

BÁO CÁO THỰC HÀNH

Môn học: Nhập môn bảo đảm và an ninh thông tin

Lab 3:

GVHD: Đoàn Minh Trung

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: IE105.P13.CNVN

STT	Họ và tên	MSSV	Email
1	Hoàng Bảo Long	22520807	22520807@gm.uit.edu.vn
2	Đặng Trần Long	22520805	22520805@gm.uit.edu.vn
3	Nguyễn Duy Phương	22521165	22521165@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Task 1 (1.1, 1.2)	60%
2	Task 2	100%
3	Task 3 (3.1)	0%
4	Task 4	100%
5	Task 5	100%
6	Task 6	100%
7	Task 7 (7.1 done)	50%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

Task 1:

Ex.1. Key for lock is 042

EX.2.

Approached using brute force technique since the test case is quite low (1->9)

Label each symbol as alphabet letter from a to i

Column 3 re write as $2b+2f=10i+i \Rightarrow ii \% 11=0$

After brute force I came out as 2

Continue brute force

7	7	5	1
9	9	6	9
5	8	5	4
8	9	6	9

Final result:

a	b	c	d	e	f	g	h	i
7	5	8	1	9	6	3	4	2

Task 2:

Encrypts or decrypts text based on the key and mode.

Attempts to decrypt ciphertext using all possible keys.

Prints the application menu.

Prompts the user to choose an option (1, 2, or 3).

Option 1 (Encrypt):

- Prompt for plaintext and key.

- Encrypt the plaintext.
- Print the ciphertext.

Option 2 (Decrypt):

- Prompt for ciphertext and key.
- Decrypt the ciphertext.
- Print the plaintext.

Option 3 (Brute-force):

- Prompt for ciphertext.
- Attempt to decrypt using all possible keys.

Invalid choice:

- Print an error message.

```
1. Encrypt a message
2. Decrypt a message
3. Brute-force a ciphertext
Choose an option (1/2/3): 3
Enter the ciphertext: Mfuzpn Rzwpfrnn bfx gtws ns Pdtvt ns 1949 fsi stb qnaxj sjfw Ytpdt. Mj nx ymj fzymtw tk rfad stajqx fx bjqq fx xmtwy xytwjnx fsi sts-knhnys. Mnx btwpn nshqzj Stwbjlnfs Btt i, Ymj Bnsi-Zu Gwld Hmwtshqj, Pfkpf ts ymj Xmtwj, Fkyjw Ifwp fsi Bmfy N Yfap Fgtzy Bmjs N Yfap Fgtzy Wzssnl. Mnx btwp mfx gjjs ywfxxqfjji nsyt rtwj ymfs ktwdy qfslzfljx, fsi ymj rtxy wjhjys tk mnx rfad nsywsfntsfq mtstzx nx ymj Ojwzxfqjr Uwej, bmtxj udwjantz wjhunjsyx nshqzj O.R. Htjejjj, Rnqfs Pzsjjwf, fsi A.X. Sfufzq.
Brute-forcing all possible keys:
```

```
Key 0: Mfuzpn Rzwpfrnn bfx gtws ns Pdtvt ns 1949 fsi stb qnaxj sjfw Ytpdt. Mj nx ymj fzymtw tk rfad stajqx fx bjqq fx xmtwy xytwjnx fsi sts-knhnys. Mnx btwpn nshqzj Stwbjlnfs Btti, Ymj Bnsi-Zu Gwld Hmwtshqj, Pfkpf ts ymj Xmtwj, Fkyjw Ifwp fsi Bmfy N Yfap Fgtzy Bmjs N Yfap Fgtzy Wzssnl. Mnx btwp mfx gjjs ywfxxqfjji nsyt rtwj ymfs ktwdy qfslzfljx, fsi ymj rtxy wjhjys tk mnx rfad nsywsfntsfq mtstzx nx ymj Ojwzxfqjr Uwej, bmtxj udwjantz wjhunjsyx nshqzj O.R. Htjejjj, Rnqfs Pzsjjwf, fsi A.X. Sfufzq.
Key 1: Levom Oyveoem aew favr mr Ocxs mr 1949 erh rsa pziw riev Xsocs. Li mw xli eyxlv sj qerc rszipw ew aipp ew wlvx wxsvmiw erh rsr-jngxmsr. Lmw asvow mrgpyhi Rsvaikmer Assh, Xli Amrh-Yt Fmh Glvsrmgpi, Oeje sr xli Wlsvl, Ejxiv Hevo erh Alex M Xepo Efsyx Alir M Xepo Efsyx Vyrrmr. Lmw asvo lew fiir xvrwpexih mrxs qsvi xler jsvxc perkyeki, erh xli qswx vigirx sj lmw qerc mrxivr exmsrep lrsyvw mw xli Nivwepiq Vmld, alsui tvizmsy vigntirxw mrgpyhi N.Q. Gsidxi, Qmper Oyhrive, erh Z.W. Remteyp.
Key 2: Kduxl Pxdndpl zdv eruq lq Nbrwr lq 1949 dag qrz oiyhv qhu Wnrb. Kh lv wkh dkwru ri pdq qryhov dv zhoo dv vkruw vrvulhv dag qrz-lilwlrq. Klv zrurv lqfoxgh Qruzhjldq Zrrg, Wkh Zlag-Xs Elug Fkurqifoh, Ndind rq wkh Vkrub, Diwuh Gdun dag Zkdw L Wdon Derxw Zkhq L Wdon Derxw Uxqlqaj. Klv zrur kad ehqg wudqvdvuhg lqwr pruh wkda iruw odajxdjvh, dag wkh prvw uhfhqwr ri klv pdq lqwhuq dnlrqdo krxpxuv lv wkh Mhuxvdohp Sulch, zkrvh suhylvxv uhflslhqv lqfoxgh M.P. Frhwchh, Plodq Nxqghud, dag Y.V. Qdlsxo.
Key 3: Jctwmk Owtmcoq ycu datp kp Maqvq kp 1949 cpf pay nkxgu pgct Vqmaq. Jg ku vjg cwtjat qh ocpa paxgu cu ygnn cu uqjtv uvqtgu cpf pag-hkevkap. Jku yatmu kpenwfg Pqtygikcp Yqaf, Vjg Ykpf-Nr Dktf Ejtqkeng, Mchmc qp vjg Ujstg, Chvgt Fctn cpf Vjev K Vcm Cdoav Vjgo K Vcm Cdoav Twqkpi. Jku yatmu jcu dggp vtcupncvgf kpva oqgt vjcp hqtva ncplwgu, cpf vjg oqgu tegpvp qh jku ocpa kpvgtp cwkapan jppqku ku vjg lgtwengo Rtkbg, yjauv ntkpkwa tgekrkpvu kpenwfg L.O. Egvbgs, Oknep Mwfftc, cpf X.U. Pckrcw.
Key 4: Ibsvlj Nvablnj xbt cpso jo Lzup jo 1949 boe opx mjwft ofbs Uplz. If jt uif buvils pg nbzo opwmt bt xfm bt tipsu tupsjft boe opo-gjdujpo. Ijt xpslt jodmvef Opaxfhjbo Xppe, Uif Xjoe-Vq Cjse Dispojdmf, Lbgbl po uif Tipsf, Bgufs Ebal boe Xibu J Ublm Bcpvu Xifo J Ublm Bcpvu Svoojoh. Ijt xpsl ibt cffo usbotmbufe joup npsf uibo gpusz mbobvhft, boe uif nptu sfdfou pg ijt nbzo jousfo Bujpoom Ippovst jt uif Kfsvbmfn Qsajf, xiptf qsfvdjvt sfdaifout jodmvef K.N. Dpfauff, Nmjob Lvofesb, boe W.T. Objgbvm.
Key 5: Haruki Murakami was born in Kyoto in 1949 and now lives near Tokyo. He is the author of many novels as well as short stories and non-fiction. His works include Norwegian Wood, The Wind-Up Bird Chronicle, Kafka on the Shore, After Dark and What I Talk About When I Talk About Running. His work has been translated into more than forty languages, and the most recent of his many intern ational honours is the Jerusalem Prize, whose previous recipients include J.M. Coetzee, Milan Kundera, and V.S. Naipaul.
Key 6: Gzqtjh Ltqzjzh vzr anqm hm Jxnan hm 1949 zmc mnv khudr mdzq Snjxn. Gd hr sgd ztsqng ne lzmz mnudkr zr vdkk zr rgnqs rsqndhr zmc mnm-ehbshnm. Ghr vnqjr hmbkted Mnavdfhm Vnnc, Sgd Vhmc-To Ahqc Bgqnmhbk, Jzejj nm sgd Rgnqd, Zesdq Czaj zmc Vgzs H Szkj Zants Vgdm H Szkj Zants Qtmhmff. Ghr vnqj gsr addm sqzmksdc hsmn lndq szgm enqxs kzmtzfdr, zmc sgd lnsr qdbdms ne ghr lzmz hmsdqm zshnmzk gnmntqr hr sgd Idqtrzkdl Qahdy, vgnrd oqdunhtr qdbhohdmsr hmbkted I.L. Bndsydd, Lhkzm Jtmdqz, zmc U.R. Mzhoztk.
Key 7: Fypsig Kspykig yqz zmpl gl Immm gl 1949 ylb lmu jgtcq lcyo Rmiwm. Fc qg rfc yarfm md kylv lmtcjq yq ucjj yq qfmr qrmqpcq ylb lml-dgargml. Fga umpiq glajsbz Lmpucegyl Umbb, Rfc Ugib-Sn Zgpb Afpmlgajc, Iyidi ml rfc Rfmpc, Ydrpc Bypj ylb Ufyrr G Ryji Yzmsr Ufcl G Ryji Yzmsr Pallgle. Fga umpi fyq zcel rpylqjyrcb glrm kmcp rfyl dmpw jylesyeca, ylb rfc kmqr pcalir md fga kylv glrcpl yrgmlyl fmlmcp qg rfc Kcpagjck Npvc, ufmc nptcmsa pcagngclrq glajsbz H.R. Amvccc, Kqjyl Islbpy, ylb T.Q. lyngysj.
Key 8: Exonhfr Jroxvixr exp ylok fx Hwld Fk 1949 xka xlt ifsbp kxvo Qhylv. Eb fp qeb xrgelo lc jxkv klslbp xp tbiu xp palog palofpb xka Klk-cfzqflk. Efp tlloh Fkzirab Klotbdfk Tlla, Qeb Tfka-Rm Yfoa Zeolkrzib, Hxchx lk qeb Pelob, Xcabo Axoh xka Texq F Qxih Xylrq Tabk F Qxih Xylrq Onkkfkd. Efp tlloh exp ybbk opxkpxaba fkl jlob qexk cloqv ixkdrxadb, xka qeb jlpa obzbq lc efp jxkv fkbok xqfklxi elkrop fp qeb Bhorpxibj Mofoib, telb mbsflrp obzfmfbkq Fkzirab G.J. Zlbqbb, Jfivk Hrkabox, xka S.P. Kxfmari.
Key 9: Damage Iqmwde awo xinj ej Gukpk ej 1949 wjz jks herao jawm Pkguk. Da eo pda wopdkn kb iwxu jkraho wo sahh wo odknp opkneao wjz jkj-bayepkj. Deo skngo ejyhqza Jknsacewj Skkz, Pda Sejj-Ql Xenz Ydnkneyha, Gwbgv kj pda Odkna, Mopan Zung wjz Sdwp E Pwhg Wkxqp Sdaj E Pwhg Wkxqp Najjejc. Deo skng dwo xaa pwnjohwpez ejkp ikna pdw bknpw hwjqcwao, wjz pda ikop nayaip kb deo iwxu ejpanj wpekjhv dkjqpno eo pda Fangowhai Lneva, sdkoa lnarekpo nayeiajpo ejyhqza F.I. Ykapaa, Iehwj Gajzanw, wjz R.O. Jwelwqh.
Key 10: Cvmppf Hpmfvfhd rvn wjmi di Ftjoj di 1949 vjy ijr gdqzn izvm Ojftj. Cz dn ocz vpcqm ja hvit ljqzgn vn rzgg vn ncjmo nojmdzn vjy iji-adoxdi. Cdn rjmfnd dixgpyz Ijmrzbavi Rjjy, Ocz Rdiy-Pk Wdmv Xcmjdgz, Fvafv ji ocz Ncjnz, Vaozm Vvmf vjy Revd F Ovgf Vwjo Rczl D Ovgf Vwjo Mpidib. Cdn rjmf enw czvzi omvingvozy dioj hjmz ocvi ajmot gvibpvbzn, vjy ocz hjo mzxzio ja cdn hvit diozm ivodjlv cijjmn dn ocz Ezmpvngzh Kmduz, rcjnz kmzqdjpn mxzdkdzion dixgpyz E.H. Xjzouzz, Hdqvi Fpizymv, vjy Q.N. Ivdkvpg.
Key 11: Buloc Goluegc qum vllh ch Esini ch 1949 uhx hia fcpym hyul Niesi. By cm nby unobil iz guhs hifpm um qyff um mbilin mnilcym uhx hin-zwncih. Bcm gilem chwfoxy Hilqyacuq Qixx, Nby Qchx-Oj Vclx Mblihcwfy, Euzeu ih nby Mbily, Uznyl Xule uhx Qbun C Nufe Uvion Qybh C Nufe Uvion Lohhca. Bcm gile bum vvyh nluhfumyx chni gily nbuh zilns fuhaouaym, uhx nby giml luywih iz bcm guhs chnyl hunchuf bihiolm cm nby Dylomufy Jlcly, qbimy jlypciom lywcjcyhnm chwfoxy D.G. Winynty, Gefuh Eohxlyu, uhx P.M. Hucjuof.
Key 12: Atknd Fnktdfrb ptl uhkg bg Drmh 1949 tgv ghp ebowl gxtk Mndrh. Ax bl max tnmahk hy ftrg ghoxel tl pxeel tl lahm Imhixl tgv ghg-ybvmhg. Abl phkdl bgvenwx Ghkpxzbtg Phhw, Max Pbgv-Ni Uokv Vahghvex, Dlydt hg max Lahkx, Tyxmk Htkd tgv Patn B Hted Tuhm Pang B Hted Tuhm Kngbgz. Abl phkdl uli uwxg mktpletmxw bgmh fhkx yatg yhmtr etgntzxl, tgv max fhlm kxvaxg hy abl ftrg bgmxk gtmhgte ahghkbl bl max Cxkntwefr Ikbx, pahk ikxobhnl kxvibvngl bgvenwx C.F. Vmoxsxx, Fbstg Dngwakt, tgv O.L. Gbitne.
Key 13: Czjsa Emsjcsa oak tgif af Cqgl af 1949 svf fgo danek fhwj Lmgw. Zw ak lzmz szgjj gx esqf fgmwk ak owdd sk kzgjl klgiaw sfv ffg-xaulagf. Zak ogjck afudmw Fgjoayaf Oggy, Lzw Garv-Mh Tajv Uzjgfaudw, Cxcsx gf lzw Kzggj, Sklaj Vajc sfv Oszl A Lsdc Stgml Ozwf A Lsdc Stgml Jmffaay. Zak ogjc zsk twof ljefkdlaw afg egjw lzsf xgjlq dsfymywk, sfv lzw egkl jwuwlfx gx zak esqf aflwj falfesdf zefemk ak lzw Bymkdswe Hianv, ozrkx hnmnmk iwhnhwflk afudmw B.E. Uvulwv. Edsdf Cnfvyia, sfv N.K. Fshsmd.
```

The correct is 5

Task 4:

1. Convert the key to uppercase, replace “J” with “I,” and combine it with the alphabet to build a unique 5×5 matrix.
2. Remove spaces and non-letter characters from the plaintext, pad it if necessary, then split it into pairs.
3. For each pair, locate their positions in the matrix and apply Playfair cipher rules to encrypt or decrypt (adjusting columns, rows, or performing a rectangle swap).
4. Return or print the resulting encrypted or decrypted text.

```
Enter the key: K
Enter the plain-text to encrypt: IE105 UIT N15 Long Long Phuong

Playfair Matrix:
K A B C D
E F G H I
L M N O P
Q R S T U
V W X Y Z

Encrypted Message: EFZPSOMPSNMPSNOITPSN
Decrypted Message: IEUITNLOGLONGPHUONG
```

Task 5:

1. Define generate_key function to extend the key to match the message length.
2. Define encrypt function to encrypt the message using the Vigenere cipher.
3. Define decrypt function to decrypt the encrypted message using the Vigenere cipher.
4. Set the message and key variables with example values.
5. Generate the extended key using generate_key.
6. Encrypt the message using the encrypt function.
7. Decrypt the encrypted message using the decrypt function.
8. Print the original message.
9. Print the encrypted message.
10. Print the decrypted message.

```
Encrypted Message: PVAMC UE PEATKCTBNBG MLGBA YD3C EHWASA TJHEFUDMKCR NAGGINZI WM YECQVAB AGL QXGJRNH R BTDCGX IFBRY TMAVNTGP EIIPSE. LXQH POJG IRPEQQWMMGG PS A BPAUAZH JBXZ YH CEPHE 100 KBKHK Y
BX A ZPG OY OOHYL 10-20 APBVEKA. MLWG JYIUIJ BJE ZSFNPL UAWY DISMT VZMCHSVKYDRP IDZTU
Decrypted Message: WRITE AN APPLICATION USING YOUR CHOSEN PROGRAMMING LANGUAGE TO ENCRYPT AND DECRYPT A MESSAGE USING VIGENERE CIPHER. TEST YOUR APPLICATION BY A MESSAGE WITH AT LEAST 100 WORDS A
ND A KEY OF ABOUT 10-20 LETTERS. THEN VERIFY THE RESULT WITH OTHER CRYPTOGRAPHY TOOLS
```

Task 6:

```
\extensions\ms-python.debugpy-2024.12.0-win32-x64\bundled\libs\d
Decoded message: Welcome to Crypto Island!!!
PS C:\Users\Duck Triton Predator\Desktop\Project\IE105\Lab3> █
```

1. Defines a list ascii_codes containing ASCII integer values.
2. Converts each integer to its corresponding character using chr(code).
3. Joins all characters into a single string decoded_message with ".join(...).
4. Prints the message "Decoded message:" followed by the decoded string.
5. Outputs the human-readable message represented by the ASCII codes.

Task 7.1:

```
Plaintext: HELLO WORLD
Key: KEY
Encrypted: RIJVS GSPVH
Decrypted: HELLO WORLD
```

Vigenère cipher for encrypting and decrypting messages. The process involves the following steps:

1. **Key Generation:** The generate_key function extends the given key to match the length of the message by repeating its characters.
2. **Encryption:** The encrypt function shifts each character of the message based on the corresponding character in the key. Letters are shifted alphabetically (considering case), while non-alphabetic characters remain unchanged.

3. Decryption: The decrypt function reverses the encryption process by shifting the characters back using the key.

Finally, the main function demonstrates the process by encrypting and decrypting the message "HELLO WORLD" using the key "KEY". It prints the original plaintext, the key, the encrypted ciphertext, and the decrypted text to verify correctness.

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này



YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File **.DOCX và .PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).
Ví dụ: [NT101.K11.ANTT]-Exe01_Group03.
- Nếu báo cáo có nhiều file, nén tất cả file vào file **.ZIP** với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm bài nộp.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

Bài sao chép, trể, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT