Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

WS 2018/19
9. Jan. 2019

Preisaufgabe

für die Hörer der Vorlesung Kryptographie

9A4047D51ACB 17B13864A438 68E1B9315BB9 6E9169F77910 0C92085BAD2A 0D39C38F3ADE
1DC8F5E810B0 3C08349CE4B7 2650A0C1C672 0CB0A3476F83 5E78E6FE5841 44A4F1314F2A
57AA9E4F25E3 CD587E736E5C 66172DD8E581 54F309D674A6 BC65D84BDA80 C6A034EB2C85
C82C7D8C941C 5AB1C2298E3D 1CA7333EEAF8 DDB1318420EB BDC09E03745F 66C1788692EA
F934B569BF69 8F608557103D 248226B93C2B 293A6B1E0719 08F1CAAA452A 55A539569D7D
2F5E2347EB4A 2D6240A48991 5EEF7CE182B0 3D95BA67E2F4 CD6E9D691D88 4E36C2783DB0
6042618D78EE 1BD50480CB4C 761F821F80D0 5536D4EB1BCE 331E31C2F33D 70DA1589D27C
9EBEC203D636 2FE26B361400 98AA5301022C 98DDE5DE99B6 4FF00EF5A01B 7C83007DDF7E
41313D82E523 6258AD44180F 47134217C26F 0B053407D430 4223254432F8 D616092003EC
D694FCB5340A DDB283A72270 2BA514A87965 48A0BB20DAEC 0BB9B45CE914 1CCA4D3B66AB
E8F1948E5A79 24DF652D95EC 9BDCD8947FB8 F719B821F398 19EBFA9BB15C 0ED06CFD7931
E8F31A74AD67 B7F5B80AD8C9 6A14ECC67607 0ED4216883E6 BD6F96BEF249 EB51CB3254D9
38379633919B E34844E76BE8 CF8B37FF9D5C 3F75F7C72C31 90D1C1C13FEA 33AA6FF70C71
41F9A6572D92 7C995435F723 C21214D5F979 0D6AF4B39751 5267A615BAAD 69C121F18B65
131861B50118 0D25FE6B6462 6C8463352F1B D85AB28E603E C8FEA2FF1C03 7B4CA47C7154
A5D55BCC9726 E11B2B1DFCA1 743F4EA1400E D8089844BB3C 73AF386CFCBF 3650AD6ED462
B1300C4D9405 47B4651D2997 8872DC0884FC FB11E2364D36 8AF7A26858A0 98DA3A0C9DA2
53788C4B7EA3 B1521449E5F6 7E0D3F5AABCA 442EA5C45679 652A156A4E79 D1E4D756F50B
DD69E3B927D8 57D3868DBA3F EF77D7E4620C B7B14E4AB1D2 2883320DEE33 2BFAACD1F837
8926BFFCD09A 0774582BC76D D5A8EDF866FD 7CBF7B8666D1 4B0B3A2D8963 F82024293C6D
041C544DBF87 AA462A1CA93E 1AC973231C25 40EA18277E14 BC95C359F96A F1D0BA2E80EA
75FFF6DA2F9E 7115880B7FDB 7F3CF17B5F67 907EE81AC841 CCD5487307C7 19C5845E73D3
AE1CDF215A79 D5E47973CA10 C7CD609FF1CC 09CF2328E520 643240D48C56 445627919CF5
C29EA15CFD5C EEE54F7EDA41 67C36E0C6023 86F277735CFE 4303014B075A 5EC46F0B590D
29B048290863 4136E4CB5908 6E02E6989EFA A82E00DFB69C F43D6C68B10B B161750EACB0
378FF119B4FA 59B04007825C 736FEAEEA49A 860E7C218678 2BDBFCD993E7 B655FFA21EB5
37BC9E14E3F4 DD905A0F916C F97E2BA9FC52 60AF62A6BBB0 09D8C36C01A4 D37A570FDC2C
7B86E0FC73DE 80CD62A54B94 3245D87B3D8A 2290D5EE0610 FE7BA9C2902F FFC8412366F3
C135318D98C7 C93EE376F96F F958785DB7B6 1F209867CD54 29F166C25B5A D4B5790B27F4
E796545833A8 15EEEC25C92E FF9D6D10563C F6220D487BAC 4534776CCB6B 323F1DD254FC
9A2F33D3EEEB F417406047ED 667E11F6815C D1D820E40D32 5CFBA6742A57 A35808D40FD1
59B47D72AB6C 7AE4A1364AAF 3D9563B3300D 5C9B024DF427 1E33869F72D3 0086FBED5BE2
1140348CB2A1 294AE9C1C67A 49F5AE4573DA 4D63E1E7530F 45A0EC654136 12A7D1452EE0
CB4D2A627D13 241C68D4EE83 50BD1ADC6EE8 A178D84CD5C3 E8A828F86A85 F62B2994D509
5CBDC0288E25 4EF9762DF6EF D0F5658F2DAA B2CA8D0A3A47 29DD6D86A3E7 F527E769FA2F
836C824C423B 2CC572B0356C 36206D1E001A 57F687B54431 05AB38179D7C 25106042F84C
202C5DBBD0D8 45BC7CE8D2A7 36CCB963ECF0 DA2F9A680083 4E31C97923B8 745F71947EBA
02C812D39C44 741782198093 5E3BD7FC1FD4 351F3F

---

b.w.

Aufgabe

Der umseitige Geheimtext (Bytefolge der Länge $L = 1353$ Bytes in hexadezimaler Schreibweise) wurde von Alice aus einem englischen ASCII-Klartext Länge L durch bitweises XOR mit einem Pseudo-OTP gewonnen. Der Pseudo-Random-Generator zur Herstellung des OTP's war jedoch defekt, so dass sich für das OTP eine periodische Bytefolge mit Periode $N < L$ ergab.

Man bestimme N sowie einen möglichst großen Teil des Klartextes.

Lösungen sind, zusammen mit einer kurzen Beschreibung des Lösungsweges, per Email möglichst bald, aber spätestens bis Freitag, 8. Feb. 2019, 12:00 Uhr, zu senden an

`forster@math.lmu.de`

Die besten und schnellsten Lösungen werden mit einem Notenbonus von 0.3 bis 0.7 auf die Klausur-Note honoriert.

Viel Erfolg beim Entschlüsseln!

Otto Forster