Departemen Teknik Informatika
Institut Teknologi Bandung

Tugas I IF5054 Kriptografi
Kriptanalisis Sederhana

Batas pengumpulan : Senin, 19 September 2005, paling lambat jam 16.00
Tempat pengumpulan : Lab IRK (di atas loker)
Berkas pengumpulan : Kertas A4
Deskripsi tugas :

Seseorang mengirimkan dokumen kepada anda, tetapi sayangnya ia mengenkripsi dokumen dalam bahasa Inggris tersebut menjadi chiperteks dengan **metode Substitusi sederhana** (mungkin dia tidak infin dokumen tersebut dibaca oleh orang lain, eksklusif buat anda saja). Pada proses enkripsi ini, orang tersebut hanya mengubah karakter abjad (a..z). Huruf kapital diubah ke huruf kecil sebelum dienkripsi. Karakter lain (angka, spasi, koma, titik, dan lain-lain) tidak dienkripsi. Setiap paragraf dienkripsi dengan kunci yang berbeda.

Anda sebagai penermia dokumen tentu harus **mendekripsi** chiperteks tersebut menjadi plainteks, sayangnya teman anda itu lupa memberitahukan kunci yang ia pakai pada waktu enkripsi. Anda sekarang berlaku sebagai seorang kriptanalisis yang menggunakan **metode Statistik** dan metode terkaan untuk mendekripsi dokumen. Anda diperbolehkan mengggunakan kakas bantu (coretan kertas, aplikasi Ms Excel, maupun membuat program kecil sederhana untuk menghitung frekuensi kemunculan karakter atau ntuk keperluan lainnya) untuk menyelesaikan masalah ini.

Yang dikumpulkan adalah: laporan yang berisi
a. Berkas cipherteks
b. Langkah-langkah yang anda lakukan dalam melakukan dekripsi
c. Plainteks hasil dekripsi

Pembagian tugas :

Kelompok	Arsip
1	`cipher1.txt`
2	`Cipher2.txt`
3	`cipher3.txt`
4	`cipher4.txt`
lainnya	`CipherX.txt` X = nomor_ kelompok **mod** 4

Selamat mengerjakan!

LAMPIRAN

(soft copynya dapat di-*download* dari http://www.informatika.org/~rinaldi)

cipher1.txt

```
mjymuzujuzkd wznsgam

zd mzbnqg mjymuzujuzkd wznsgam, x nxauzwjqxa qguuga ka mebykq zm
mjymuzujugi cka gxws qguuga. usg qguugam xag mjymuzujugi zd usgza dkabxq
kaiga, jmjxqqe rzus dkabxq rkai izozmzkdm. mjws wznsgam xag agwktdzlgi ye
usg kwwjaagdwg kc x mgu kc dkabxq qguuga caghjgdwzgm xuuxwsgi uk usg rakdt
qguugam. usge xag mkqogi ye jmzdt caghjgdwe xdxqemzm xdi ye dkuzdt usg
wsxaxwugazmuzwm kc nxauzwjqxa qguugam, mjws xm usg ugdigdwe uk ckab
ikjyqgm, wkbbkd rkai nagczvgm xdi mjcczvgm, wkbbkd czamu xdi qxmu qguugam
zd rkaim, xdi wkbbkd wkbyzdxuzkdm, mjws xm hj, us, ga, xdi ag.

x mjymuzujuzkd wznsga zm ngackabgi ye agkaigazdt usg qguugam zd usg
xqnsxygu. cka gvxbnqg, x wznsga igozmgi qkdt xtk ye fjqzjm wxgmxa mszcum
xqq usg qguugam zd usg xqnsxygu ye usagg nqxwgm. usjm, rsgd usg qguuga x zm
dggigi, x i zm jmgi, xdi rsgd x y zm uk yg razuugd, xd g zm jmgi. usg
qguugam raxn xakjdi xu usg gdi kc usg xqnsxygu. mk, zc x ngamkd rxdum uk
gdwznsga x l, zu zm razuugd xm x w. mzbzqxaqe, x e zm razuugd xm x y. usg
gduzag wznsga zm agnagmgdugi ye urk akrm kc qguugam. usgmg akrm xag wxqqgi
x qkkpjn uxyqg.

rszqg usg xykog mjymuzujuzkd wznsga zm gxme uk agbgbyga, zu zm xqmk gxme uk
yagxp. uk bxpg x mjymuzujuzkd wznsga bkag wkbnqgv, bjquznqg mjymuzujuzkdm
xdi mkbguzbgm gogd djbygam xag xiigi uk usg wznsga.

zd bjquznqg-mjymuzujuzkd (nkqexqnsxyguzw) wznsgam, x pgerkai ka djbyga zm
gbnqkegi. usg czamu bgmmxtg qguuga bztsu yg gdwznsgagi ye xiizdt uk zu usg
djbgazwxq oxqjg kc usg czamu qguuga kc usg pgerkai; usg mgwkdi bgmmxtg
qguuga zm gdwznsgagi mzbzqxaqe, jmzdt usg mgwkdi qguuga kc usg pgerkai, xdi
mk kd, agngxuzdt usg pgerkai xm kcugd xm dgwgmmxae uk gdwznsga usg rskqg
bgmmxtg. rsgd xiizdt usg djbgazwxq oxqjg kc x pgerkai qguuga uk x bgmmxtg
qguuga, kdg muxaum wkjduzdt rzus usg bgmmxtg qguuga. usjm, uk gdwznsga usg
rkai ukixe ye usg wkig rkai izt, u ygwkbgm r, xm i zm usg ckjaus qguuga kc
usg xqnsxygu (wkjdu u, j, o, r); k ygwkbgm r, xm z zm usg dzdus qguuga kc
usg xqnsxygu; xdi i ygwkbgm f, xm t zm usg mgogdus qguuga kc usg xqnsxygu.
cka usg agmu kc usg bgmmxtg usg wkig rkai zm agngxugi, xdi usjm ukixe zm
wkigi rrfit.

ye jmzdt wkbyzdxuzkdm kc usg yxmzw uengm kc wznsgam, wznsgam wxd yg wagxugi
uk oxazkjm igtaggm kc wkbnqgvzue. usg pge, skrgoga, mskjqi yg gxme uk
agbgbyga ka agnakijwg, cka rzuskju zu usg wznsga zm dk qkdtga x bgmmxtg yju
x njllqg. tzogd mjcczwzgdu uzbg xdi bxugazxq, bkmu wznsgam wxd yg mkqogi
xdi usgza pgem izmwkogagi, yju cka x nxauzwjqxa njankmg usg wkbnqgvzue dggi
yg kdqe mk tagxu xm uk kyuxzd usg qgogq kc mgwjazue igmzagi. bzqzuxae
kaigam usxu bjmu yg pgnu mgwagu cka kdqe x cgr skjam, cka gvxbnqg, wxd yg
gdwaenugi zd x wznsga usxu rkjqi yg gduzagqe jdmjzugi cka iznqkbxuzw
agnkaum jmzdt x wznsga koga xd gvugdigi ngazki kc uzbg.
```

Cipher2.txt

waenuktaxnse, xau xdi mwzgdwg kc nagnxazdt wkigi ka nakugwugi wkbbjdzwxuzkdm zdugdigi uk yg zdugqqztzyqg kdqe uk usg ngamkd nkmmgmmzdt x pge. waenuktaxnse (taggp paenukm, "mgwagu"; taxnskm, "razuzdt") agcgam ykus uk usg nakwgmm ka mpzqq kc wkbbjdzwxuzdt zd ka igwznsgazdt mgwagu razuzdtm (wkigm, ka wznsgam) xdi uk usg jmg kc wkigm uk wkdogau wkbnjugazlgi ixux mk usxu kdqe x mngwzczw agwznzgdu rzqq yg xyqg uk agxi zu jmzdt x pge (mgg gdwaenuzkd). waenuktaxnsgam wxqq xd kaztzdxq wkbbjdzwxuzkd usg wqgxaugvu ka nqxzdugvu. kdwg usg kaztzdxq wkbbjdzwxuzkd sxm yggd mwaxbyqgi ka gdwznsgagi, usg agmjqu zm pdkrd xm usg wznsgaugvu ka waenuktaxb. usg gdwznsgazdt nakwgmm jmjxqqe zdokqogm xd xqtkazusb xdi x pge. xd gdwaenuzkd xqtkazusb zm x nxauzwjqxa bguski kc mwaxbyqzdt—x wkbnjuga naktaxb ka x razuugd mgu kc zdmuajwuzkdm. usg pge mngwzczgm usg xwujxq mwaxbyqzdt nakwgmm. usg kaztzdxq wkbbjdzwxuzkd bxe yg x razuugd ka yakxiwxmu bgmmxtg ka x mgu kc iztzuxq ixux.

zd zum yakxigmu mgdmg, waenuktaxnse zdwqjigm usg jmg kc wkdwgxqgi bgmmxtgm, wznsgam, xdi wkigm. wkdwgxqgi bgmmxtgm, mjws xm uskmg sziigd zd kusgarzmg zddkwgdu ugvu xdi uskmg razuugd zd zdozmzyqg zdp, igngdi cka usgza mjwwgmm kd ygzdt jdmjmngwugi. kdwg usge xag izmwkogagi, usge caghjgduqe xag gxme uk igwznsga. wkigm, zd rszws nagigugabzdgi rkaim, djbygam, ka mebykqm agnagmgdu rkaim xdi nsaxmgm, xag jmjxqqe zbnkmmzyqg uk agxi rzuskju usg pge wkigykkp. waenuktaxnse xqmk zdwqjigm usg jmg kc wkbnjugazlgi gdwaenuzkd uk nakugwu uaxdmbzmmzkdm kc ixux xdi bgmmxtgm.

ukixe bkmu wkbbjdzwxuzkd qgxogm mkbg pzdi kc agwkaigi uaxzq. cka gvxbnqg, wkbbjdzwxuzkdm koga ugqgnskdg qzdgm, zdwqjizdt cxvgm xdi g-bxzq bgmmxtgm, nakijwg x agwkai kc usg ugqgnskdg djbyga wxqqgi xdi usg uzbg zu rxm wxqqgi. czdxdwzxq uaxdmxwuzkdm, bgizwxq szmukazgm, wskzwgm kc agduxq bkozgm, xdi gogd ckki wskzwgm bxe yg uaxwpgi ye wagizu wxai agwgznum ka zdmjaxdwg agwkaim. gogae uzbg x ngamkd jmgm usg ugqgnskdg ka x wagizu wxai, usg ugqgnskdg wkbnxde ka czdxdwzxq zdmuzujuzkd pggnm x agwkai kc usg djbyga wxqqgi ka usg uaxdmxwuzkd xbkjdu, qkwxuzkd, xdi ixug. zd usg cjujag, xm ugqgnskdg dgurkapm ygwkbg iztzuxq, gogd usg xwujxq wkdogamxuzkdm bxe yg agwkaigi xdi mukagi. xqq kc uszm xbkjdum uk x tagxu nkugduzxq qkmm kc nazoxwe. waenuktaxnse zm kdg ukkq usxu rzqq yg xyqg uk gdmjag bkag nazoxwe. usg xyzqzue uk gdwaenu ixux, wkbbjdzwxuzkdm, xdi kusga zdckabxuzkd tzogm zdizozijxqm usg nkrga uk agmukag ngamkdxq nazoxwe.

waenuktaxnse zm zbnkauxdu cka bkag usxd fjmu nazoxwe, skrgoga. waenuktaxnse nakugwum usg rkaqi'm yxdpzdt memugbm xm rgqq. bxde yxdpm xdi kusga czdxdwzxq zdmuzujuzkdm wkdijwu usgza yjmzdgmm koga kngd dgurkapm, mjws xm usg zdugadgu. rzuskju usg xyzqzue uk nakugwu yxdp uaxdmxwuzkdm xdi wkbbjdzwxuzkdm, wazbzdxqm wkjqi zdugacgag rzus usg uaxdmxwuzkdm xdi mugxq bkdge rzuskju x uaxwg.

Cipher3.txt

wkigm xdi wkigykkpm

x rgqq-wkdmuajwugi wkig wxd agnagmgdu nsaxmgm xdi gduzag mgdugdwgm rzus mebykqm, mjws xm czog-qguuga takjnm, xdi zm kcugd jmgi bkag cka gwkdkbe usxd cka mgwagwe. x nakngaqe wkdmuajwugi wkig wxd tzog x szts igtagg kc mgwjazue, yju usg izcczwjque kc nazduzdt xdi izmuazyjuzdt wkigykkpm—ykkpm kc pdkrd wkigm—jdiga wkdizuzkdm kc xymkqjug mgwagwe qzbzum usgza jmg uk nqxwgm zd rszws usg ykkpm wxd yg gccgwuzogqe tjxaigi. zd xiizuzkd, usg bkag x wkigykkp zm jmgi, usg qgmm mgwjag zu ygwkbgm.

zbxtzdg x wkigykkp rzus urk wkqjbdm. zd usg czamu wkqjbd zm x qzmu kc xqq usg rkaim usxu x bzqzuxae wkbbxdiga wkjqi nkmmzyqe dggi uk jmg uk wkbbjdzwxug. cka gvxbnqg, zu wkduxzdm xqq usg nkmmzyqg tgktaxnszw xagxm zd x agtzkd, xqq nkmmzyqg uzbgm, xdi xqq bzqzuxae ugabm. zd usg kusga wkqjbd zm x qzmu kc nqxzd rkaim. uk wagxug x wkigi bgmmxtg, usg gdwkiga razugm ikrd usg xwujxq bgmmxtg. sg usgd mjymuzujugm rkaim zd usg wkigykkp ye czdizdt bxuwsgm zd usg mgwkdi wkqjbd cka usg rkaim zd usg bgmmxtg xdi jmzdt usg dgr rkaim zdmugxi. cka gvxbnqg, mjnnkmg usg bgmmxtg zm xuuxwp usg szqq xu ixrd xdi usg wkigykkp wkduxzdm usg ckqqkrzdt rkai nxzam: xuuxwp = ygxa, usg = fjzwg, szqq = kaxdtg, xu = wxqgdixa, xdi ixrd = kngd. usg gdwkigi bgmmxtg rkjqi agxi ygxa fjzwg kaxdtg wxqgdixa kngd.

zc usg wkigi bgmmxtg cgqq zduk gdgbe sxdim, usg gdgbe rkjqi pdkr zu rxm zd wkig, yju rzuskju usg wkigykkp usg gdgbe rkjqi sxog dk rxe uk igwaenu usg bgmmxtg. wkigykkpm qkmg mkbg kc usgza oxqjg koga uzbg, skrgoga. cka gvxbnqg, zc usg wkigi bgmmxtg cgqq zduk gdgbe sxdim xdi usg dgvu ixe usg szqq rxm xuuxwpgi xu ixrd, usg gdgbe wkjqi qzdp usg gogdu uk usg wkigi bgmmxtg. zc xdkusga bgmmxtg wkduxzdzdt usg rkai kaxdtg rgag wxnujagi, xdi usg ckqqkrzdt ixe, mkbguszdt gqmg sxnngdgi kd usg szqq, usg gdgbe wkjqi xmmjbg usxu kaxdtg = szqq zm zd usg wkigykkp. koga uzbg, usg gdgbe wkjqi nju uktgusga bkag xdi bkag wkig rkai nxzam, xdi gogdujxqqe waxwp usg wkig. cka uszm agxmkd, zu zm wkbbkd uk wsxdtg wkigm kcugd.

Cipher4.txt

waenuxdxqemzm zm usg xau kc xdxqelzdt wznsgaugvu uk gvuaxwu usg nqxzdugvu ka usg pge. zd kusga rkaim, waenuxdxqemzm zm usg knnkmzug kc waenuktaxnse. zu zm usg yagxpzdt kc wznsgam. jdigamuxdizdt usg nakwgmm kc wkig yagxpzdt zm ogae zbnkauxdu rsgd igmztdzdt xde gdwaenuzkd memugb. usg mwzgdwg kc waenuktaxnse sxm pgnu jn rzus usg ugwsdkqktzwxq gvnqkmzkd kc usg qxmu sxqc kc usg 20us wgdujae. wjaagdu memugbm aghjzag ogae nkrgacjq wkbnjuga memugbm uk gdwaenu xdi igwaenu ixux. rszqg waenuxdxqemzm sxm zbnakogi xm rgqq, mkbg memugbm bxe gvzmu usxu xag jdyagxpxyqg ye ukixe'm muxdixaim.

ukixe'm waenuxdxqemzm zm bgxmjagi ye usg djbyga xdi mnggi kc wkbnjugam xoxzqxyqg uk usg wkig yagxpga. mkbg waenuktaxnsgam ygqzgog usxu usg dxuzkdxq mgwjazue xtgdwe (dmx) kc usg jdzugi muxugm sxm gdkabkjm, gvuagbgqe nkrgacjq wkbnjugam usxu xag gduzagqe igokugi uk waenuxdxqemzm.

usg mjymuzujuzkd wznsgam igmwazygi xykog xag gxme uk yagxp. ygckag wkbnjugam rgag xoxzqxyqg, gvngau waenuxdxqemum rkjqi qkkp xu wznsgaugvu xdi bxpg tjgmmgm xm uk rszws qguugam rgag mjymuzujugi cka rszws kusga qguugam. gxaqe waenuxdxqemzm ugwsdzhjgm zdwqjigi wkbnjuzdt usg caghjgdwe rzus rszws qguugam kwwja zd usg qxdtjxtg usxu zm ygzdt zdugawgnugi. cka gvxbnqg, zd usg gdtqzms qxdtjxtg, usg qguugam g, m, u, x, b, xdi d kwwja bjws bkag caghjgduqe usxd ik h, l, v, e, xdi r. mk, waenuxdxqemum qkkp xu usg wznsgaugvu cka usg bkmu caghjgduqe kwwjaazdt qguugam xdi xmmztd usgb xm wxdizixugm uk yg g, m, u, x, b, xdi d. waenuxdxqemum xqmk pdkr usxu wgauxzd wkbyzdxuzkdm kc qguugam xag bkag wkbbkd zd usg gdtqzms qxdtjxtg usxd kusgam xag. cka gvxbnqg, h xdi j kwwja uktgusga, xdi mk ik u xdi s. usg caghjgdwe xdi wkbyzdxuzkdm kc qguugam sgqn waenuxdxqemum yjzqi x uxyqg kc nkmmzyqg mkqjuzkd qguugam. usg bkag wznsgaugvu usxu zm xoxzqxyqg, usg yguuga usg wsxdwgm kc yagxpzdt usg wkig.

zd bkigad waenuktaxnszw memugbm, ukk, usg bkag wznsgaugvu usxu zm xoxzqxyqg uk usg wkig yagxpga, usg yguuga. cka uszm agxmkd, xqq memugbm aghjzag caghjgdu wsxdtzdt kc usg pge. kdwg usg pge zm wsxdtgi, dk bkag wznsgaugvu rzqq yg nakijwgi jmzdt usg ckabga pge. wznsgaugvu usxu zm nakijwgi jmzdt izccgagdu pgem—xdi caghjgduqe wsxdtgi pgem—bxpgm usg waenuxdxqemu'm uxmp kc wkig yagxpzdt izcczwjqu.