# CP3404 Assignment

SP2, Townsville & Cairns (2018)

**Due by Friday October 19, 2018 (no later than 5:00pm)**

---

**Aim:** This assignment is designed to help you improve your critical thinking and problem solving skills, as well as your information literacy skills (i.e. the ability to select and organise information and to communicate it effectively and ethically).

**Requirements, Method of Submission, and Marking Criteria:**

- Answer all of the following questions in a single document. Each question should begin on a new page.
- For each of the first four (4) questions, write a report of approximately 750 words in the structure of a scientific paper.
- Include your name on the first page. Include list of references for each question with proper in-text citations.
- For marking criteria of the first 4 questions, see the included rubric.
- In your answer to question 5 (i.e., cryptanalysis), show all your work. Five (5) marks are assigned to the determination of the correct keyword, and five (5) marks to the determination of the complete plaintext (partial marks count).
- Upload your solution to the Assignment Box, located in the subject's site.

1. **Security + Certification Jobs**
   What types of jobs require a Security+ certification? Using online career sites such as monster.com, careerbuilder.com, jobfactory.com, and others, research the types of security positions that require a Security+ certification. Create a table that liststhe employer, the job title, a description of the job, and the starting salary (if these items are provided).

   [5 marks]

2. **One-Time Pad (OTP) Research**
   Use the Internet to search OTPs; who was behind the initial idea, when they were first used, in what application they were found, how they are used today, etc. Then visit an online OTP creation site such as www.braingle.com/brainteasers/codes/onetimepad.php and practice creating your own ciphertext with OTP. Exchange your OTPs with other students to see how you might try to break them. Would it be practical to use OTPs? Why or why not? Write a short paper (approximately, 750 words) on your findings.

   [5 marks]

3. **Bring Your Own Device (BYOD) Policy**
   Use the Internet to locate BYOD Policy from two different organizations. After reading that information, create your own BYOD policy for your school or place of employment. What restrictions should be enforced? What control should the organization have over the personal devices?

   Write a short (approximately 750 words) report on your research.

   [5 marks]

4. **Open Authentication (OAuth)**
   Use the Internet to research OAuth. What is the technology behind it? What are its strength? What are its weaknesses? Will it replace OpenID? Would you recommend it for secure applications like online banking?

   Write a short (approximately 750 words) report on your research.

   [5 marks]

5. **Cryptanalysis of Substitution Ciphers:**
   In this question you learn a classical monoalphabetic (substitution) cryptographic system, and are required to cryptanalysis a given cryptogram.

   In substitution ciphers, a permutation of the alphabet is chosen as the cryptogram of original alphabet. That is, every letter of the plaintext substitutes by corresponding letter in the permuted alphabet. For example,

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
c o d k s z r g e l u y a f m v p h i n w t b j q x
```

   Figure 1: A possible permutation of English alphabet

   is one of such permutation, in which letters $a, b, c, \cdots, y, z$ from the plaintext are substituted by corresponding letters $c, o, d, \cdots, q, x$ respectively. Since remembering permutation is not easy, one may employ a **keyword** and use a table to generate the permuted alphabet. Let CRYPTOGRAPHY be the keyword. The permuted alphabet can be obtained as follows.

   - Choose a $6 \times 5$ table/matrix, i.e., a table with 6 rows and 5 columns.
   - Write down the secret keyword in cells $(1,1), (1,2), \cdots$, one letter in each cell, but skip repeated letters. Figure 2 shows how 'CRYPTOGRAPHY' (as a keyword) written down in the table.
   - Write alphabet letters (in order) from the first available cell after keyword, but skip all letters that are already written in the table. You will come out with Table 3.
   - The permuted alphabet, which will be used to generate the cryptogram, can be obtained by simply reading the content of Table 3 in columns order (see Figure 1).

   **Your Task:**

   Cryptanalysis of an information system is *the study of mathematical techniques for attempting to defeat information security services.*

| | | | | |
|---|---|---|---|---|
| C | R | Y | P | T |
| O | G | A | H | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Figure 2: CRYPTOGRAPHY is the Keyword

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

Figure 3: Table for permuting alphabet

A cryptographic system is said to be *breakable* if a third party (i.e., cryptanalyst), without prior knowledge of the key, can systematically recover plaintext from corresponding ciphertext within an appropriate time frame.

In this question, you are required to determine the plaintext and the keyword associated to the given cryptogram. Note that brute force attack (i.e., searching all possible keys) in order to find the keyword is not efficient. However, letter frequency (see Figure 4) attack is an efficient tool for breaking substitution ciphers.

In the following you can find 10 cryptograms, where the breaks are genuine breaks between English words. You are required to decipher the cryptogram that matches with your Student-ID.

[10 marks]

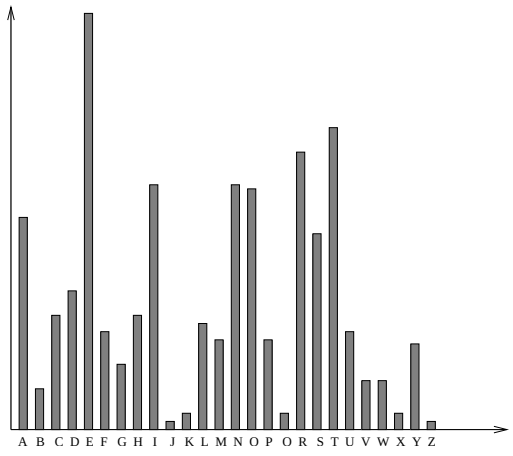


Figure 4: Letter frequency in English texts

### Cryptogram for whom their Student-ID is XXXXXXX0

vehmdrt-uts (dnkq gdnnto ksbbtrehg) gesvrqkskrtbk wkt
rct kdbt ktgetr uts zqe tjgesvrhqj djo otgesvrhqj.
dnrcqwyc rct tjgesvrhqj djo otgesvrhqj utsk oq jqr
jtto rq it hotjrhgdn, rct ujqfntoyt qz qjt qz rctb
kwzzhgtk rq qirdhj rct qrcte. vwinhg-uts (dnkq gdnnto
dksbbtrehg) gesvrqkskrtbk wkt d ohzztetjr uts zqe
tjgesvrhqj djo otgesvrhqj. rct ujqfntoyt qz qjt uts,
cqftmte, oqtk jqr dnnqf rct qrcte rq it otrtebhjto.

### Cryptogram for whom their Student-ID is XXXXXXX1

gq dtj mxgfvrs cutrgyul qatq qau tjjxbwqgph pz th gehpcthq
tqqtfvuc dtj hpq cutrgjqgf. bpjq utcrs uxcpwuth fcswqpjsjqubj
ducu lujgehul qp dgqajqthl qau tqqtfvj pz ulxftqul pwwphuhqj
dap vhud qau uhfcswqgph wcpfujj, nxq lgl hpq vhpd qau
fcswqpectwagf vus. tllgqgphtrrs, gq dtj cumxujqul qatq qau
uhfcswqgph thl lufcswqgph wcpfujjuj fpxrl nu lphu mxgfvrs,
xjxtrrs ns athl, pc dgqa qau tgl pz bufathgftr luigfuj jxfa
tj qau fgwauc lgjv ghiuhqul ns ruph ntqqgjt trnucqg.

### Cryptogram for whom their Student-ID is XXXXXXX2

jupiini, hi uhj jtahipo fnbv, ophl qut qutnbtqhgpo
znxilpqhnij nz anltbi gbswqnrbpwus. ut xjtl hiznbapqhni
qutnbs qn piposjt ghwutbj pil gnijhltbtl qut jn-gpootl
wbnlxgq ghwutbj, fuhgu xjt japoo jxdjqhqxqhni dnktj
gniitgqtl ds opbrtb wtbaxqpqhni dnktj. jxdjqhqxqhni dnktj,
pojn gpootl j-dnktj, pbt gniqbnootl ds p btopqhetos junbq
gbswqnrbpwuhg vts qn wbnehlt gnizxjhni (dtgpxjt nz qut
xivinfi jtgbtq vts).

### Cryptogram for whom their Student-ID is XXXXXXX3

fi phfj wswub, cu lfjdxjj judxbfpq, pbxjp, sil lujfti fjjxuj doipbsjpfit
phu lfzzubuiduj gupcuui nsbfoxj sxdpfoi pqwuj.
cu cfrr jhoc phsp woob lujfti zob si urudpboifd sxdpfoi gbusdhuj phu
judxbfpq oz phu jqjpua sil lutbsluj fpj wbsdpfdsrfpq --io asppub hoc
judxbu uzzfdfuip sbu phu gxfrlfit grodvj oz si urudpboifd sxdpfoi.
zxbphubaobu, cu lfjdxjj s jup oz buexfbuauipj zob wbsdpfdsr
sil judxbu urudpboifd sxdpfoij (iopu phsp srr ukfjpfit fipubiup sxdpfoi
jfpuj hsnu io judxbfpq --iufphub zob phu gflj iob zob phu gfllubj-- sil
pbxjp fj zxrrq wrsdul fi phu sxdpfoiuub, chfdh fj iop sdduwpsgru zboa
bujusbdh wofipj oz nfuc).

### Cryptogram for whom their Student-ID is XXXXXXX4

qat lnqn tigdswqhpi jqnilndl (ltj) fnj qat zhdjq
gpcctdghnm-udnlt cpltdi gdswqpudnwahg nmupdhqac fhqa
pwtims nil zxmms jwtghzhtl hcwmtctiqnqhpi ltqnhmj.
hq fnj ltetmpwtl zdpc mxghztd nil etds jppi rtgnct n
jqnilndl zpd tigdswqhpi hi rnivhiu nil pqatd ipi-chmhqnds
nwwmhgnqhpij. hq xjtj qat jnct zthjqtm jqdxgqxdt
fhqa japdqtd 64-rhq lnqn rmpgvj nil n japdqtd 64-rhq vts.

### Cryptogram for whom their Student-ID is XXXXXXX5

cxfognhi fch eq fuciigzgqk cffnbkghl on orq hxaeqb nz iquuqbi chk orq
achhqb ep drgfr egkkqbi ixeago egki.
ch cxfognh orco rci nhup nhq iquuqb chk achp expqbi
gi bqzqbbqk on ci c ighluq cxfognh.
ch cxfognh dgor achp iquuqbi chk achp expqbi
g.q., c iqfxbgogqi acbvqo) gi bqzqbbqk on ci c knxeuq cxfognh.
egkkghl gh ch cxfognh fch opwgfcuup eq nz odn opwqi:  iqcuqk nb
nwqh.
gh c  iqcuqk egk cxfognh, iqfbqo egki hno vhndh on orq norqb
egkkqbi cbq ixeagooqk on orq cxfognhqqb.
nhfq orq egkkghl wqbgnk funiqi, orq egki cbq nwqhqk chk orq dghhqb gi
kqoqbaghqk cffnbkghl on inaq
wxeugfup vhndh bxuq (q.l., orq rglrqio egkkqb dghi).
gh ch {\qa nwqh egk} cxfognh, egki cbq vhndh on cuu wcbogfgwchoi
orbnxlrnxo chk czoqb orq egkkghl wqbgnk funiqi.

### Cryptogram for whom their Student-ID is XXXXXXX6

seu ulwudhujgu fhse seu cjcmtkhk rz seu puk ociu icmxcnmu
hjkhoesk hjsr seu pukhoj wdrwudshuk rz gdtwsrodcwehg cmordhseak.
carjoks seu acjt pukgujpcjsk rz seu puk, ferku ksdxgsxdu
fck nckup rj zuhksum wudaxscshrj, cdu seu qcwcjuku zcks
ujgdtwshrj cmordhsea (zucm) cjp seu cxksdcmhcj mrvh cmordhsea.

### Cryptogram for whom their Student-ID is XXXXXXX7

ij 1976 pizziu cjp bummecj ijsfrpxhup sbu hrjhuws rz
wxdmih-vut hftwsrktksuek. wxdmih-vut hftwsrktksuek
(cmkr hcmmup ckteeusfih ktksuek) xku sgr pizzufujs vutk;
rju ik wxdmih gbimu sbu rsbuf ik vuws kuhfus. hmucfmt,
is ik fuaxifup sbcs hrewxsijo sbu kuhfus vut zfre sbu
wxdmih rju bck sr du ijsfchscdmu. ij 1978 sbfuu pukiojk
dckup rj sbu jrsirj rz wxdmih-vut ktksuek gufu wxdmikbup.

### Cryptogram for whom their Student-ID is XXXXXXX8

bftuhq, hornfb rgk rklunrg hopcuk opc qou zrdqpbfhrqfpg
wbpilun dpxlk iu xhuk qp dpghqbxdq r wxilfd-vus
dbswqphshqun (qofh fh qou cull-vgpcg bhr dbswqphshqun).
nubvlu rgk oullnrg xhuk qou vgrwhrdv wbpilun fg qoufb
dpghqbxdqfpg. ndulfudu ixflq r hshqun cofdo rwwlfuk
ubbpb dpbbudqfge dpkuh. lrqub fg 1985, ulernrl kuhfeguk
r wxilfd-vus dbswqphshqun xhfge qou kfhdbuqu lperbfqon
wbpilun. nfllub rgk vpilfqy hxeeuhquk xhfge ullfwqfd
dxbtuh qp kuhfeg wxilfd-vus dbswqphshqunh.

### Cryptogram for whom their Student-ID is XXXXXXX9

tigcsvqhpi hj qat vchbhqhet gcsvqplcfvahg pvtcfqhpi
xjtm qp tijxct jtgctgs pc gpizhmtiqhfohqs pz hizpcbfqhpi
qcfijbhqqtm fgcpjj fi xijtgxctm gpbbxihgfqhpi gafiito.
qat tigcsvqhpi pvtcfqhpi qfutj f vhtgt pz hizpcbfqhpi,
fojp gfootm btjjflt pc vofhiqtkq, fim qcfijzpcbj
hq hiqp f gcsvqplcfb pc ghvatcqtkq xjhil f jtgctq
gcsvqplcfvahg uts. mtgcsvqhpi hj qat ctetcjt pvtcfqhpi
qp tigcsvqhpi. qat ctgthetc dap apomj qat gpcctgq jtgctq
uts gfi ctgpetc qat btjjflt (vofhiqtkq) zcpb qat
gcsvqplcfb (ghvatcqtkq).

CP3404 Assignment Rubric

| Criteria | Exemplary (9, 10) | Good (7, 8) | Satisfactory (5, 6) | Limited (2, 3, 4) | Very Limited (0, 1) |
|---|---|---|---|---|---|
| **Title 5%** | - Informative and summative in an excellent way<br>- contains most keywords<br>- Intriguing and thought-provoking in an excellent way | Exhibits aspects of exemplary (left) and satisfactory (right) | - Too long or too short<br>- Partially informative or summative<br>- Partially intriguing and thought-provoking | Exhibits aspects of satisfactory (left) and very limited (right) | - Too long or too short<br>- Hardly informative or summative<br>- Contains no keyword<br>- Hardly intriguing and thought-provoking |
| **Abstract 10%** | - Excellent summary of contents containing problem statement, approach, and result | | - Satisfactory summary of contents containing some of problem statement, approach, and result | | - No or very limited abstract |
| **Structure 15%** | - Highly appropriate structure and professional format, according to the genre/text type and task requirements, including clear attention to word length limit, and effective use of sections, paragraphs and/or links | | - Largely appropriate structure and format, according to the genre/text type and task requirements, including attention to word length limit, and use of sections, paragraphs and/or links | | - Inappropriate structure and format, according to the genre/text type and task requirements, with no/limited attention to word length limit, and use of sections, paragraphs and/or links |
| **Content 35%** | - Identifies, explains and prioritises key issues in a complex IT related situations, drawing upon relevant theory and real or hypothetical examples.<br>- Demonstrates clear mastery of the material in the topic area, and shows excellent ability to synthesise and abstract knowledge | | - Identifies and explains key issues in a routine IT related situations.<br>- Demonstrates moderate mastery of the material in the topic area, and shows moderate ability to synthesise and abstract knowledge | | - Demonstrates little mastery of the material in the topic area, and shows no ability to synthesise and abstract knowledge |
| **Readability 25%** | - Excellent progression of topics<br>- A highly conventional academic writing style, including the use of appropriate terminology and unbiased language | | - Satisfactory progression of topics<br>- A largely conventional academic writing style, including the use of appropriate terminology and unbiased language | | - Unsatisfactory progression of topics<br>- Unclear explanation for all concepts |
| **Referencing 10%** | - Adheres to IEEE referencing conventions in in-text citation, presentation of tables/figures and reference list, with next-to-no errors | | - Mostly adheres to IEEE referencing conventions in in-text citation, presentation of tables/figures and reference list, with some errors | | - No referencing or very limited use of references |