Date: Wednesday, January 23, 2002
Lecturer: Dr Jean-Yves Chouinard
Office: Colonel-By Hall, room A-610

ELG-5373 Secure Communications and Data Encryption

Assignment #1 (due on Monday, February 4, 2002 at the beginning of the lecture.)

Question 1: *(language redundancy)*

Problem 1.1 from the course notes.

Question 2: *(monoalphabetic cipher)*

Problem 2.3 from the course notes.

Question 3: *(Vernam cipher)*

Problem 2.5 from the course notes.

Problème 4: *(cryptanalysis of a substitution cipher)*

Decrypt the following cipher:

$C =$

YUAYWFEATSSLOJWSNNPGXSKYJFQEVOFIAWJTCWNSYVKULMNPJSSYAHVYBYVJW
RHHLJQOJSYGAYASTPOWZFQHDFFOBEUGEVFNFPOSYCQSKJFWYJNIEUYFGZPXKR
NLFYQASSDFWYWSBPJGWEASSYRZOGBRRLJNGEZHTFOPTQRPOSYGSVOFIAZONGD
KAKSAYWSGBHJKVASVWRBSWHGKYKMNRLLMROHEJYKJSQEAMDJPPVJXPWBKNACA
ZJSWKASTPVTJPKYJJYWAWIGDPKNFIVJJYERWQLEUMWOWUSWRWZOMRNLLMRZPK
YEEIMYVKUGKNJNDJFKMSWEECSQVOVXYRJSARVPLVFGWNAARJAARRZBWYBPOWU
EAZWSPAVXGHESVNACZSQFKAZJRMBAANHLFYCQSKJNPAZJEAJWNIAYKNALBLMN
OHDNZEAWIEAZGQHPPGSQQLLTSESLJEEUYNAWTMQGEWSYUAUNNEKUEJAPAZNFI
HQQRWKLTCWYLNNHWMQFAVNJEHHHBVPOSHBNYWXCKUVNACSGXFEUVNIAYKNGUP
FLRJLJFYPOWXRPDGUUAUGRRJHSWREUVNPWAATAOAZFGPOWIVRLJXVPFGWQAYS
YGDLJJPAPNJEOPFUHPTSDOAKAKSAYWSGPOSSGDLFZZXLJTSNLKTYRHTQRLBDX
ROPFYUAHNJEWNWUBSLJIRHHQUEKMAQRBYGRNZLLJPPPGSCKPFYBBCAJJPOWHB
NYWQNPPGSCDLFTZAUGSVOVXNAPLJJFPVFQLSOWSNYLJYNEUDJIASAXEAHUMRZ