Quiz 3
Answer

1. Determine the keyword length of these two encrypted message using I.C.

For Part 1, we determine the keyword length by the following steps:

1. Assume the keyword length = n, n >= 2.

2. Split the encrypted message into n groups.

3. Calculate the I.C. of each group.

4. Calculate the average I.C. of all groups.

5. Increase n by 1 and restart the process until we find the average I.C that is closest to the English value 0.068.

For Message 1, we get the following result:

Keyword Length (n) = 4 , IC = 0.040914228893610 49

Keyword Length (n) = 5 , IC = 0.0657576727070966 8

Keyword Length (n) = 6 , IC = 0.040950905335368 8

Keyword Length (n) = 7 , IC = 0.041660629440825 44

As the result, we can determine that the keyword length of Message 1 = 5.

For Message 2, we get the following result:

Key Length (n) = 4 , IC = 0.044713888814682 23

Key Length (n) = 5 , IC = 0.041331642778006 78

Key Length (n) = 6 , IC = 0.070135022428600 41

Key Length (n) = 7 , IC = 0.042478880798427 09

As the result, we can determine that the keyword length of Message 2 = 6.

2. Solve the encryption keyword letters.

For Part 2, we solve the encryption keyword letters by the following steps:

1. Determine the alphabet frequency.

2. Assume the shift value of alphabet = n, 0 <= n < 26

3. Calculate the inner product of the shifted alphabet and the alphabet frequency.

4. Iterate step 2 and step 3 from n = 0 to n = 25, find the maximum inner product and determine the shift value.

5. Calculate the shift value of each group and find the keyword letters.

According to the step above, we get the result:

For Message 1, keyword letters = HOMER.

For Message 2, keyword letters = POIROT.

3. Break this ciphertext and recover the plaintext.

According to the keyword letters above, we can shift the alphabet of each group correctly and find the plaintext.

For Message 1:

SCEPTICISMISASMUCHTHERESULTOFKNOWLEDGEASKNOWLEDGEISOFSCEPTICISMTO
BECONTENTWITHWHATWEATPRESENTKNOWISFORTHEMOSTPARTTOSHUTOUREARS
AGAINSTCONVICTIONSINCEFROMTHEVERYGRADUALCHARACTEROFOUREDUCATION
WEMUSTCONTINUALLYFORGETANDEMANCIPATEOURSELVESFROMKNOWLEDGEPREVI
OUSLYACQUIREDWEMUSTSETASIDEOLDNOTIONSANDEMBRACEFRESHONESANDASW
ELEARNWEMUSTBEDAILYUNLEARNINGSOMETHINGWHICHITHASCOSTUSNOSMALLLA
BOURANDANXIETYTOACQUIREANDTHISDIFFICULTYATTACHESITSELFMORECLOSELYTO
ANAGEINWHICHPROGRESSHASGAINEDASTRONGASCENDENCYOVERPREJUDICEANDI
NWHICHPERSONSANDTHINGSAREDAYBYDAYFINDINGTHEIRREALLEVELINLIEUOFTHEIR
CONVENTIONALVALUETHESAMEPRINCIPLESWHICHHAVESWEPTAWAYTRADITIONALAB
USESANDWHICHAREMAKINGRAPIDHAVOCAMONGTHEREVENUESOFSINECURISTSAN
DSTRIPPINGTHETHINTAWDRYVEILFROMATTRACTIVESUPERSTITIONSAREWORKINGAS
ACTIVELYINLITERATUREASINSOCIETYTHECREDULITYOFONEWRITERORTHEPARTIALITY
OFANOTHERFINDSASPOWERFULATOUCHSTONEANDASWHOLESOMEACHASTISEMENT
INTHEHEALTHYSCEPTICISMOFATEMPERATECLASSOFANTAGONISTSASTHEDREAMSOFC
ONSERVATISMORTHEIMPOSTURESOFPLURALISTSINECURESINTHECHURCHHISTORYAN
DTRADITIONWHETHEROFANCIENTORCOMPARATIVELYRECENTTIMESARESUBJECTEDT
OVERYDIFFERENTHANDLINGFROMTHATWHICHTHEINDULGENCEORCREDULITYOFFOR
MERAGESCOULDALLOWMERESTATEMENTSAREJEALOUSLYWATCHEDANDTHEMOTIVE
SOFTHEWRITERFORMASIMPORTANTANINGREDIENTINTHEANALYSISOFHISHISTORYAS
THEFACTSHERECORDSPROBABILITYISAPOWERFULANDTROUBLESOMETESTANDITISBY
THISTROUBLESOMESTANDARDTHATALARGEPORTIONOFHISTORICALEVIDENCEISSIFTE
DCONSISTENCYISNOLESSPERTINACIOUSANDEXACTINGINITSDEMANDSINBRIEFTOWRI
TEAHISTORYWEMUSTKNOWMORETHANMEREFACTSHUMANNATUREVIEWEDUNDER
ANINDUCTIONOFEXTENDEDEXPERIENCEISTHEBESTHELPTOTHECRITICISMOFHUMAN
HISTORYHISTORICALCHARACTERSCANONLYBEESTIMATEDBYTHESTANDARDWHICHHU

MANEXPERIENCEWHETHERACTUALORTRADITIONARYHASFURNISHEDTOFORMCORRECTVIEWSOFINDIVIDUALSWEMUSTREGARDTHEMASFORMINGPARTSOFAGREATWHOLEWEMUSTMEASURETHEMBYTHEIRRELATIONTOTHEMASSOFBEINGSBYWHOMTHEYARESURROUNDEDANDINCONTEMPLATINGTHEINCIDENTSINTHEIRLIVESORCONDITIONWHICHTRADITIONHASHANDEDDOWNTOUSWEMUSTRATHERCONSIDERTHEGENERALBEARINGOFTHEWHOLENARRATIVETHANTHERESPECTIVEPROBABILITYOFITSDETAILS

For Message 2:

THATPROCESSSAIDISTARTSUPONTHESUPPOSITIONTHATWHENYOUHAVEELIMINATEDALLWHICHISIMPOSSIBLETHENWHATEVERREMAINSHOWEVERIMPROBABLEMUSTBETHETRUTHITMAYWELLBETHATSEVERALEXPLANATIONSREMAININWHICHCASEONETRIESTESTAFTERTESTUNTILONEOROTHEROFTHEMHASACONVINCINGAMOUNTOFSUPPORTWEWILLNOWAPPLYTHISPRINCIPLETOTHECASEINPOINTASITWASFIRSTPRESENTEDTOMETHEREWERETHREEPOSSIBLEEXPLANATIONSOFTHESECLUSIONORINCARCERATIONOFTHISGENTLEMANINANOUTHOUSEOFHISFATHERSMANSIONTHEREWASTHEEXPLANATIONTHATHEWASINHIDINGFORACRIMEORTHATHEWASMADANDTHATTHEYWISHEDTOAVOIDANASYLUMORTHATHEHADSOMEDISEASEWHICHCAUSEDHISSEGREGATIONICOULDTHINKOFNOOTHERADEQUATESOLUTIONSTHESETHENHADTOBESIFTEDANDBALANCEDAGAINSTEACHOTHER

Bonus 1: Recover the two hash values.

5f4dcc3b5aa765d61d8327deb882cf99

=> password

5a105e8b9d40e1329780d62ea2265d8a

=> test1

Bonus 2: Perfect secrecy achieved with RSA?

No, because the key must be changed every time the perfect password is sent, but the public key and private

key of RSA are unchanged, so it cannot be called as a perfect password.