

Lab Assignment 2:

1. WAP to find the solutions of equations:
 - a. $14x \equiv 12 \pmod{18}$
 - b. $3x + 4 \equiv 6 \pmod{13}$
2. WAP to implement Additive cipher (key=20), Multiplicative cipher (key=15) and affine cipher (key=15, 20). To encrypt the message "this is an exercise".
3. WAP to perform brute force attack on the cipher text "dvvkzeczssprkkve".
4. WAP to perform brute force attack on the cipher text "YMJHFJXFWHNUMJWNXTSJTKYMJJFWQNJXYPSTBSFSIXNRUQJXYHNUMJWX".
5. WAP to use brute force attack to decipher the message :

XPALASXYFGFUKPXUSOGEUTKCDGFXANMGNVS

Assume Affine cipher is used and "ab" is encrypted by "GL".

6. WAP to perform statistical attack on the ciphertext:

"ymnxhtzwxjfnrxytuwtanijdtzbnymijyfnqjipstbqjiljtknrutwyfsyyjhmstqtljnxfsifuuqnh
fyntsymfyfwjzxijsymjnsyjsyjiyzytymjgwtfisfyzwjtkymnxknjqiyjmhtzwxjhtajwxtsqdx
jqjhyjiytunhxtkthzxnslnkwxysxtrjfiashjiytunhxnsnsyjsyjiyhmstqtljnxjlbwjqjxx
qfsxrtgnqjnsyjsyjrzyqynhfyfsiymsfxjqjhyntstkhzwwjsyfsisjcyjsjwfyntsfuuqnhfyn
tsxfsixjwanhbjxluunuyaatanudtzbnnqqjfwsmbyjnsyjsyjbtpxfsimtbxjwanhbjxfsifuuqn
hfyntsfwjwutanijiytzxjwxtkymjnsyjsyymnxpstbqjiljbnqqmjqudtz"
7. WAP to perform statistical and pattern attack over the ciphertext:

"ziolegxkltqodlzfzkgxetngxzgizthkfoehstlqfrzteifoxtlgyltexkofuegdhxztklqfregd
hxztkftzvgkalvoziygexlgfztkftzltexkoznzitegxkltoltytezoctsnlsozofzgzvghqkzlyo
klzofzkgxreofuzitzitgkngyeknhzgukqhinoxesxrofuigvdqfnesqlloeqsqfrhghxsqksugkozid
lvgkaturtklqrouozqsloufqzxtlqfrltegrhkgcorofurtzqoslyktqsofztkftzltexkoznhkgz
gegslqsugkozidlqfrziktqzltuohltecokxltlyoktvqsslitfetngxvossstqkfwgzizitgktzoeqsq
lhtezyegdhxztqkfrftzvgkaltekoznqvtssqligvziqzzitgknolqhsotrofzitoftkftzliol
afgvstrutvossitshngxofrtloufofuqfrtctsghofultexktqhhsoeqzogflqfrftzvgkahkgzgegsl
qlvtssqlwxosrofultektftzvgkal"