Assignment 1
BITS F463 : CRYPTOGRAPHY
(Using of same pad (key) multiple times)

In the class we discussed that using the same pad multiple times could lead to an insecure cipher. Following are hex-encoded ciphertexts that are the result of encrypting corresponding plaintexts with a stream cipher, all with the same key (k xor m). In this assignment, your objective is to decrypt the last ciphertext (Ciphertext #10). As part of the submission, you have to submit the pliantext of last ciphertext, your source code and the approach that you took to break the cipher, in three different files.

Ciphertext #1:

fa6a8378c519cd8cc62d3b09f4e276c86b27e4736879ee96a120097c6a52d153fb0e9575aa7867fc246
cd22b88f0f20a5f069eb8fa08e910330e0cf1bb28a4e36c9220d4948d5b1e811271703420475e2c3ac5
5f70ae514931a7a8c8f35fe5274667136edc9bd5837972e7f206bab3e68a552844f0d19bcc7c75b904b
6cd94546fca0e291fa0e070bbc6625b3c939b70129e3735f43658c4dd5d4339fe610104bcef009cb7d5
d3d92bf191548f7b72709a43bc8d0f32f252a72ed3e3cf576ab6d5d6082d4fdc22f52bd2d7d0b2e2101
1919fa1209be9fe6b40c8338a065ad8fb56129df1d0be4cacbd0aa1c949f44ed2e65916abef2bb3e313c
761f1ba9d882ef00a63369587f77eabf88dc45ef694e022a5290f6a931bd7d8b0b08ae7396ab889d11af
6defb1ee55c956d4e0dbd9b0b10ac3ae7e4ccea6efe1be9de165fb8c3c01e4f0e090badd903a7be9ced5
d9f7e68ff4914dfde8d2c11530597cbf702e0854069ddbe65cf7b216347e9b81c47cffaef4c0ed88ba80d
02fddeafb62b4a55ee5db24f82ef7e751ab3c8a774840f56bcd73da9daddda5bb1c36832138eaabfa08b
ca25f67a8ad667b1c740a6d6d7ca06d54d53472f747962131cd20f54dc7cf1c14f7b8cbafbb5b4317ef0
35b8ab2ed292090b6f4aa9592bdcb138bd403847337b8c2661ac99123646b759d4ce30155c5c41bd22
e44ba1f36b67d99e4bf95d503133eab235f7ecff0d64bdea7682bfc23fe34384ff5086ca5f8ea8943f445
687e561a7e45d23adf1d43d253a6636ed7ad34b09f20ca6417e733b3db796a888405622e76182802fd
ae5bac734426d562adc36a6512d52553816724e0e1630252b5426aa5d2dd6ddc560c57ab0149bfd33e
69198e4e44f69006ca984069ef6cf8b75bd6c8155f8d742d0beacf32d602cb5b63b938e4d6103914374
8b484965519e14a2b952120b7bbde38194b110b4674d17e8c65cc84afbe2

Ciphertext #2:

e4698369cb1a88c8d02e3709b1a335cb6a3ae03a6365ee9bb1200935644fd14efd4bc16fac6433bb396
5873edef4e21c5e1ad781f549e9583f130cd8a42bb3a538ad21db878d450881127f70673640553c3bd8
4e62b31b4918bbe7d1bb4ead2d416a56789580d7986e21e7fb48b0fcfad911394af8cbdebf7c73b219b
6c1db486f84053518a0f276e9d72a5f7e9d9965408c3131f3651dd3da1e433dee2f2a1efaa25090b693
92e636bd89039d667a7bdf43badd0526b45eb222c0f6cf406ebed2dc5b64499d37ff65c3d1dcb3b7130
d919fb7699cacf22250c8338b175ad7e00416c7fd93a645a0be4fa68653ef4ccfa9600ca3ef78a9b041c
330f7a38a8e34b1152c3a8281fe79a2fac0ce45f6c7e620e0640178c71dca98e39c8da83871b3cccd1db
ecfe61eef58db68193aaa9a4a11be77e7fec1a276fa13f8c51659a1c0c95f5208091de88d02b5eadd814
3966924f21a5bded89f2b06554096c9b20ffb8a5f2ac0be30d174306451b5b83c47c4aee44812d89eac
5457e7d5eaa8375151a158e61f99f42e791bffc5e83d8b4240be9e26a29edacd41abc526324195b2aae
58c8522fb6b958233b6c44086dcd7cd00ce024952616562741f4ff40e0f9005ffda0b2ca4a0f3f1e0357
0eb66b4f86dd995090b7356af4f2199ab25bd6434443a61d82638edb45d3e57a859d9cc751e085251b
d76f846babd6560d0d9188d5459620fbfb578f0ecf81561f3fd3998a48b39f347d6ab59d4c04ac7b98f6
b4303a0f561a6ef0925b8a5de7231262275d471c4490ee918f55f7369247ce4b0bec0514c34e7468680
359ff8e98218516d4a6fd96cf463680651761f6402165e383f7f7667aa412d84aed97dc934be0cd7bc7b

e49995e6b71a680a29af9f17d1e9c7ca6fbd6acc02fecc0ee7fda9f92c702cbbf51d89dd477b4c835f758
a1b4e2a59971caca515541660b8a691dbb110fd7d4201e19b15f847edeceb69dda109340ac4f7523b05
920a1df078665e91f62263e9627eb42d3f4cddebf62984c5b0eaf6344c93bc17bb6c7cd5d3df57ea7e19
8ec082b6815098556d58f4572b66882df933d863e449c3eeca1d17e774047ee7c5f3efe12a35b93ea5b
0a7a64145104e623b4cedc73c49e7d2f20e8d960bf3d0dfc093a567d972bebe961490b24dc4b64a1a26
006752c8ac81916d75ebb842d7458436f846ff4147958da7cfb56d325d58843c28751d1f658efa95d45
b888ee7a2be2fcd1f57eb576e05effcbe59e0e7c61ee47cb7a9b44e45489473769050331d41706b68ea
887f1753b6005e8d8c71bcee6d472dab3642f1607832c5f0910a03f2a475960b3571fa4f730c06da2b6
ea9ddb956a2f1df6c548c289dfcb7c083f0d1502b07

Ciphertext #3:

f967c662c14fc9ded0682902b8ef76cf6a26f43d2c76f287b73609356c52d154f45a946fa62b2bf23d66
871ec4f4f311581dcd9bf31df4537a125e9db53ca0aa25b129c189c2421acd51767166364c496768ff45
31b45d0823f5b4c0bd58e862416a5678d0c8df852a6fe1bd0ea6e1ec9c552844f0d19bfc7069b00ef5ca
d11d7f8b0c2a0ee4b369a0c5271a38939c6757c77f15a0704fd3c65b5975e2262a4db5f80094e48896f
321bd80158f346970c849e9910537b456a133d3ed80586fb49cda18794ecb3de4729e92e0b2a60511d
48db43e9de3ea395ec1229d4319dee112129ab8dcbc5ee9f006b1c94afd44c3b5350abdaa6ab4f413c2
28f1ba948a3ee24625228b99b67da9e981c35feeddec64e331007d9317ca98e3df90af2c76fdcad60fec
daea4ae84f92730b7bb9df0617ae32a9f08fe164fe16b58d7f54e0d2df5f40011e4fecde4bb2a2d981449
66f2df84e5dcac0cc240d42408bcae119f98d422e89f123d77639374ffeec1c4bc4b6e54e40998ab9440
1faceb3e43d4653f24de113d0f4667548b9c3e867874101bc902fe7d1ca885ba0c762765095b7b6e4c8
c72eb57c95cc34b7c50597dcdd9904d04b50516f3143771f45ee1501c029e48f583eaeb1ecb5a9373fe
535bcb16dc4945a1f7b4fbf1c6f93ae33f3363b4c203599673ce4a20f6216b15fdace7951085251ef25e
94bb7f36f7280d759a94c59232eeaae36e6eff91c77b6fa7693a89632f44c97b35a8d8b12e6a58c2e5a1
3a6aa28abfe093db1f0cb79643c6360de3fdb4514f24df259733a273db09cb6944c453de74285c13c9ff
ea48e17426d476fcf67e2262c1b4d261564175a1d3930797824aa4c3acd8ed87a8667ff0fddbc7ff8929
1a6e46e6f017bbe911d83fc878b72ad7d8455e2dc07e7aee9b627663aebff06828e507a469f5e3b81074
f67109a51a2bb02111866b1ad809ee958f77c501eac9557c90feba3d66fdae51b291accb3132b4a981b
15fa23

Ciphertext #4:
ec2fc075c80388c1d4317e05b1a335cb6a3aea376962f891f432167c7359d14efc428d3db76322bb356
bc236c1f2f1090a13d08bb219f54929144fdcbe6ea2b42dab2fd0938d4515d218747b3421415f692bd3
477de053063bb9a8d2f35ce82e59225062d49ad7957e64fcf412acf7af9410284df3cad7f67c3cac0ba1
c0c35c6599402705e4b366accf2e1a339d876a4688363af33655d3d15b5826f3203e04a9a400a1ac9ed
3f52af09818996c7661c310a69b4a34fc5ee42adde38a5773bbd9c85b64499d20f86e90d1d0b0ae4002
9a88e43a87e9f33917c9388c0608d0ec021281bfc0f240a4be06a38c4ee85c86a7665fbae26aaeb044c3
61e1ab948767dd0f2532c9d5df7eece988c410e3d6fc21eb270b3e88188597fedf81a9396ba9d09e19f6
d2ea56ad4e94640b7ba89a050eb43ee7f4ceee6db209f4d85a16e0c7c41a06030903e18d0ebea2d5c35
d8d6868e45f59cade8723005c05d9dfe003e4815e3dc0b4368c3a017f47e8fd5d59d9b5fc48128c80a8
5e57f6d7afb63f5b1ae04ab25ed0a06d7f06acd4f668874142bcd727a19eccc04de5c1693b4396a7a2e9
9cdc6bfa79dacd35b9c00e8cc3d8cd0cd34c06552f752a774a52e21448df32be8f7f33a2a6bff6af346fe
870a9f87dd38f5a077c19bc49219fac3ff2782e033b66d83027edb95d6153e555d8de39155c5955a33a
ac42bab5673d

Ciphertext #5:

fa6a8378c519cd8cc62d3b09f4f73ed66b3ce43b6365e9d5a03b1f356d55824efa5c983dac6d67e8356a
c235dcf8e3080a06d68ee649f4447a1e43c8be2ae1b223b168d098dd401ac81f307f7a2c5d522026d10
b72af5b0a25b0b3c0f34aef2d40761365c781d19f6421e1fb48a5fae99c597c41f0d1cffa6d30fc0bbbcc
94487283162319f3f62be9ee2d5e3b8e802457842f3df27f5eddd01e4436ee24230ebfaa4f9ba882d3e5
26ef89009f7c7a669a44a1984a2fe14fa13592fc9a4660b6dfde5b62419d20f86e90c6c7a9a74011918d
a8279bf5b46b63c8238b430dd9ee025b9db2dab743b1b91cb19a1dfd5dc3e6650dace97fb3f35ac826a
2a38bcb28ff0a3a7786d5e565aef785c244ebc2ea64e62b006d930cd095e4968ba96d6dbb89d301fade
e54dad52956c4e3abe8b0f0cf83aa9f8dbea64e05aecc44252afc6d85f54050d0ce5c405a1eac8ce43986
92ce51a55c5d5cc210d5e0395dae105e2810c2cc7b56b824e3d7202fdf71145c4ade95f13d886ab0d18
fddfeaa9375a5fed19f34d95a06f620faad8e97ac24e46b89e26b4ca98dc40a08260375a8eaafaef8e852
dfa7396cd30bbd313c5d6df9904d24d525c24632a785b53ed4040de38b0db432eb8f5ece0a3313fe535
a1aa61d59e091b3a5aa8592e88bd25bd7333473e708b346fe5a9127a45e541dedf3d51085251ef30e34
2bfbc75768b8418b65a1c273da9b378eaece91c69a0be3784b5c234e94c82b65881c45ec2b3db3f5e0f
bde86fe2fe466abbe8d7712b2d2272d279d14f15e303f21175753924ad97bb894b4371aa539e89349ef
fe98b10487c023fc165ef7221115f3a59761b0a0e3e237f3928ac0929c8918c7c917cba129bea76e2809
1ece457620567a8d7069eb9c8c46fac6c8319b1ca01eab8abe22a6520f8b60082dd41735195443b9b0
71d691e9807a6b906540d7cb5e3859aac0cfc334a14e8d35ac043e7bbdd6ec0a1113d5fc7fd17780398
1118be646d0a8ab96368fe7f65a57f7e19fdf0f63ec18cacaca23f46dfa217b97435cadb9e58fa331786c
08cb68b468952225ee4502b7b9866f760e126e95c8df8ce5e1be674162cea9ca2ffe92929b122a2eaad
b341551d497f754af7cb7341a69edf12da834af285dddb93b3619070a6ee801e97b84b8dad4d193100
79498db0c89e6c72e7f7558148933db741f4154b8ac1abc6a46a25541d896f7c694904618efdc795439
e99e7afb766ce1741e4426e2ef4a8ea5feab3900ffe6abbfba30f0313947a71d377325a0c576e2bdc933e
1140a5415fd39f79aae3281407a63305e5783677e0eb9c4f26e3a828de323c30ed037f1e54c23a2becc
0bf53a7fddf7c11d83499e4fbdd85f88240784fd82887b5dd49a0f77a15fb05472e5595037b13925ea1
d0e21f08b051fe1ee9f03abb402e3cac2487919d54e8

Ciphertext #6:

fa67c67e8418cd8cc52d2c04b1ea20c12428a3216974bd86a0211b6267598348ec0e8073a72b20e933
66c97bc4f4f1134f0192cfe50cbd583b0b499db920aeab20a02cd2858d431d8105787b79754a552438
d95874a4150631f5b4cabe4ef92a5c6c542ac281c29e2a65e7eb0dbbe0ead9073948ffc0c8ec3f7db20e
f5c9945a6e8f052805e5e076e9d2375b32959a6d579a7174a04255d3c9595f75e6613e14b7e84f99e49
79afd20bd9c1c9934687ac854e98f0f24b454b667c6e78a1468a2d1d91e7f078c78b068d1dc95aea710
11919fa1209bacff2243c8338a4f5ac5e7135b99bec1b60db7b50be58d52f95c86a87a0bede26aacf513
d229e3bed89922f508262494d5e765adf189d549a2c0e721a5270170941dcc99e58cc4ac236daac5db0
af9dea95ae2588829063aae9a445ef802a8e28fe160fc5af8c25b4ab5c7c95f49124c1be5c405adeacbc8
40913b29b64d5bd9c8cc2d10100e8cc2f009e6c44020c2b465d07f313b02f1ed0e5d8bbbff0d079786a
90d16e09ab8a13c505ff24ab2549eef797c0dbbd6e23d814e4ff9952de7cbcbcd4ce5d669765095afaaf
59cc039b57e94c667aac9098bd2959907c95606432865627e4a48a10b4fdf2bf9c14c7ba3bae8b5b436
3ff560b0b467c29a0e016c5cb6456f95b622f8642d513761d8266fffb4107459a916dbc23e145c4851a
b7aac57bca6227098991fad1c572c33bdfb2fefe2f9596ca7be3f85f09322e74e9fab5780cc44cba6826b
581ebde863abe44e6abfe7c868307a2236ec77d25802a60cf51162723272b69cbc8e405722e7479f803
793f8b0c71645394d3adc29ed68270552331d620b5a0c34207e7035bb5a68ca928c7a8b60ba12cbee7
6e59580e1ab542b4460afd71884eadf8b68ab3e9e10f5d707f0aee5b6376b2cbbe01795d70476469045
75861c54651fd61ea5eb051c1860f0a2c38caa0af033491ba3d015de4aececd579d2ef0d755f88dc1c3d
4a9f1f1abe6f661684ef6726fe792da16e2419c5f1f428c191b7e9f6385797b500f43874c4d79651b333
178e8c98f98645db456d58a7512f639e23b860da26ee5582e2c60d15aa661f37e58da2f9e53761a023a
4e0adb20d585541652140ebde2142bdd2da0983d04ad698dbc1d6f26ec331b9eb805184be47c3a7500
6684b604e9fb28d926264e7f252d254d626e404ba164792c5add4b524275f44c075326e58197d99f69
39540968fa9eda323c01e59eb053d0abaeafb5ee1f4c618e968abb2e6445608

Ciphertext #7:

f967c630c806dcc9c7292a12a6e676cb6269e0217560e99ab3211b656d45d152f45dc17ce36832e93f6
cd22888f9f9165e1dcc96bc49ce55390f49deab62e1b32ae52bda95df5f1e8d51787f677548563e29cf5
831b059082eb0a385b20bee275b76416bd9c8c4996664a2bd0abce7af8c1b2845fd85cff77a3c9a03a7
dbc01d4b85122a0fa0c464bb8f6253338c817646883120a07258cad9525825ea242319a9aa4185b49e
92e420f9c81d92346f67d35ebddd032eb45ae42addfd8a1469a59cd71e7e549d20f966d5deccfca4011
09c85ab20cfedf42f17d43e9d431cd8ea1a1fcebcdca448a1f009aa9b4afd5dc2e67c11ede77eb9f813d2
29e7ea8b8a2af44634369ed5f763ecf294c955f094fc34e027077f8b17df93f4df80ae3e61b4d9d207f0d
efa10

Ciphertext #8:

ec69d775d64fdcc4d068180ea6f022845326f13f6830ca94a67f5a7d6a4b944cf05ccd3db7632ef53170
8739cdf6f10b0a06d1cff101fc5e3d18029d871de19d3ea8319581c3485bef106667343a5b5d2826df5
170b45c0639a6eb85a444ff295c6c542ad086c29f7864e2e448a0fdaf8a103f5ef4d197bf7d79bb0bbb8
8c0523c87012d0ea0f570a7c723573b929a655ec93e30f67753dfd94d173ce9612e1fa3fa549aa38992e
62de4c654b8616d7cd457e9890225b44fac2ec0fb865175f7ddd51f2d41d226e462d5c195bde206068
3cca62f9ce5f96b47c1269d110991eb1f1fceb0c3a248a4a24fac871de847c3e67a0fa8e42bb6f947c333
e3be8d9922b1072d33c786f366a9ef81cd10f6c6ea25f12d1d7b945eca98b08b8ca26d71a8cbd40bfdcf
a949e84f9e291e2eba93030db03ea3bb8fe074e65aefc5531aacd2d80b43124c18e8df0ee6acddd34091
7e3ab65b5acf8c8a231044089cddb20ef18c4527cdf131ca7f756456faec1809c4bcac59089dc9ac5f03
bd9a88bd784a52e419f75194a0617648abd9e23d954e53f98320a29eccda49abd16f225a95acfaf789d
66bf67097d22bbbd505cb99eed011d402495a2431647e4b5de30c449039e8cc4e2bbfbcf0fbec796bec
70f1a87bd497130b3a55b3482a8eb922e86438033a749c672be5a8193816915ed6df7514045951bf22
e541bdf375728ad77bb55d492639ea8830e6ede3166ba0be2697a08725a802a2b753d4e65dc3a78e25
4515b5f261ade4091eb6e0c86f3d746d709b4cd24915e30eff1145632426a194abcc055339ae5582c13
a8afcac860b467d0226c029f26e2d527c3315694e290722256e74678a4c2bcc93c5708478ff2ad4e961
ff9598a8ad54275530efce5cd1b9eacd75bd6ccc01f9dc42d0b8a6f92d6769ccf9008bca044542840c7e
810c586e519f05e3bc13075970b5a08f9ab60bfd754c17ac9915dc40fbbfd17edff85e390688fe1b2b1e
9d1511b0

Ciphertext #9:

ee7dda60d000c4c3d2317e17a6e625c16a3df0736d30f99cb235137670508543b5408e69e36d28ee38
678732c6b1fe0a581fdf83b208fe513e1841d4b16ea5b53fa621c58cc4421ed25164767175475f2c2c9
64d7eb2151d3fb0e7d5a144fd2747225a64c18dc4976975e7f206e9fce9d9162e55e1d1d4f86d7dac02
ac88d55378ca033412f0e764a7c22e432d959d2a12bd373df3365cced54d5226a72e3819fae546d5b09
396b623fc8b00dc607774ce10a0934a34fc5ee426d0fc8a5a65b29cd41d2d55d835fc2bd3ddd8b1b70e
0a978db02780e2e96b45c5278d0a08d4e213159aa29ff244b1f006b6c958fd5cdfe66110edfa79b5e05c
d524a2abd8983ee212263ac781fe71b8bd81d140e7d5fd37a531007c951bc49df19d88a2632290c8d0
17bedaea5fe95896600d7bbc9a1917bf35b4b7cef064b209f48d5555adc3c01a5e401807ecd94bb2a2d
98143966e24f21a56ce8c8f301b401498c1f300ed975869cdbe20d1743a6302f0f6125e8bade448129d
c9b94257e0ceabb62c1e5ff949fd4c99ee69300eb3d0f06ec2464ff98320a2cddd884ca0d16f315d89e2
b3f3c8c32ae73f92c335bac412c5cdd1d80b9c46434728766478515ba11449d531b0c6457bbfbdfab5a
6306df761f1a862d7981f463a6db2596f8ebd25e87a29033b66d83327edb95d625ea016d4c43801194
e5dbb3ffa4bf3a3707c9a924baa101c3534a3b830a7eafe596abdfb7685a49038e845d6b25980cc44cfb
e92244256bde828a3e9482ebbe8ce7e64266765de7ec5490faa4de55078743826e48db98b400439a85
a8ecf

Ciphertext #10:

f967c630d307c7c0d0682e08bded22846b2fa3307e69ed81bb3408747554881afc5dc169ac2b2cfe337
3872fc0f4b0154613d781e60ce5447a0e49dea02bb5fc2ab727d8c0c84d0dc402746c7b25595f3b3b96
4a7db35a4934b4abc9b64fad2351745678c689c49f6f72a2bd09bde7ee9a1e395ee2899bf67168b918b
6cdc4497398136a4be9fd71acd12e552e999c771ec9363af46448d8d94c4479a72e3d1db5e4459bb08
8dfb62aefc80795796f79c310bd950f60f155a12acba1cf7167a1d9c81f7f48cd24f579c392d4aea74002
879fb1238ae8ba3f58803e99151f91ec19169ebdd6a648e5b10ca68c4eef0fd2a9350ba5ef2bb9ff5ecb3
4eca39b8a33f8092d24c797f364bbf885cf10f6dcea64f621007a820c8597fe9bc4b52861b8c0c80bec9
5a97dff448b7d0f35b993130db128e7fedca275fa1fbbde5553a5ddcf1a060f0a4fffc808a9bcd9d35d97
7c68e252518bdc80230b5e149cd7e64cfb820c2889bc20d169347047bbef145dc3b5f95940998aae48
04e09abeab784a52e419f95a89ae2e431dbcd2e26e914954b5d72bb5c7c8dc49abc36a2f4093b1faed8
9dc6be77a99cd31bbd34091d1dc9915d0434f5a357472651f53f34055d839b0c44e22e5f5d6e1e0387
3f77af1b56fcfdb1c01745dfa4b2a9db338f8652e46213591296feded1e644fb542d8d82c02085f59ef2
2e44fa7f367659c994cac5d502e25eab73de6e7ad0d6af3ea3e93f09225e3549fb043878540cbb98e275
805faa62096e24c6ab2ead46e643b6436da3fdc4f1ea619ee43796f303ae497b78e465628b7428b8f3a9
6f5bd8e1a0374472ec07aa66f3b525d3715690b1e5e307168762aae5b27c994df76cb3d