopeningoftutankhamunstombalmostonehundredyearsagobyabritisharchaeologistwilliambattersbywhohaswrittenextensivelyaboutthefranklinexpeditionfromtheimagesitisclearthatahugeamountofevidencewillbepreservedfromtheexpeditionpossiblyevenincludingtheremainsofthemenandmaybejustpossiblysomeoftheirphotographshesaidthelossofhmserebusandhmsterrorwhichwasbuiltintopshamdevonpromptedoneoflargestsearchesinhistoryrunningfromeighteenfortyeighttoeighteenfiftyninethemysteryhasgrippedpeopleforgenerationsinpartbecausenooneknowsforsureexactlywhathappenedtothecrewexpertsbelievetheshipswerelostwhentheybecamelockedintheicenearkingwilliamislandandthatthecrewsabandonedtheminahopelessbidtoreachsafetyreportsatthetimefromlocalinuitssaythemendesperateforfoodresortedtocannibalismbeforetheydiedsirjohnfranklinswifespearheadedanattempttofindhimlaunchingfiveshipsinsearchofherhusbandandevenleavingcansoffoodontheiceinthedesperatehopehewouldfindthemintotalmorethanfiftyexpeditionsjoinedthesearchthreebodiesdiscoveredoveracenturylaterinthenineteeneightyswerefoundtohaveahighleadcontentandtothisdaymanypeoplebelievetheonehundredandtwentyninecrewmemberswerepoisonedbyleakingleadintheirpoorlysolderedtincansmorerecentresearchsuggeststhecannedfoodsuppliedtofranklinwasnotacidicenoughforthattohappenandtheleadwasmorelikelytohavecomefromtheinternalpipesystemontheshipsthesearchresultedinthediscoveryofthenorthwestpassagewhichrunsfromtheatlantictothepacificthroughthearcticarchipelagothediscoveryoffranklinsvesselsisconsideredoneofthemostsoughtafterprizesinmarinearchaeologyateamofcanadiandiversandarchaeologistshasbeentryingtofindtheshipssincetwothousandandeight