Secure Communications & Cryptography

One Time Pad?

OLLSCOIL TEICNEOLAÍOCHTA
BHAILE ÁTHA CLIATH
TU DUBLIN
TECHNOLOGICAL
UNIVERSITY DUBLIN

Many Time Pad

Let us see what goes wrong when a stream cipher key is used more than once. Below are 13 hex-encoded cihertexts that are the result of encrypting plaintexts with a stream cipher, all with the same cipher key. Your goal is to decrypt the ciphertexts, and submit the final secret message within it as your solution.

Message 1:

0f381a39fe6f41bd57c44646eacc3ecb2b695ae729ee174ac650ab0c92547a73b19ca7a2
4d40162bea9c0d1c2c1395678f6dec2ae8b4eaa449b1511507c3e06dd6c9c02c69c5eca4
241d3f3585f44440ad011078381bacc075e4c3

Message 2:

0f351c71d96e59b742c34053a6853d9930664da237f24456874ae61198546b7ea6c8f7a3
4b581823ead8490c29568e618b68a929f3e6e6ea0ca35f1944c2ec70d686df3028c4f9a42
a0720748cbb4e41a74c07773213bad56eefde922d44cdbcbf3e008be80870a5eb7c55ab9
07f18fcf347dd433bcf83432d0849e80c22b0

Message 3:

127d183cb07342a042d40553e9cc3dd83d2e5cea3be91756cf46f904d74f6c3fbcd3b8f04f
431c27af8842003147c27a9425b82fe2e6f8ed5fb2540e05c9ee23d681cc3d28c7f6e2275
22466c2fe555aa34f116d7b1fb58168f4d8d72c0dd3b3bb701197fe087baefe784eac9c30
02b4f9488f0029c08606341d49ef113ff7cdd8c60abe6f5cefbff792e9317e4f9d36b948dfdd
f409e264580f65

Message 4:

0f351c71e76f5fbe548d4c54a69a2bcb3d2e4ceb3cfb5250c24dff419949683f8ed3a5f04f5
7116fe797410d2c138b60db6da534a7abe0f658b65b5c0ccbeb67d1c9d9216d8befeb351
73f3596f40d4fa84e1e702818fbc06bec90d4315fceacfa7112c3e55d74aaf3394bb08f7504
a8e5019c4e3e838e0f364946f31721a49ad2d24ff6775efcb4f79fe4217a01b43cb5068bf3
b52ca76543187274

Message 5:

1a311571ff660da658c80545e98325ca646746a22ef55202d04cf90d93067c70a6c8b6b94
c161120af95421b3a138b609d6abe2ae6b2e6eb42f7431405c4a56ad1c9cf3b67cafbe723
01393583e80d58a34517767b19b58166a0c3db304acfbafa721591ea4d398af07c49b69a
7118fcff4889597aca81433b4953f50b2bbbdf9dcd0aff7013d3b5a3d3ec2b73019c3aa91b
8bddf411a72b480c636cc6597494151386

Message 6:

1835183ce0614abc558d4c41a69521cc646f5ae77aee5247cc4ae506d752777ae8c8a5a
5565e5f26fcd84f0c2b47877cdb71a426e9e6eea440be525c00cff166c19dc23b28e2eba4
271c2e7a97e94c49af5252787b1dbacf27f4df923c4883baa26e158dfe416faebd7c4dba97
3004b9ff4a914529d0cf1432004cf94520bedf9dd00aea6750e9b5a580ad266d44de3cb30
4d295f447a1634c117a68c41e67d50d09c35928a62e6d6648371b40ac83b274cecb04d6
c41b6fba

Message 7:

1928103df46943b510d94044ee8227da256208f123ee4347ca50ab0899507073bed9a4f0

43161320fbd8420f7f5b837c9f25bb28f5adafe542b3170f14cfe66ac385c4336dcfbfef2c1d
3a7987ff4a4bea4d13773c05bac662f390d3304983afa871008cee4775b8bd7a54bb907e
11fcfd4f99003ec68d163d0e49f2026ca3dfcec006f06513fcb4b3d3ff2279409d27b21ac2d
bf2

Message 8:
12290a71f96d5dbd43de4c45ea896ecd2b2e45ed2cf81756c803e70881433f6ba79cb8a0
47441e3bead84c1d7f528c77db69a931e2aaaff345a35f1311dea56fc788db2066ccbff030
132e7091bb4f47be52526a3e15b6c869e7dccb7e40c6beb4771a84e14d6ab8bd7f49be9
e7d13b2e852dd4f3c839f06281a4ff20420f7d3d3d200ec6f52e9b3b89d

Message 9:
14331c71fd614eba59c34007e58d2099206108f632f81755c851e04198403f79a1daa3a9
02590d2be6964c1b26138f6b95258228a7abeee744be591944c9e46d828dc2697cc3faa4
351d3f7ec2f44b0ea54f17393e08afd366efc2d63743c2ada33e1982e3

Message 10:
127d0c22f5640da65f8d514fef822599306649f67afe4e40c251f81196457a3fbfdda4f0445f
193bf6d8540c3e41912e9a72ad3ea791e7e558f77e5c10c2ea76c581d9697fcaeca4241b
2b619bbb544bab5301393a07bad827f7d1c17e42cdb3a33e0086e30860aefc6b48ff9867
17a5bc6093447ad487022e4969bc1124b8cfdadc1bbe7552eefaa396e36766449f21ae48
cac2f41ee262595d616cd95963990b03824934ea2a287844722140b583a2638bcf16c3df
0323a212740f3d5b517fbd10e4e253512e

Message 11:
0c385930e2650da658c80544ee8522dd366b46a235fb17438757ee029f487073a7dbbeb
3435a5f2ee89d0d3e3a138a6f8d60ec21e8b3e1e00ca4430e01cbe86fcb87c82d28dcfefd
31522273c2ff4247a44652742e13b38168e690dd2b5f83adb56b008ae34d39bcf26b50ffa
9621fb2e84893477aca9c43340600f00a22b0dfcf941bf66713f2b4bb8aad307e58de3cbb
48d9d0e515ad6f581e7f63cd59609a160d900d1faf2329634f354814b793bc37c3d700d5c
71271e30d740e7815516dbd1af8a344533fcb

Message 12:
0829003df52058a155c90553e9cc2cdc646f46a233f34347d542e8159e49713faad9a3a74
753116ffb90484937468f6f9525bf28f2aaafe542b317080bc5e970829dc5287c8be8e1301
76d798bf6445aa34f1539121efbd56fe590d6374acaabbb725486ff4939a2e9394cb6957c
56b4fd5798002ecccf00350445bc033eb8d79dc007fb2240f2afbbd3ec2b704f9b

Message 13: This is the message you need to decode:
0f351c71c7654ff251de056ea68920cf2d7d49e53ff9174bd303fc04d74e7e69ad9cb9bf561
60c2aea960d002b139b6b8f25982fe2e6e9f158a2451944c3f623d19dc425648beceb621f
38768abb4f47ad46176b7b04b3c069a0c4da3b0dd3bea96a54b7e4453989f86b55ba8b6
35b90f944

Deliverables:

You need to submit a pdf file detailing your attempts to solve the challenge and your report should also contain any source code (appendix) used.

1) describing in detail how you solved this challenge, if you didn’t succeed you can still submit whatever you tried.
2) The solution