Summer Internship in Cryptology 2017

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 (2017) 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

Background: Let there be N identical packs of playing cards, with 52 cards in each pack. Suppose that one card is drawn from each pack, uniformly at random, and independent of one another. At the end of the process, we have a collection of N cards drawn from the packs.

Problem: Find the minimum value of N such that the probability of finding two identical cards in the collection of N cards thus drawn is more than 0.5, and submit this value of N in the form.

Problem 2

Background: Given $r \in \mathbb{Z}$ and $(m_1, m_2, \ldots, m_n) \in \mathbb{Z}^n$, for $n \geq 0$, define H as follows:

$$\begin{aligned} H(r) &= 0 \\ H(r, m_1) &= m_1 \\ H(r, m_1, m_2) &= m_1 r + m_2 \\ H(r, m_1, m_2, m_3) &= (m_1 + r)(m_2 + r) + m_3 \\ H(r, m_1, m_2, \ldots, m_n) &= H(r, m_1, m_2, \ldots, m_{t-1})(m_t + r) + H(r, m_{t+1}, m_{t+2}, \ldots, m_n) \\ &\quad \text{where } t \in \{2^2, 2^3, 2^4, \ldots\} \text{ and } t \leq n < 2t. \end{aligned}$$

Let M_n be the total number of multiplications and A_n be the total number of additions required to compute $H(r, m_1, m_2, \ldots, m_n)$, where H follows the recursive definition, as mentioned above.

Problem 2A: Find $M_{20172017}$, and submit only the numeric value in the form.

Problem 2B: Find $A_{20172017}$, and submit only the numeric value in the form.

Problem 3

Background: We associate a n-bit binary string $A = (a_{n-1}a_{n-2}\cdots a_2a_1a_0)$, with the polynomial $A(x) = \sum_{i=0}^{n-1} a_i x^i$, where the coefficients of $A(x)$, that is, a_i for $i = 0, 1, \ldots, n-1$, come from the set $\{0, 1\}$. Given a string A, we denote the polynomial representation of A as $\mathsf{polyRep(A)}$. Similarly, given a polynomial $A(x)$ with coefficients in $\{0, 1\}$, we denote the string representation of the polynomial $A(x)$ as $\mathsf{stringRep}(A(x))$. For example,

$$\mathsf{polyRep}(1000011) = x^6 + x + 1 \qquad \text{and} \qquad \mathsf{stringRep}(x^9 + x^2 + 1) = 1000000101.$$

Given two n-bit strings A, B and an $n+1$ bit string P, we define the P-product of A and B as

$$\mathsf{Prod}_P(A, B) = \mathsf{stringRep}\ (\ \mathsf{polyRep}(A) \star \mathsf{polyRep}(B) \mod \mathsf{polyRep}(P)\ ),$$

where the multiplication $\mathsf{polyRep}(A) \star \mathsf{polyRep}(B)$ denotes ordinary polynomial multiplication between $A(x)$ and $B(x)$, but the coefficients are added and multiplied modulo 2, and the modulo operation with $\mathsf{polyRep}(P)$ is also computed with coefficients added and multiplied modulo 2.

Note that it is natural to extend the multiplication defined above to P-exponentiation as follows:

$$\mathsf{Exp}_P(A, k) = \mathsf{stringRep}\ (\ \mathsf{polyRep}(A)^k \mod \mathsf{polyRep}(P)\ ).$$

Problem: Compute $\mathsf{Exp}_P(A, k)$ and submit the answer as a binary string in the form, where

$P =$ 10000000000000000000000000000000000000000000000000000000000000000000000
000000000000001000000000000001

$A =$ 00001000110101100111001110110010010011010001001000111110111100010100010
00101111101101010000100110010

$k = 2017$

The text version of the paramters is at `www.isical.ac.in/~rcbose/internship/power.txt`.

Problem 4

Background: The following ciphertext has been generated by taking an English plaintext, and encrypting it using a standard Classical Cryptosystem (ref: any standard text on Cryptography).

The text version of the ciphertext is at `www.isical.ac.in/~rcbose/internship/cipher.txt`.

```
AMWTALAMDWKMOYBAFMUALPALBZXEQJKMOYBAFMUALPALBZXIIWGYWBAVHUKLOTSMPWTOGGXY
OHTALPPWKLIMESLBJWWIOVPGYJGDAXFBBOTAVZWXPHKZHNKFUKEWCDBBAALPALBZXAGSKHNH
NDBOJLAMWTALAMUWSLOGWXWITCFXSLQLPIULZXSIZAGOQXZHPXQLPIULZXWBVLXZQXVXSIIA
KEGZSWEOMJRBJAFZBXNGKMWKOXHTLFHBJAFZBXNGKMWKOXWXZWTTNYGBNZLAKMELLHHXINXV
YWOXRXIDEOQAFZDBZWVBVZWHTAMJPIAAFLHHZLMPGHWKIHLOTAUGXTREQCXBJWHKELMFMXGJ
AHDMPSMAQEWHFBBKGWKKAXSMIMMPQJAMIXAAGAKKLXDHVAMADWAGGKMUXQXWVYOKOGHLQJXH
RXDAEQPLZXSNXWKTCLAOEWMYKMGGXVOFXSKQUGFHNEGLAMTWOXRXICBVIOAMHTTSKOGBSPAG
LSJCGWFPIMPSITCAFYAVMGGBJWLARHVWHNGFYEAGLLAMTWOXRXICBVIOAMHTTSKOGBSPAGLS
JCGWFPIMPSYIKJXTCXWFMPGLZKOGMGYNTSFVEBVTHBJUGNNMZAXAKLOTSVTWTZGJLAAGKJRA
VSDMOMPWEWTVKHFMPWLBCLWIRXAWKDGKGYLHINXACFVYILPWLBJSLMHBVYLQPYWGEKIDPMTW
KXTMTWWNQJWOEKQLPIULZXYXIJHNQMJEOKLGGMVZGNSTVVLMXWFAUGLJXLCFVLEOMFMGHANX
```

SIQJBBWSDKEOMDTBKGFLWXZWVWPUWWEWBGXVIDSGDTBLAIVXSOONZWWXGJAHDTASMBJAKFRL
AGNBJUGMTAIVKMEWFMLRILMIKFWWHXZXBDGSFWTPMFMQGLZULXAKXLDAJMHWIQHNYZGFAIZG
IPGLAVPKQNTBGAFMHXTAYMIMSKDLPSWPGJSEDXLLAMUMTEIFMSIXGSJTNVMTRIPFGNNVQFZB
JSLTRKIFZMOWFMSPMJXUCVWYOKBZXAYSDEOPQFZCRGXEOGLGGIPVOXSMUAGAVWJXVXVLAMEG
UDLTVWZPQKLAAWJWXVNSAWOGTQTZQMFWDHHWGWHQWTRLIXMMTJSIPBVYHCVALLMXAKTOGKSL
TAMKIQTALLOYBZBAXWJRYXIJEIULHTSMAMIMTFSMUKIDEGFWXBCBMFMQPGJBGBVSEQVQJTPI
MVHCVLZXIKAEXZGEWLSTOWLQPLZXETZLATAGJWEKWXXDGFLLHTLDTBGDQVOFMLHBJWWGGEQK
AKTGOGAGLHXWRDWYRHUSVWPYJXSLWXUZKLALHLCTCMELKBNTUWKQESOAIVPKMZCFYXTHZWEI
VWZTVXXJHDGVEHRXQEIWTLSGTMWLAMJMETNKIUXBJSFTNRKGFUWFAVAMQGGAAWLKEVMAOMFL
ZKONOZTVAGXMHXKZBKMWFLOYBZXKQUCEAGMTKWQVXKAGKWEMUKXTVHCJXLQFLAEPPGEMCKLH
MTBLXZUKHBRBBMTTVZSGHXZKBAVWJHFMPWLPKWDWAGLLKQFWFMRHTDXLYALAEQKWXLKFYLMH
WLAVGKKWOPVZBTNESDIGOHTXGJEHNXGSGLUHWGDBVYBBWFVXRMPWZCKVSGCXWXAMTUZKILBA
TVRSKMOKAKAMGFLXRMIAGMFZWKSXTXUMUAVXSPQLAAWUZAUFIFXIEZAXVXUWGBUSKLEGBWGK
KFYTYHCLABQZSOEAQKAIPVKVUMWXYPKKLHNZCWMWTFGNTPQLAXKFUXRLIFWPKKTHDRJMKVGV
SEIOMTXKCMKXHXPSWVQLCGEXTWWLQOFBNMPWKIKFLHDHPGGWWJLHAWQJMGRJGVELAAHVQXEH
NDAOAQEZHTSLMVPQVZAGHBANBMYSLTDBALTVEWGYSHUWYQHLQHRLQPMGASJWSBBALTKCWEYX
VGNOJLZTTKWGMMFAFMHXEGHLUGXYRTVUXIPVFHRPIQMPGJWPEKMYKWYAFZTKMWLEJWFMHTBK
NNHWJXRPIKICVLGWETBZTTTWSWYFIJDMFTQMHXEGHLOSFYAMMLHKQEWWOPVSGLDWKTWGQFMW
DGSKDLBGFIMWSVEKBSBVOGNTBEMXKIOWOHRDEAMPCKSVKTVVTSPAXXIGQLMMTJAULXQFAQUL
GKYBBALTKCWEYXVGNOJLZTTBVLAMTGMZHHCLAWWKWLOYAGFMVADEEKAGYBJWZXAOGDTVFKSW
JTKWGBVGHTRBALAMTWOXRXAZXTVWJXDYZGFBJWOXAMPWKBJSLOEKGVTGTMVXCTZLLJGKHTTM
MJXLYALARNALBKOAJXSGCXYMFSTHUMJQIQIKSGDKWGLBGVAGBRXGNTVJQPHBKZMPGXSKMXZV
XIVZZTDTTJXIFQKXTTXSKBVGTXHBALNUDJAESHNLAMTWNHLNBAHVDMLMHTBOHWFESGAGLLAI
VXSKMXZLAWWYZMHXGOHZMMFVETAAGONQOHRDAAEMPLDRAGLFHWPWZXAKLLAMOSKMHXGOXVVS
THUMEAMPOMXYLXLLKMCVLAEKILAMTXGKALUMVPCKLHEGBWKBCAFTNRAMLXKUAHNMPSMBJWQP
EKMSPIMWOTSMWTXIVZWBSMQUTTCFVMRTQLHZQMKBNXVYEIPVLAEKMOTAUUSKCXTQTVCEGNNM
WXHZFWJTNWXJHBGULBOGBGCCULAYYFCUAVCLAHNTTTHIULAGGWIJBVITMKGEIJBMUTQTRFMV
FMPSFWHBOZPIAJGUBXZAXAVGGDPEIUXQPLZXCTXAMINALLEENWOMTQFBGABXTUKDAXSPMJXX
WTDBCEGUTCVAGGEWVGMBQYGHUMWXMWYFOBTAWMMZGEGOIGOLAMKJXNRGQLNZGLGNPAWDLBGJ
WKSPIJXPQMKXSYWJLMEMJBTRBZXPKYZPARUSGQPLZXDTZCPIUSUBTRBJTLGKETNBVLAMNAYA
TTVVUMKFYKEVWYGQUWVTNWKZTTNWFZEWJQAQUXWELHELKIFWKFAGEZHUJWKMOIXWWQPZALCA
IJTKVWJHFMPWVIRLSBNZIDEIPLDRSAWLAQOLZKONOZMPGZWTDTVVKWFWSPARBZXUCADPALES
RTCAVUYLMNXVTGTUEKASGLVZWZUTZVLPQLLARXMVXIFSFWTAMFZWVKZHTWMSWPKEKXLYJQMP
GGLAEKNGNZKFUHNLMINMPUWHFMPWYIKDMKEHNZBACEENNBBAHVCXLXRPPAVPVZWFABTOTATG
TUEWQFIMCUWMHTBETOPAXBCXVLIWVWFMAMMLAMNGJWMTGGKWHDGGDHVOTAOSVXTHALTVFSFW
DXTAOMTGFMUKVZTUIJWXNUGGGMJAYAWTGETVYZGWELXGBTGVLAEBTDNAVJAHULKJXIVMJXIG
AAZPVGXTLEPALZGLAGUXXJBAQFWKSBVDHVFGFZAHTKYWWYZMBTBLEMUOAMHMPWBZVMJGKXGK
TVFLZXMTRWLBAGXMHXTSPNKJWWBECFWMTTMLSXAAGIOGFZTAMEEWCVWWWBBZKWWFVLOYAZHB
CFVUAETLAQGNWLSGQHIMFGXYDBIEHVFUJHSLMKYZQELAEGMUDAQXFHBEMDHZFKSMCHCJMLTS
OBNZZGHUUEMLKXBWXZUOWGTBVLHAVYAEELALHAGSJVHYWJVWPLJTBTVVZWQVKTNWBZXUQTXB
RXLGGBJWENSDMLXMTKSGDMPWFCUCWMEXZKYQTWVHNMPWFWDSFWNHJGWGVZGNGABSGGQXLAEL
MGVKWJJXNVMKFCEZGNTHNLAMEGEFOGESRQPLZXMBLKMWHLZXMMPWAIPYETNXDWKJWKQTNWMN
XZYGJLEMPSGCUWDXSLESLQPUGGSMIFMZGIMBSBBAHVPGOLTKQFZQPYMILHVYKWYKGYMBAUXT
NSFXONAUKQOAFTLLVGPPCFYBNZIZHCUWTKETSWKWPKSMUKLSREJGZTDUMWGBCCWGOGBMXAFS
QGOPJMKVKFYIEHXDXQPLZXHTVVTBPWOZAMMTRBJWVHZXVSGLPGOUUKVAGORSEIHEMLLIVLZX
DHWJHNYWKMMBVKMMTZSELMWVTGVSCBNZBZXTKXWHFTVSMZQUAHULUMKLGJWKAGLLHUQJJHWH
NSPZGLUAEWXAENGJWKWAWZTLTGTUEWIXTZOWJLBHGGYAKPHXNVMSETVZWLEMPAGOUSFWAMPG
NACFVEIDMLAMOUSFEMWHTAUAFTNWKDHAGMHHNMPWWMCJGEDRMSKWPWLAONASGLUWNXNACFWZ
GVSGDLMNXVVQXBVXMFOQTGFXDUGLAMOOZBLXBZXEQGVFAGIFWBJWXTRFMJPWTCWWUGPWXLGV
LAOLMLPWQXLAEEIJZMLSOLAGLLAWUWGMHXZLPWQXLAEITSBVCFVMHXNSBZHSUXSMZGWEKLZL
TBZWGWWYZTNWKSKZKWVMHXQJWQXAFXRBOZMAYALAAAQYAPCFVMHNAVBLVZWRETZGGMVZGNST
VVLMXWFAUGLJXLCFVLEOMFMGHANXCHVVNKVLZXIKOJXIVFWLSTVVFGTASWSHNKFINDUKETBM
KMULZXCKMSMCTWKHFMPALKJJGGIVTWTUQFYMHXZWLBCDGGGMPWKWCVKMHTBDTGDWXHRXBZXU

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