1. Break the following cipher. It is a mono-alphabetic substitution cipher, in the English language. Hint: compute the letter frequencies.

JXAJQHQXQHIP I Pnte B JHIROT OTQQT E JHDVOT JXAJQHQXQHPI GBI AT

LTDPIJQEBQTL AS FEHQHIR PXQ QCT BOVCBATQ HI JPDT PELTE QP ETVETJTIQ

QCT JXAJQHQXQHIP. QCHJ HJ QTEDTL B JXAJQHQXQHIP BOVCBATQ. QCT GHVCTE

BOVCBATQ DBS AT JCHZQTL PE ETNTEJTL (GETBQHIR QCT GBTJBE BIL BQABJC

GHVCTEJ, ETJVTGQHNTOS) PE JGEBDAOTL HI B DPET GPDVOTK ZBJCHPI, HI

FCHGC GBJT HQ HJ BOOTL B DHKTL BOVCBATQ PE LTEBIRTL

BOVCBATQ. QEBLHQHPIBOOS, DHKTL BOVCBATQJ BET GETBQTL AS ZHEJQ FEHQHIR

PXQ B UTSFPEL, ETDPNHIR ETVTBQTL OTQQT EJ HI HQ, QCTI FEHQHIR BOO QCT

ETDBHIHIR OTQQT EJ HI QCT BOVCBATQ.
2. A common method of generating mono-alphabetic substitution ciphers is by using a pass-
word, as follows. Write the password horizontally, omitting any duplicate appearance of
letters. Then write under the password all the remaining letters of the alphabet. Read off
the substitution alphabet vertically. E.g., if the password is FOOTBALL:

FOOTBAL
CDEGHI
JKMNPQ
RSUVWX
YZ

and the resulting substitution is

Plaintext letters: abcdefghijklmnopqrstuvwxyz
Ciphertext letters: FCJRYODKSZTEMUBGNVAHPQLX

The cipher of question 1 was generated this way. What was the password? Hint: write
the substitution alphabet you broke in q.1 ordered by the plaintext letters, then look for
sequences of consecutive letters in “hops”. E.g., in the example above the letters C,D,E
appear in positions 2, 7, 12, with a hop of 5.

3. Encrypt your name using the cipher you broke in q.1.

Submission Instructions

1. Send your results via email to crypto-netsec@eng.tau.ac.il. That’s a dash (“-”), NOT
an underscore (“_”).

2. The subject should be: ex1

3. The body of the email should contain 4 lines, including the leading keywords and the “:=”
symbols:

TZ := your "Teudat Zehut" number (9 digits)
Q1 := the last line of decoded text from question 1 here ...
Q2 := the password you broke in question 2 here ...
Q3 := your name, encrypted as in question 3.

4. Send plain ASCII email. In particular:

(a) No attachments
(b) No HTML email: configure your mail program to generate “unformatted” or “Plain
text” messages only (not “Rich formatting”)
(c) Be extra careful with Outlook which by default sends the text encapsulated in an at-
tachment called “winmail.dat”. A recipe on how to fix this can be found in http://facstaff.gpc.edu/~jbenson/resource/winmail.htm (scroll all the way down)
(d) When in doubt, use a Unix text-based mailer like “mail” or “pine”.

2