Summer Internship in Cryptology 2018

R C Bose Centre for Cryptology and Security, Indian Statistical Institute

Solve the following **FOUR** problems and submit the solutions in the appropriate fields of the online Application Form to apply for the Summer Internship program in Cryptology (2018) organized by the R C Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata. You may refer to any academic resource for information regarding these problems, but sharing the problems on online discussion forums or blogs will lead to disqualification of your application.

The online application form is available at `www.isical.ac.in/~rcbose/internship`.

Problem 1: Expected Number of Repetitions

A bag contains 5 white balls. The following process is repeated. A ball is drawn uniformly at random from the bag (that is each of the five balls have equal probability $(= \frac{1}{5})$ of being drawn in each trial). If the color of the drawn ball is white then it is colored with black and put into the bag. If the color of the drawn ball is black then it is put into the bag without changing its color. What is the *expected* number of times (up to two decimal places) the process has to be repeated so that the bag contains only black balls.

Problem 2: Square Roots

Let $n = pq$, where $p = 13710221545914561761$ and $q = 11066328760152681859$ are both primes. Find the (two) square roots of $1 \mod n$ that are $\neq \pm 1 \mod n$. Let the square roots be $a_1 \mod n$ and $a_2 \mod n$, with $a_1, a_2 \in \{0, \ldots n-1\}$, and $a_1 > a_2$, find a_1.

Problem 3: GCD

Compute the GCD of $5^{2^{303}-1} - 1$ and $5^{2^{309}-1} - 1$.

Problem 4: Crack the Cipher

The following ciphertext has been generated by taking an English plaintext, and encrypting it using a standard Vigenere Cryptosystem. The text version of the ciphertext is at `www.isical.ac.in/~rcbose/internship/cipher.txt`.

```
ASUVRAPTQTDHVZEXXSEYGMMPVLDHGOMWILTMFOMAHSYKUDPTVPARBDTTHRUMFMZTIHXIELBWIHEVYKPPWYEXOL
MCFCEORUCEMYJSSYIVQPDXFIGCECHSJKWBIDJMPDIAPDMLRYMLSCTWPVUTSFJJEVUILPTICAPDJEHYGOEWICUXVYMA
IDIWGYQKMYWWGYMIGSUWVAAPVXIXBDIGHAUVSLKIMZDAULZTXSUGYLIGWEHINTWUVPQWBUPPWYEXYVAIMEIANFQ
CXZJLRKZTECOHRZMGXDQRQVNSILTLNIQIASUVRAPTQTDHVZTTHQEVJHZSFJJLRLQCXZUZRYEXHPDMANBWSFWLGHVS
ENJMBUQCXZJLNAPTEGURBMNGIPTSZTGUEEXIESMIQJSSHUBGCLMEXLQIVTUHZFPPVOUWGPBWEDRIRUNDYCVMAHTH
MHQRGTWGIEXEAHVNSYUXBDQCEEYXYLEXXSJLRUIIMZDEYAMPQMKXHUNDVEKRNAMACTJHVKVDXSQTCLVXXSYRXAP
XWTIFRZBUSCUZRYGDRPVMEZBACQEVZLICHQEVNSWISQFIBWTTXSQXJPAWXSYWGOMIILCLNZMCHPTJBYUTEOUGVZQD
RXQHRPBHIPCIQHAXJSULNKJTIYFPNFQCKHYXUBAPPWXMFSQUITVIRSADVCOJBYBWSDUAUVEPREJSPVUEIEUJBYUTWD
YWGOZDRPYXFPUESDIMOSMILTIOVKQHYYYUHLUTWDYMFHVPPTURGOIIHPTMPHBTWSYQFLTUXZFPNFQCKHYXUOCBE
YIMUHDTJFDPVRMPGSYPQPVILPIXELMIASURGOMSEJSSZLALLPDMZUWIIYZSLPVVMEYAVSTAILLISVWIFLBPZLAHMTIXUL
JTWEFPNFMGMYJLRDWGPORCFVUTHTIXNUKTLPIPVRMPTWQCFAIIMZDLRJICXLAINKDPREQKRVNTZPHCZPAIEVUARTIZ
IEXEGPABILDHZLAHMHUVRYQVLEKTGOMGILRWBSCIIWOPRAUTIXRVNJMILPUWBBZPHGUVFPBNJZHAVZMBIYIELPBXWE
XIJPATWESSHYATMRDSEHVRITIXULKJVDUSSNWSOYEAYLLVITIXULEXRRMLRYMLMEXARMTNXZXINCMCXSYWYPNTASY
GUOISFPURGOMISXRSSOQHZTHXHLICHZVLVZPDRZKVVZJJXLMEYRQCKDXEQVEPTZEVCSINICJLNAAIVFJWNULUVPJWUP
AWSFHYCVVILPIXNNMPROJLRUQHLPQVQUWBSCUMGPAPXLBIGVTSFJQRVKQDXQKPYVNHSFDHNULUYCOWVNVXJJYRT
UWILTDKNMBTVEXIOPOQEYWMGDIHGZBHNULQPLSONULILPDXULZTALIPVNPIRZMJBYBWIQYVFABXQPQWGYWCSXUVF
OIKIRBMZWATHEXEGKILRZVXULCCMGUVFLBWMCJIRUJXPWYSAFMPVDQKBDPTREXIRHZAMPIXFAIGWHUVRACGRTDKB
UBWIWYKUAQCXSUGBZUXGOQVXUMHWLDHVMBWEEYWAVBTRZKKUAPTCXQCUHDTHPJIPAMSQJIXRYQDYDTEERUPXE
UVNAEDVVJSBAPTKWYQCZMRSYIMFAMSSQQJNPVIVLTMBZQVRLBJEVUSIPFWCHKTTTSORKCEFJQRNUBTRYQXUHBXWD
BMTOBACMYKTLZILLDEELNGMRUVNAWGEYTGBZBHPPIWGOICJTLIZPTAMZDFHAQCGPHXNPVLEJIGNUODFLSOZBKWJL
HXULZXREYQRHVSHTIXNUKTXSQRGOMRIWUFEHBTHXKPGPJXPWYSAKWAPLHLHIJAIDFEPLBTPPIGBWMYYOTFBDUPRZ
VEEPHDRLIXNAMJRTLIEZQICWUEQHCILZHSSHAIYOOMAQWJVYQPAHBJVPIEVKBWIDYKAHTREXUJEVUILPLIEFNXVDJSO
QMRXDYRGOMJRTLIEZMPWTJANZMBICWMANWJXZVHNYSCIDIXJVPJROHIQTQAPTERLLIGWLVXRYBWIMYKOHVVWPUM
ANBWIFDMILZHIUKWGSQVLEYRTBXTZPDXUVCVLTJANZWCPJQJNPVIWTWRNSQHIGURZVZTMXFSEAICXEXEAAPTFTWF
NUOQINQYFLETECUQNKMDJDJEEZBJJQQRQZWLILHITSQBTDYRTHBDYCEVVNQCWLYHNZBGSYEQRYZXGSQVQLTAMDML
BDIHRZJMACWAZPTMAAPTTCENRJBILPIMTUIAWSEARKCCIIFIPAMSPJSSYKBTQAUVNACGIDQRQHVJRFIYNSTNTCERBBV
RIOMEILEWIYQWGYWCSXUVFAZXIOJSSPOJVPEYGDPNXSUFRZBTBABEAHBXSYMEFAPPXPBYFPDTHLHOZHBIICCELOIKIM
UIAHBLSCAMSCMGMQYIQAPPXHEYYKJTXSUJVYAIGZDJVYUPXTERBMQIWVYRQVNSECAQNABTVHXMPOQHEDKFFAICXT
QPCHZISQJLRBVXZPHWRAPPXDSMRUBXWEILNCMQIPDWRHZRLTDKSVZDZPHHRJISIDYJPVVUMCCIQAPXWOYWPVDTVJT
IFLZKIDJABUWQIWFVVGMHJZHFBAPREAJYEPVVXSUWVNVPPZVXULNXVDJWGHZHEYTTBAMCXTQPQHZZQLJXRYKDRQY
VZHBXSYIEVKPPVGQVQHAIVZDSZLZPZTBSRIEWSHQWAVBEECJSSAPTVPIINYKWXPQQPHCIMZDMANBWEEUBGYIDVOYR
NYGRPLYQFYMFYTHIREBGEZHHVUIGCPLMQLVRISUWNPLXROUTRULTREJIFAAPVPDIRKMSXZLIEPNNXSUJVULXRRIFBD
UPRLWVRLLXROUTRULTREJIFAAPVPDIRKMSIGURGOWJKSXMFAMPQDFIAABLSJUEEZLDYMBINULIVTFPRJPTGVYRTAPT
MCMSERQIMDQXVTMDJEXIHUQKICIIJLZTEWBCQVVDXVDSJHVNXSYRTHJDYERSJTICWLYHULAPMOJLRKQHGZLIEFQHPT
AIGOMUMCIXFLVIIYSIVUICILHPLJPPTEUVBMBWISYWGVZNSQJLRJWHQZIXUPAXWYEXUPVVXSQXNZBGSYEQRYARSFBHN
JBJEWBCFLMXRQQGGPBXWLBPVULXVPSXOHATHZDGUHVVIDYRGOMLEGUPRUOILDFVBKCRIORCEHLXSDYKAHTHXSUIN
YTNYYYZRYATALIHNYSPROSSYKNXPWUHJPBWNFIXUFLGSRURNULWIWYYZVVRIDJEEZNDVXUHGOMNIXYXGLLJPEHEIP
WAIEBMTOBXREEXULLPVVQVRHAQIEMIRUBWIXJLNACAXCQZVVTTXWYKUAKWEYWIFAPTIYUVTFAXKYQXHYMDJSOHE
VOTRLJSZZJDAXQRFHQSEDJVBUWBICIPBVSTHLJEFWMRMQYGJHDTPPDKGOQUXSUVRDMGIDJEEZICHFBXEHDXSWUXYP
OWXEXILDWJPOIIRVVTWTWRNACGITVXULZTAPHIAVAIECIXULGLSFBHFLMPRZJLRYBWIJIEJHKAILHFHANPMYJWVNVPP
DXSJPVVXSUVRDMGIDJEEZXGSMQFYFUPRJEJGOMBFZMQNUAPMOVMAKQCKEXEGAZPGPIMTUIAALIRBAMPWJRIPHCHIE
XIZPTZCHQCTHTPBJQPBUMQSZCWJPBWVLTMBDIKIYEMFLBTREXSHZICHEYQRZTDYOUVFHQSTPJIERCGGKORFRQPHGQ
RPLLEVZWVNTBTGSDSYVONHTHIPAWGJZHXULVPXTERNSARMPDGRMWJROQXVVVLLTSLULTEIOVYAKBWICUWRHZRLQ
YRQPVVXSUMZWIRXZVXULNXVDJWGHZHMYJLNAKPGZFLBUGLSFBHOLTXOPJVLPVVXZXINYBWIQBECVNPLFCQVUOQMC
TWJPVVJCEQVUAXHPQLHYZXGLDIXBZRDJDWXPAPMOYRNUVHJGYHRVJTGLKWRAPTLTWLRULDJEXISYMFYPDGLAPTC
HUVRSWDOTDKVUQHXSUWNTMPWQCVNKQDXSUEFAZDRZCIEZPPHEEKBAWILPQYFAZPPTQRQLATVEJSRZKPTPYRGLZUI
```

CURPLBWEEMEFDPTVPJLRFQCWEQPYLLILPYVNUBTRYQWGOMNXSURYHJDVPTXBJWCJTHQJOIIXSUCSVCCHTDTNYBQCEUWGPVVMEQKNPVHXOKQZFAXKYQPFPVILPBEOHVSMEQPYZPDAPTXUHBLLLJXULGHTZJXRKEPWEXIREQHXPDGRVNILPVMEZBHXLHWOVEBEYIEVK

Problem: Find out the KEY that has been used for encryption, and input the key in the form.