Summer Internship in Cryptology 2019

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

Solve the following problems and submit the solutions in the appropriate fields of the online Application Form to apply for the Summer Internship program in Cryptology (2019) 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.

Please keep a soft copy (scanned image, doc, or pdf file) of your detailed solution / calculation readily available. If selected for the second round you may be asked to submit it. Your detailed solution / calculation should contain the essential steps to solve the problem also it should contain your name and the name of your institute. It is your responsibility to maintain sufficient clarity, legibility, and authenticity of your solution.

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

Problem 1: Bags and Balls

Alice and Bob play an interactive game as follows. Alice is given 5 empty bags and an unlimited supply of balls of 6 different colors. Then they execute the following steps sequentially:

(i) Bob selects a number $b \in \{3, 4\}$ and tells it to Alice,

(ii) Alice fills the five bags with balls and shows the bags to Bob,

(iii) Bob selects b distinct colors and tells it to Alice.

(iv) Alice wins if she can provide Bob with b balls of the colors chosen by Bob in step (iii) by picking **at most** one ball from each of the five bags.

Let n_b be the **minimum** number of balls that Alice needs to put in the bags in step (ii) such that she wins for **any choice** of b colors made by Bob in step (iii).

(a) Find n_3.

(b) Find n_4.

Please note the following:
The "minimum" in the above questions refers to the minimum of the total number of balls in all the five bags. For example, if Bob selects $b = 3$, then Alice can put one ball of each of the six colors into each of the five bags, that is, she puts a total of $6 \times 5 = 30$ balls into the five bags. Then for any choice of 3 colors by Bob, Alice wins. However, this is certainly not the minimum possible, as Alice can do better; she can remove any one ball from (any) one of the five bags and

again she wins (for any choice of 3 *colors by Bob) with less number of balls which is* $30-1=29$ *in this case. Therefore, clearly* $n_3 \leq 29$.

Problem 2: Tails and (Heads or Tails?)

Alice and Bob play a coin-tossing game. A fair coin (that is a coin with equal probability of landing heads and tails) is tossed repeatedly until one of the following happens.

1. The coin lands 'tails-tails' (that is, a tails is immediately followed by a tails) for the first time. In this case Alice wins.
2. The coin lands 'tails-heads' (that is, a tails is immediately followed by a heads) for the first time. In this case Bob wins.

Who has more probability of winning the game?

Problem 3: GCD

Let (a, b) denote the greatest common divisor (gcd) of the numbers a and b. Let

$$X = ((61^{610}+1, 61^{671}-1)^{671}+1, (61^{610}+1, 61^{671}-1)^{610}-1).$$

(a) Find X mod 10.

(b) What is the minimum number of bits required to represent X?

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/cipher2019.txt`.

FBHJLZINOHBYTYCNCZLUYZUFIGDMZMYKVQDSPUEFJIGJPOQUFQDRJQJNTVDREXXJEOQGDUUWFWGOXQQHKJLUWFDY
CMFRZTUIKVHHZPATEHKKLHUTWRLTZTQZIGEOCEIFISWNPPDQPAHSMFHXFTWNPEYSFTDSTMOYISHZSBJXLFYOGFTYY
SRXOFQQRBGZSFEUVBQONIUXCSIZMFXNERJGGFJMVADTOPKWVOURJNQRDOOGYDUXKCUYEIUNIHLSPJDYYSHIZMELZQ
DRDQEYCWJNECKYNVDZTGSFCOPOEZXFUBWHPGQQCSQZSFTNECVGFSIBFIOJEIUDJHLRWIQAVURTPPKYECWCTUXFSO
QMMVJFNVLSAFHRRMEKYPJFTQRXOJDLKCDTPXIYLRBZSBJXRMVJTOEXRIUYDUYQCVDJAMUSKMRLGJCFERYORPHQVO
GOYHKUKCWNPNQXJSAZTOSYZCQGEUXJVBGUQUXJTFHZLDUTLGSKCJEIISYKLMUILGLTRIKLVGLSFMQYZCQYEIQYRFHT
PXJTGOOKZOJTCCJEEIUKZBGOYHCFIYVZSFBFKSVZEVHSZBDJPCQYVCYKCXXJKVHXOJDTJOXXDXUWVOOXPBTDZBWKC
NYSRZGKNMYSVPBZSFJNDSGUZNIIRMVZCVSPZBDJOJJNFBWNPTJZUMVIFUJNEUHJRFQUGFRGNISTLZGNPMFZJPHZEFHQ
FCNHLDAFKDDYEFDAZFRTXFDYRZWACNENCOQJWFQWEWQLTOUWUSWGTMMMRHZKXJWMKSAVPDJKICPSZEUWEQOO
XBJJTVDTRFVTIAHGYEVTIOOUEPVUVCSRPUXFKKLYSUXNJHKKEFQRYOVKYEUIWCUSPBTJTWVOZOCFUSLZDFURVRDYT
GXJYOGHPFDUCOBOYHMNKVXYLMBMZGOOQFYKVSOYZSHDWCUZSPIJNVRCLOJYFQRSAFJJWCUSPTINJHKXZOUNKGLSA
PIXZPOKEIYXBWGODVDNHIHSPTINZGDTLMYJEHKGEEUIZQDZPTXNDGHRQUEUCOBOYHMNKVKAXBDXZVDBPGKSCWNK
LDXNCRLTEIUXKFHKEXXJEHKKOBOHFAHYHIUSZAQUEFDOFMLTRJJNNWORWFQAVTRUECQQCAHYDJYXKVHHPTJUCOB
KCJDYYSZUCMTGPGRSPEYXKOQIPIUXCWNKLQBFPGWGEJESYSFGYUQPVOGBLOJFXSRLPWUWPALYEBAJNSPGVFJMRHL

YXFQSUAHYDJMJISUORIJZGHKKCFQGJCOAEFBDCSWSPFCGIOFKEIUJJCXXLELJIGLZJGEWNWVKXFDXRMLZTTJMVKLYP
TJHFIUYPJWSFFDTNFYXKVHIFSIJFTJUOLDTNZHJRFYXKVHCTOWBYSUKHJJMNSIRJUEMVOYKYUXNJZLLPXXNTVKGOCU
JEHKKEPCGFTKODWYWKIHGYEEKYWVNZOEZIWVHFUQBRZNOYHIMRRRCLQETIDOGJFHYYOWYESKYJOQJQSUYJVLYSP
KWLDRTEIUXKOJKLOTYYSQODIUFIRQUXPHJZHLYLUQQVHRROCOFEWGOZUVZCZRLDPKSUOQJQVHDJWJTTGONEUQUEI
YSXOIZPSJMVPLMMBDLZHZGDDEQUOQJMMQHBOQJEIUSKVHXPXQXCWJNEOEBWCUZSFVNIGWZTNUFJHUUYPCJIGKGGF
WQZASYPEJMRHGGHOEKKVHAYJLJIGHZSJHYVSQHTMBNFBBKLSIFXCZNPOJMVSDXWJUXKGWGCTMJISWACOYSXCQZSF
BNXVWOYUXJTCVSTDTFIYQKDTQSUWIZSBJNJBRZPOEZXVWNPZCFPVDBPEUYVQWKONOXKSUOZVIIRFNSLUJJIOWCZSA
YFCWNPHBNDDVKNPDXZGWKOPVFWOLTESQIZCVOROQQWFRSOFUUJDDIPQYHBSGAACOFEOQZPODFKVDZTTIQZUKZWZ
RNXUHXEIQSRFHLCJWJIOWUCBDITCVZDMUXJHKGYGYAVALRWJESSIWOYDUWKOLTHBOXTOQMZCQHBAXISGQWKVHXT
OJNDSDTOEYXKOQIPUXFEHKKNFBJSFDZPECZCHLHTMBNFBGUWMQWYIEHWFIURQHZPMUXTCSKUVTISCZSLOEKRFLFZO
QXKOWKFOYAVFVOEZBJRRDAEIEWFTDYEVTDZBMUFSDFCBDZFSUXRWGZSFINXBDRNBCJWFRSEIUAVFBLTSIYFPMKNUI
NEHKKFOYAVFVKLTYYNOVKXFHLZBJUFUEKUOUQYFIXKKRNFOTWVRPOWMYTEMHGCTQKKSUZSFRNXPDTRTUJZBJZSF
KSZJHXDFZZJHOORIJNEUXVPWUSKVRARIYYNOVUYMOFWOLTETYLEOOODFLJEARXPJCUFFWGYUJMRBWNPCYLSOQMM
FSFLGHCPBHJDOGKZGIYRFVZFGVFERVUHFQWVUOOXQINEUDZZVHTIWJOYTQNUOVZCPDTDSUXTDXFIRHRWJIBYCZGDO
EYZBYUWWUIZBWNPQHTASFZEIUXZUQGWTXTNSGAYFNUVQWKOMOHFZGZPNFJIOWACFIFERDTFOKXLOORJQHTECXTN
FTBRJHCSFDFJHUUYPCJIGWXTFTYFTLMFSUTLHZNJUXJSSVZPYFQRBDZTPDBRGWNLUUQLGLBPEQWBADZEFHRRMKGG
FRJVBDZHPHPZTYKCJVNVRWNLUMTLZGHPUXJWWUYEDESWWUSLUYTECIOETANERRLOBHPDOWZPSMMZQKODBIZSGW
GYUYFCDDXEPVYYSXTTWUWJSWNLUIHZSQZTTJXYOYKMFUSJSDXNIYSXTRXZWUWUSFGOFINWQRTQJHRVRWNTTTNJQ
RBPSOIVGHXGFIYNCQUMFBUIWCKDGEWSCWNNBFYLFLTRUXJJWJTLMEKKVHLTSIYJHDXDBDIGCWKYUYFCRDXVNQYKS
UIZOVNIADZTPDXRWGNLSLFIRDYESESFAHXLWYQFSECSPMFJBRZABHYFTWNPSUXVOUISUUFDQDAEJESZBJZSBJJOHUGZ
STNEOUENMQNDGUKBVYWVSAZCBEWUWQGCZUAZRHTNFXJJOLJTOTJGSQJPOJYVGWYLSUSVSGKOUEAVFLLJUXJWWQJ
TOWXSCZSLOQLISHJTOTJGSQJPOJYVGWYLSUSVSGKOFLJEHKUFHXMZGWKLNIUVBWZHPOJRFVJZVRQVOQJESYUCSFNPD
ANEUWNPJHBFFNOEJIFKWPKZGJMVIQOGFHXVKHXPBBQPRRTZUASFKDTJUXNEUDHZVJGFKPGYTQNUVHYLJTYYSGODD
EAVFBODMYPVHKKQJHXKGHTEFDHVWQGYFQWCMFNLQJJICIZSFXNJHRXJPVYYSFUDNEXKVLYTTDTKVLTRUXFKOVZC
PDTDSUYNPKQUOFZFBBQPGHKTOVFTHLZTTQQCWQJTSUHKPDYPEESTVDTRFINEHKKHBLJCSQMEIIUICGANFTGPFDJTPI
NXBDRDUXJVOURJVDNMSUYPXQXUOUQLOTHFZGLTMBJUKLZSKKXKVBJCPWJEOQJSFBNLARTNFIYRFVLZSCJUHKKJFCN
KHHJFMJWRJLUWFJQZUKZTOJTKVHJLSAFISDYMFJBVSQZSFCYYOWAWUHFMWRRPUBNXVWISBDLVGWNPFDJIUBYTHDF
KIUKZGXDUFRMPOQYFAVHZXCFEGDOOBIYICQUXFHXCCRQPEQYRGSKNJVNTKDBPMUSXHKOQUXJISZKCFIYRFVGYEKQ
KFDBTPBJKZLMSUJMVMZUFMTXVSRTPTYLEOWACFYKKVHXPXUWVBRYEBHXKVHEHPKQUGHKLOEYYSUZSFOXRKDIWF
QWSIWLLJDYJWJTLMIMFKLTRUXJISZKCFIYRFVVCPRFSZBSLOOTWHKKXCEBDOQYLJTKZBGOYHJMRHWXLDUXZUQGWX
QXECWKLTOGVQDADFJMVALRVZMFPUDRLYOFCCQKMPERJKLZSSQIZCZGGFDTZGHZPOJMFIVGYEJNDSVRZVTJIGDOOQU
YVFNACDPDEGNOLELFEQHJASELIOPZPDXSFZRMJEYWVQWUCGEWKVHTLUYTEOOYNJUSTSIUFOTFKWRTHIYHYVHRAFT
KLBGZSFHJJSDXNIVNERLTRUXJZASGNUEKKVHLTSIYJHDXDJDYYOWILDEUYCQEHPKQUPHRTLUYIMLTRUEMVOUZSFVQR
DRLLIKRDWQMMJHIJKLTRGHTDWQYTEUFYIUXTDQSVYXXNAOSJYLYLJTNEOQTDGLNUSRHPDQZJSWNPIYLYSQJZGJMVT
UKBVUSTMWNPZMJISOUZLYSXWQODUXJJOPKLTVRIOGOZUXJRGWXZOERVFVNLEJTXCWUEIUFLGWXLMYFERHYPSJYFS
VILQUNEHHXQFHJEQHZSBJBRGZNPSUYYSBOYTJFCZHJEIUNIOQZPODFJHKKJUXJEZDHZSUIKCFUYGYWDKKGEUXJPTRAY
EYSGOUZMZJJJHLTRJJFXOLTDUTZDABYTHDFCGLTEIUQRPDTOJJFCZVNZXUIKVDZHIQYKVHEDQEYKSGCLTJMVSAODUU
STSRLEIUKZFVZDUQWJPRCXBDXRWG

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