Semestrálni práce - IBE 2016/2017

Jiří Kerner

3. listopadu 2016

1 Úloha 1

1.1 ŠT

AZQOAGXPZAFNQEGDQFTMFFTQEQMMZPFTQSDAGZPIQDQTA DULAZFMX-
TQZOQFTQDQXMFUHQ BAEUFUAZARQHQDKFTUZS QXEQEQQYQPBTMZF-
MEYMXXKHMDUMNXQ

1.2 OT bez mezer

ONECOULDNOTBESURETHATTHESEAANDTHEGROUNDWEREHORI ZON-
TALHENCETHERELATIVEPOSITIONOFEVERYTHINGELSES EEMEDPHAN-
TASMALLYVARIABLE

1.3 OT

ONE COULD NOT BE SURE THAT THESE A AND THE GROUND WERE
HORIZONTAL HENCE THE RELATIVE POSITION OF EVERYTHING ELSE
SEEMED PHANTASMALLY VARIABLE

1.4 Šifra

Monoalfabetická šifra s posunem.

1.5 Klíč

Koeficient A použitý pro šifrování je 12.

1.6 Popis řešení

Brute force útok pomocí skriptu v Pythonu. Více v ceaser.py. Tokenizer pro rozložení věty na slova a následně kontrola pomocí slovníku, jestli se jedná o anglickou větu.

2 Úloha 2

2.1 ŠT

JYJWTBUJGLDKJUJCHUCJYJWTBUJFHDGLDKJULUXDKLG GFEJULKGRNOJWJCDGBOOJWLUXGTLUKBDLXEKHUCXWBILUX GTDPRJJAJCLKDXJGHKLUBRDXWJJULNNJUDLKTKEWBRX EKEJOGHVZCBBWFHTLUKBKEJKHLUKJCBRKDLCJHLWBQKEHK IBLDBUVLKTBQNHCUJDD

2.2 OT bez mezer

EVERYONELISTENEDANDEVERYONEWASLISTENINGST ILLWHENITLUMBEREDSLOBBERINGLYINTOSIGHTANDG ROPINGLYSQUEEZEDITSGELATINOUSGREENIMMENSIT YTHROUGHTHEBLACKDOORWAYINTOTHETAINTEDOUTSI DEAIROFTHATPOISONCITYOFMADNESS

2.3 OT

EVERYONE LISTENED AND EVERYONE WAS LISTENING STILL WHEN IT LUMBERED SLOBBERINGLY INTO SIGHT AND GROPINGLY SQUEEZED ITS GELATINOUS GREEN IMMENSITY THROUGH THE BLACK DOORWAY INTO THE TAINTED OUTSIDE AIR OF THAT POISON CITY OF MADNESS

2.4 Šifra

Affiní šifra.

2.5 Klíč

Koeficient A je 7. Koeficient B je 7.

2.6 Popis řešení

Brute force útok pomocí skriptu v Pythonu. Více v monoWithKey.py. Tokenizer pro rozložení věty na slova a následně kontrola pomocí slovníku, jestli se jedná o

anglickou větu.

3 Úloha 3

3.1 ŠT

BKTVDSQVKJTYNQDSQSONKPPQDYYSNQDSBNY SQSNODEQYOQVYJQIST-
SJTLKKNVEHOKWNSU YTVEQDAYUYNEJQDSQQY HYLSQDEOEJPQSJQQ-
DYQDEJBKAQDYETKHPQD YBNYYJPQEOGXPLSVJKAQDYPQSNPDST-
SVSGY TQKOHSEIDEPKVJQDYP QSNPVYNYNEBDQSBSEJSJTVDSQSJSBY-
KHTOR HQDSTASEHYTQKTKCXTYPEBJSCSJTKAEJJKO YJQPSEHKNPD-
STTKJYC XSOOETYJQ

3.2 OT bez mezer

GODWHATWONDERTHATACROSSTHEEARTHAGREATARCHITECTWENTMADAN
DPOORWILCOXRAVEDWITHFEVERINTHATTELEPATHICINSTANTTHETHI
NGOFTHEIDOLSTHEGREENSTICKYSPAWNOFTHESTARSHADAWAKEDTOCL
AIMHISOWNTHESTARSWERERIGHTAGAINANDWHATANAGEOLDCULTHADF
AILEDTODOBYDESIGNABANDOFINNOCENTSAILORSHADDONEBYACCI-
DENTN

3.3 OT

GOD WHAT WONDER THAT ACROSS THEE ART HAGR EAT ARCHITECT
WENT MAD AND POOR WILCOX RAVED WITH FEVER IN THAT TELEPA-
THIC INSTANT THE THING OF THE IDOLS THE GREEN STICKY SPAWN
OF THE STARS HAD A WAKED TO CLAIM HIS OWN THE STARS WERE
RIGHT AGAIN AND WHAT AN AGE OLD CULT HAD FAILED TO DO BY
DESIGN A BAND OF INNOCENTS AIL ORS HAD DONE BY ACCIDENT

3.4 Šifra

Monoalfabetická šifra s heslem.

3.5 Klíč

Heslo použité pro zašifrování je SCOTY.

3.6 Popis řešení

Vyřešeno pomocí slovníkového útoku naprogramovaného v Pythonu.Více v vigener.py. Kontrola provedena na stránce https://www.guballa.de/substitution-solver.

4 Úloha 4

4.1 ŠT

FPJWOYNQDDVTGLZDLSGSMTHDUSMRRRFSATKAGMIDHSPVDB DBYINCHNRWCEEETEITRCUYMNWHRPZTKAYAVTHRFACI OSGSITKEZENOQRLSATKAGGCAUNRPNHRRRXCAWWNWIOWOS IVRWHGLZTLTNROHLNTJMOPTUINTDRFWGAYEEIYAQDTM WBHRRHGINECSGYSHRQZCXRFMIGWHRJGEHIAKNHLPBJJDB SFIPSWHRRWOODRVOHDNGLZSWOEMZDFYPPJPVGEIVTFT UYGHXSYMYGUENWDLBIAXJTKEJEOEUAAHWEJAAXJPXRFYZ WLTUZVSWWNZZRDIFMIGVTESFEVOSGJSPIPTJTHNPC

4.2 OT bez mezer

SLOWLYAMIDSTTHEDISTORTEDHORRORSOFTHATINDESCRIB ABLESCENESHEBEGANTOCHURNTHELETHALWATERSWHILST ONTHEMASONRYOFTHATCHARNELSHORETHATWASNOTOFEAR THTHETITANTHINGFROMTHESTARSSLAVEREDANDGIBBERE DLIKEPOLYPHEMECURSINGTHEFLEEINGSHIPOFODYSSEUS THENBOLDERTHANTHESTORIEDCYCLOPSGREATCTHULHUSL IDGREASILYINTOTHEWATERANDBEGANTOPURSUEWITHVAS TWAVERAISINGSTROKESOFCOSMICPOTENCY

4.3 OT

SLOWLY AMIDST THE DISTORTED HORRORS OF THAT INDESCRIBABLE SCENES HE BEGAN TO CHURN THE LETHAL WATERS WHILST ON THE MASONRY OF THAT CHARNEL SHORE THAT WAS NOT OF EARTH THE TITAN THING FROM THE STARS SLAVERED AND GIBBERED LIKE POLYPHEME CURSING THE FLEEING SHIP OF ODYSSEUS THEN BOLDER THAN THE STORIED CYCLOPS GREAT CTHULHU SLID GREASILY INTO THE WATER AND BEGAN TO PURSUE WITH VAST WAVE RAISING STROKES OF COSMIC POTENCY

4.4 Šifra

Vigenérova šifra.

4.5 Klíč

Klíč použitý pro zašifrování je NEVADA.

4.6 Popis řešení

Vyřešeno pomocí slovníkového útoku naprogramovaného v Pythonu. Kontrola provedena na stránce https://www.guballa.de/vigenere-solver

5 Úloha 5

5.1 ŠT

TRNTBTFFGDOTITMSHTLHIOFAMENHGIESAHYENAONAHAEH OTOTABIAFODNEVFTNHUWTRDNEDTIDIIFHILAJOODWF HAIGROANXSOOLAMOECDASRDGXAHDITARLBNTTTTOXLA ENTTHAYOEBHAUXLNDTETIUHTAOEKTXASOHNEMGITFLRE OXFEVEDRSHSRTDENFXTNECESEISYEFASHXEORADOLNIT RLCOIX

5.2 OT bez mezer

THATWASALLAFTERTHATJOHANSENONLYBROODEDOVE RTHEIDOLINTHECABINANDATTENDEDTOAFEWMATTER SOFFOODFORHIMSELFANDTHELAUGHINGMANIACBYHI SSIDEHEDIDNOTTRYTONAVIGATEAFTERTHEFIRSTBO LDFLIGHTFORTHEREACTIONHADTAKENSOMETHINGOU TOFHISSOULXXXXXXXXX

5.3 OT

THAT WAS ALL AFTER THAT JOHANSEN ONLY BROODED OVER THE IDOL IN THE CABIN AND ATTENDED TO A FEW MATTERS OF FOOD FOR HIMSELF AND THE LAUGHING MANIAC BY HIS SIDE HE DID NOT TRY TO NAVIGATE AFTER THE FIRST BOLD FLIGHT FOR THE REACTION HAD TAKEN SOMETHING OUT OF HIS SOUL XXXX XXXX X

5.4 Šifra

Úplná tabulka.

5.5 Klíč

Tabulka o velikosti 14x16 a způsob zápisu při dešifrování, zapsat šifru do řádků a číst sloupce. Nebo také tabulka o velikosti 16x14 a při dešifrování zapsat šifru do sloupců a číst řádky.

5.6 Popis řešení

Brute force řešení pomocí programu v Pythonu. Více completeTable.py.

6 Úloha 6

6.1 ŠT

TWHCNENWVAITIXIHSINEEFFOGWIAOSOFESTYS TENIDERTCOAVECO-
HGHAEUTADIECTHNBDEREDPR PEREITLTRRMTTOOAYRIETTTWHPYE-
PEGEATTOE RAOALDNTOSTALAHPOOSNLHHGICONISMNIHIP EGEAIHME-
BETTANASDMIDNHPEIEBEEBEFTASRS ALTSLHEDIHEFWNWESCOHHHI-
ENRIDERI

6.2 OT bez mezer

6.3 OT

6.4 Šifra

6.5 Klíč

6.6 Popis řešení

7 Úloha 7

7.1 ŠT

HEUISIHDOSSSEBKPIISTDETNNWOIIYADBIIDU TDEEAONODFBEATRIRRL-
BWNAUAOSIEHSOITAFA ENGLEISEOZCOHLASERERIHENAWTSRERIAAET
KGLSNDMWEMINRNLPENEHLREYOSFPRMGALCLN IHVTIDMRKARCO-
ILSREHLNNWTISESABEHTVUC GSYEPOLTWHSNIEIALSTLECUCOBSEEPTLO-
HBF HDDORNLPCSYNTOSYIAACTTNMRELPHTNEADUH TCRYWTNRA-
SLNHBTPMOHOTLIVNY

7.2 OT bez mezer

HISACCURSEDCITYISSUNKENONCEMOREFORT HEVIGILANTSAILEDOVERTHESPOTAFTERTHEA PRILSTORMBUTHISMINISTERSONEARTHSTILL BELLOWANDPRANCEANDSLAYAROUNDIDOLCAPP EDMONOLITHSINLONELYPLACESHEMUSTHAVE BEENTRAPPEDBYTHESINKINGWHILSTWITHINH ISBLACKABYSSORELSETHEWORLDWOULDBYNOW BESCREAMINGWITHFRIGHTANDFRENZY

7.3 OT

HIS ACCURSED CITY IS SUNKEN ONCE MORE FOR THE VIGILANT SAILED OVER THE SPOT AFTER THE APRIL STORM BUT HIS MINISTERS ON EARTH STILL BELLOW AND PRANCE AND SLAY AROUND IDOL CAPPED MONOLITHS IN LONELY PLACES HE MUST HAVE BEEN TRAPPED BY THE SINKING WHILST WITHIN HIS BLACK ABYSS OR ELSE THE WORLD WOULD BY NOW BE SCREAMING WITH FRIGHT AND FRENZY

7.4 Šifra

Dvojnásobná tabulka

7.5 Klíč

Možných kombinací je několik. Například první tabulka o rozměrech 40x7 a a způsob zápisu při dešifrování, zapsat šifru do řádků a číst sloupce. Druhá tabulka pak rozměra způsob zápisu při dešifrování, zapsat šifru do řádků a číst sloupce.

7.6 Popis řešení

Brute force řešení pomocí vlastního programu v Pythonu. Šifra v souboru completeTable.py a spojeni dvou šifer pomocí pipe.py.

8 Úloha 8

8.1 ŠT

FXYTSWJSURNYXJPIAJSJXILFALWFJNPTFJJW NHDJNYNFTYAAFWHXQNXZXQRNJSYNJJXLHND XRWYKUSBIJTGXXFJLYPXNJTQLNNHSZGJSUSW

XNYRWJRSRYFXFXNYJJXSDUJRTLUNXNXXEFI FXKRWXJSRWTXSJRFSY-
YXTFTYSNFTSJJIJY HTFXWSAFYYNATYXZSNJJSXRFNGNTSNKXXUY TQ-
KIXFLIQSWYSNYTTFSJKRXYJJNLNFLSTGS SXAJFXNRXXTSNYKFOFIWJ-
HSXTJFMULSMTHJW YNQYFXSSRNJWNJWMHNMXXNLX

8.2 OT bez mezer

ANISMSINFORMATIONSECURITYMANAGEMENT SYSTEMPROVIDESAMO-
DELFORESTABLISHING IMPLEMENTINGOPERATINGMONITORINGREVI
EWINGMAINTAININGANDIMPROVINGTHEPROT ECTIONOFINFORMATI-
ONASSETSTOACHIEVEB USINESSOBJECTIVESBASEDUPONARISKASSE SS-
MENTANDTHEORGANIZATIONSRISKACCEPTA NCELEVELSDESIGNED-
TOEFFECTIVELYTREAT ANDMANAGERISKSSSSSSSSSSS

8.3 OT

ANI SMS INFORMATION SECURITY MANAGEMENT SYSTEM PROVIDES
A MODEL FOR ESTABLISHING IMPLEMENTING OPERATING MONITO-
RING REVIEWING MAINTAINING AND IMPROVING THE PROTECTION
OF INFORMATION ASSETS TO ACHIEVE BUSINESS OBJECTIVES BASED
UPON A RISK ASSESSMENT AND THE ORGANIZATIONS ISK ACCEPTANCE
LEVELS DESIGNED TO EFFECTIVELY TREAT AND MANAGE RISKS SSS
SSS SSS S S

8.4 Šifra

Monoalfabetická šifra s posunem a úplná tabulka bez hesla.

8.5 Klíč

Koeficient A použitý pro šifrování je 5. Tabulka o velikosti 17x18 a způsob zápisu při dešifrování, zapsat šifru do řádků a číst sloupce.

8.6 Popis řešení

Brute force řešení pomocí vlastního programu v Pythonu. Viz. přiloha.

9 Úloha 9

9.1 ŠT

MJUEYEQEQIJCDOYJYEQEIQCJYBOUIFFQFJJDXUHHDHJ DAEXUIMSXD-
HJDJDYUJMIUQHHJHUYXQLVCVCYJUHUQRXX UVCYYHIJTQQDTFEY-
UESEX

9.2 OT bez mezer

WHATEVERFORMINFORMATIONTAKESORTHEMEANSBYWHI CHTHEIN-
FORMATIONISTRANSMITTEDITALWAYSNEEDS APPROPRIATEPROTECTI-
ONHH

9.3 OT

WHATEVER FORM INFORMATION TAKES OR THE MEANS BY WHICH
THE INFORMATION IS TRANSMITTED IT ALWAYS NEEDS APPROPRI-
ATE PROTECTION HH

9.4 Šifra

Monoalfabetická šifra s posunem a úplná tabulka bez hesla.

9.5 Klíč

Koeficient A použitý pro šifrování je 16. Tabulka o velikosti 3x36 a způsob zápisu při dešifrování, zapsat šifru do řádků a číst sloupce.

9.6 Popis řešení

Brute force řešení pomocí vlastního programu v Pythonu. Viz. přiloha.

10 Úloha 10

10.1 ŠT

MNUSIKLJBTJJNDSBYDDNDKQKMNLCQKGILNTN DAVLNREBTKTSNTQ-
NJQMLZTBCRLDMDHQMDTES NKSODJLSNQCUSTCTTKLZSJMXMTTXQODH-
KLKK MSSEKUHQ MDSSMTVSDKKRSSMNNNSBQ DCKLLLT JJQNKLSSQMLNDC

KKKVSBKLNMJJVTNLME DRY DSLDQCNLQMDMSBSUTLNKHDKMTQR-
TJIMMBTK LJBDNUSIBDKMRASRTCLLNDKQKSKKRNENKMM DMNQN-
DLDIKLZSJDKKHNVMDNKSLVKFNUOTTMD EDN

10.2 OT bez mezer

10.3 OT

10.4 Šifra

10.5 Klíč

10.6 Popis řešení