B2M32IBEA LS 2019-2020 Zadání č. 694

Jméno: Dzivjak Matouš (99) Datum zadání: 05.03.2020 Datum odevzdání: 10.5.2010 3:55 CET

Pokyny: Dobrý den, v tomto mailu naleznete zadání semestrální práce. Vaším úkolem je rozluštit jednoduché šifrové texty a vypracovat o tom závěrečnou zprávu.

Pokyny k vypracování jsou popsány zde: https://moodle.fel.cvut.cz/mod/page/view.php?id=146917

Hodnocení projektu je popsáno zde: https://moodle.fel.cvut.cz/mod/page/view.php?id=146918

Projekt odevzdávejte zde: https://moodle.fel.cvut.cz/mod/assign/view.php?id=146916

Jedna z úloh je bonusová, asi sami poznáte která. Velikost bonusu bude nepřímo úměrná počtu úspěšných řešitelů. :-D

Luštění zdar! Tomáš Vaněk

Úloha 1: DFMADESQFDFUCMHMZADFURQDFMAYRMWETGSD-
INGDFURQERXETGSDODANMDFMAMRIGSZEQMXFUCDGXMHMNGVFUODENMRDOEOEOENMOIN

Decrypt: THEYTAUGHTHIMEVERYTHINGTHEYKNEWABOUTCLOTHIN-
GANDABOUTSTYLETHEYENCOURAGEDHIMTODEVELOPHIST
ALENTSASASALESCLERKANDLUCIANOREWARDEDTHEMBYBEIN-
GAGOODWORKER

Reconstruction: They taught him everything they knew about clothing and about style. They encouraged him to develop his talents as a sales clerk and Luciano rewarded them by being a good worker.

Cipher used: Affine cipher with parameters `A=15` and `B=4` e.g. `f(x) = 15x + 4`. Where function `f` is used to get cipher text character `y` for open text character `x`.

Cipher key: In this case parameters A=15 and B=4.

Steps: I tried automatic decryption of various cipher types on https://www.dcode.fr/ until I got a positive result on https://www.dcode.fr/affine-cipher with the parameters above.

Úloha 2: SBEYNUDHSINIRGESNIHHOLUQSSBEYWEQENERSTQDEKCRIHS-
BLUABRLJESDJERKDOLOLUHCKLSUKCEQRSIKCHUODIKLBLWOIKYLUWLQGDKIKLHCTIRBDLKE

Decrypted: THEYBUILTABASKETBALLCOURTTHEYWEREBESTFRIEND-
SALTHOUGHSOMETIMESNICOCOULDNOTUNDERSTANDLUCIANOHOWCANYOUWORKINANOLDFA

Reconstruction: They built a basketball court. They were best friends although sometimes Nico could not understand Luciano. How can you work in an old fashion place like this, he asked one day in the Dellasiegas store. Because I have to Luciano replied. My family need the money.

Cipher used: Substitution with key, key: “inocet”. This key is used for the decryption! Not encryption. E.g. alphabet: INOCETABDFGHJKLMZQRSUVWPYX can be used for decryption of the cipher text, where’s seemingly random substitution alphabet GHDIEJKLAMNOPBCXRSTFUVWZYQ can be used for encryption.

Cipher key: inocet

Steps: After trying few different ciphers and decrypting the cipher text using them I tried automatic decryption using https://www.dcode.fr/monoalphabetic-substitution This was successful and I obtained the original text, the only strange thing was that the key was for decryption alphabet instead of encryption.

Úloha 3: EWFANASHOEWREHMAOOSTCEMLRTTREEFWSWXCROSNT-
TOIRUEYRETLOUEEURTEKHHENXOTIIHTMUCARCNERRDENOODNPDSSHSSEEHACRHNNTAOTAN

Decrypted: CHAPTERTWOAWOMANOFSUBSTANCESANTABONATREVI-
SOCLOTHINGSTORESINEUROPEWEREVERYDIFFERENTTHENFROMTODAYALONGWOODENCOUN

Reconstruction: Chapter two a woman of substance Santa Bona, Treviso clothing stores in europe were very different then from today. A long wooden counter separated the customers from the sales clerks and the clothes were hidden away except for a few things in the window.

Cipher used: Transposition table.

Cipher key: Table with 6 columns, order of columns: 6,1,2,5,4,3

Steps: Again after trying multiple types and kinds of cipher on https://www.dcode.fr/ I got a positive result with https://www.dcode.fr/transposition-cipher transposition cipher decoder that can bruteforce permutations up to size 6 which was the case here.

Úloha 4: 00726 02736 19263 07060 10007 03509 06158 07926 09366 04011 07817
11063 03150 00176 14559 02392 13094 18806 10818 02048 06442 01967 02289
08838 04755 17853 17268 12579 01340 09775 15683 10125 09301 09389 14559
06329 15405 16918 01855 02906 03591 02421 09307 14078 08172 17123 01961
05119 14841 08479 12471 00482 15085 17997 04067 16583 12424 00547 11111
17795 15816 01763 06847 16115 07121 14716 00166 13773 14596 12047 10173
05128 01848 18172 07531 10555 15405 00364 10818 09819 07044 19460 07118
16763 16325 01755 13883 17955 05460 08479 17021 14653 13152 03900 15467
12616 01346 00547 08338 02482 12628 11955 03595 05615 08880 02910 09653
00364 17243 17215 09072 04022 09160 19130 13788 00788 06696 00364 10818
02820 12329 13129 03150 00176 08172 04504 14259 15217 09406 18699 01684
09021 03150 13935 17541 07393 09653 19463 05552 17215 17165 07429 09621
18671 14344 12401 10631 03110 14405 12721 12189 04966 06253 15306 10548
05843 13094 17650 08507 02022 09072 03486 01611 00444 13788 12480 18936

07184 19756 03551 06442 01450 03595 00444 02978 04504 00828 18806 14730
14297 11297 04512 09160 19130 10007 13644 15238 13742 01845 11549 02600
03297 01848 19629 08780 07339 01961 18806 01845 13593 01684 09021 16748
16763 12932 02392 14820 14674 08596 14647 04027 04966 16748 13671 13788
16678 06989 17360 13054 07691 08857 17689 11164 17666 15814 08274 18250
17436 01340 02820 13480 00686 15965 03704 12505 11853 15405 14637 18981
02277 17008 19016 17195 07708 Public key: e=433 m=19837

Steps:

0. e = 433, m = 19837
1. factorize 19837 = 83 x 239
2. N = p*q = 19837 = 83 x 239
3. r = (p-1)*(q-1) = 19516
4. solve e*d = 1 mod r where d coprime to N, result: 18885
5. decrypt cipher text (using https://www.cs.drexel.edu/~jpopyack/Courses/CSP/Fa17/notes/10.1_Cryptogr

8970 9851 7872 1803 6974 9805 7666 9677 6578 7699 7370 8841 7982 4723 7384
3835 8476 9827 6988 7739 8470 2791 8582 4843 7264 9735 8286 657 8268 9789
8480 3651 7862 8873 7384 4725 7986 5847 7578 8799 8770 3781 7182 7723 6584
4845 7266 9897 8768 5789 8460 9681 8472 2693 8964 7655 7766 9797 8588 4879
7380 4721 6772 9773 7074 9825 8466 5667 7668 9679 7970 6791 8272 853 7664
7765 7986 4727 6988 3849 7260 9821 6982 7693 8264 9845 7276 9857 8368 5789
6880 3791 7082 9793 8574 8715 8066 9797 8078 6699 7770 3761 7672 3793 7884
3795 7086 4727 6978 7799 8580 4841 7262 9823 6964 6855 8486 4727 6988 9689
7360 8781 7982 4723 6584 6695 6576 8897 8778 2699 8260 9841 7982 3723 7984
655 7086 4697 8288 7799 8270 5761 8562 7733 6574 8795 6876 3687 7878 9849
7170 9831 8482 2653 7374 1725 8476 2797 7768 9669 8580 4731 7882 3843 6964
5685 8766 9787 8488 4799 8470 2691 7672 3843 8474 6695 8776 9827 7588 3729
7980 871 7262 9823 6974 2735 8386 3737 8388 4699 8280 7791 8272 5693 6874
3785 7266 9827 8388 659 8260 9841 7372 7693 7274 3835 8376 3837 8468 9829
6860 9831 7372 1783 6964 8655 7866 8777 6568 8699 6680 2731 7172 2843 7684
9675 7976 6797 8268 9689 8380 7691 6582 4693 8284 3705 7986 2847 7268 9709
6570 7731 7682 9003

6. I have no idea how to convert that to text...

Úloha 5: YQQNYTGGQRJTVGGQUYWNAMJYUYUGPKCKGJVPDTIGTP-
TACDGGUFGIRFTWEVJXYHGQVUCQGXGQQPQKWQTXYTRVWPUAGX

Polygram substitution??

Úloha 6: TEUHJKDQMMVJOKYTEROJMQWIQXYBEYLSKEZHYDO-
HJBTIXUQWRFDQLITXEDYUDUTUDBUAHFEJTJMOEYJQEMCYQEJOUX

Úloha 7: HIRALPDWBOCGSRTOOOBPRRHDPNEIAAHCOIXRURCNCP-
SRNYACYDHKDHWOPCYRKKHNSWYAJXRPDSDSJSHYKKPPOJCOJROSOOHQRESRAYSCYNSCPKP

Úloha 8: KWXLSSXETTRPDLMOFFSYLTVEJAUMTMZTRHVCWKAYZCSVPXR-
WCELFVEBZLEBULWYHJMQRIFBEEQARHILQIXYDADCDXGSTWSKIHMPIUTTCRROXXLCKIXHVU