CSci 4554 Assignment 5

Due Monday, March 3rd in class

For this problem set writing software is a group work. Each person needs to write down their conclusions and solutions individually.

Problem 1 (10 points). For each of the following equations please find all solutions. If there are no solutions, please explain why. You may use a Extended Euclidean algorithm program (the applet on the course web page or your own program) to find λ. Show all the steps in computing the solutions.

1. $13x \equiv 5 (\text{mod } 27)$
2. $13x \equiv 5 (\text{mod } 26)$
3. $13x \equiv 0 (\text{mod } 26)$
4. $2x \equiv 10 (\text{mod } 26)$

Problem 2 (10 points). Russian alphabet has 33 letters.
Question 1. Which of the following are possible coefficients for an affine cipher for Russian?

1. $a = 4, b = 11$
2. $a = 9, b = 7$
3. $a = 1, b = 3$
4. $a = 22, b = 15$
5. $a = 10, b = 0$

Please show all your computations and briefly explain your answers.
Question 2. For those values that are possible, what is the encryption of the letter я - the last letter of the Russian alphabet? What is its decryption when it appears in ciphertext? Just give the letter numbers as the result, although if you are really interested, you can look up the letters at

http://en.wikipedia.org/wiki/Russian_language#Writing_system

Question 3. One of the possible affine ciphers above is equivalent to a simpler cipher. Which one and to what cipher?

Problem 3 (15 points). The following sequence of symbols (also available on the course web page for easier copy/pasting) is the result of encryption of an English text with an affine cipher. Your task is to find the plaintext and the key (a pair a and b) using letter frequencies analysis. All white spaces, punctuation marks, and letter case distinctions have been removed before encryption.
1 point extra credit: what is the real name of the author of the text?

```
KPQSAUKEBAIQXXQXIVOIAVDANCVQNAJOREQVVQXIBCZANEQEVANOXVZABKXYKXJORZKDQXIXOVZQXIVO
JOOXSAONVUQSAEZAZKJFAAFAJQXVOVZABOOYZANEQEVANUKENAKJQXIBMVQVZKJXOFQSVMNAEONSOXDA
NEKVQOXEQXQVKXJUZKVQEVZAMEAORKBOOYVZOMIZVKPQSAUQVZOMVFQSVMNAEONSOXDANEKVQOXEOEZA
UKESOXEQJANQXIQXZANOUXGQXJKEUAPPKEEZASOMPJRONVZAZOVJKCGKJAZANRAAPDANCEPAAFCKXJEV
MFQJUZAVZANVZAFPAKEMNAORGKYQXIKJKQECSZKQXUOMPJBAUONVZVZAVNOMBPAORIAVVQXIMFKXJFQS
YQXIVZAJKQEQAEUZAXEMJJAXPCKUZQVANKBBQVUQVZFQXYACAENKXSPOEABCZANVZANAUKEXOVZQXIEO
DANCNAGKNYKBPAQXVZKVXONJQJKPQSAVZQXYQVEODANCGMSZOMVORVZAUKCVOZAKNVZANKBBQVEKCVOQ
VEAPROZJAKNOZJAKNQEZKPPBAPKVAUZAXEZAVZOMIZVQVODANKRVANUKNJEQVOSSMNNAJVOZANVZKVEZ
AOMIZVVOZKDAUOXJANAJKVVZQEBMVKVVZAVQGAQVKPPEAAGAJWMQVAXKVMNKPBMVUZAXVZANKBBQVKSV
MKPPCVOOYKUKVSZOMVORQVEUKQEVSOKVFOSYAVKXJPOOYAJKVQVKXJVZAXZMNNQAJOXKPQSAEVKNVAJV
OZANRAAVRONQVRPKEZAJKSNOEEZANGQXJVZKVEZAZKJXADANBARONAEAAXKNKBBQVUQVZAQVZANKUKQE
VSOKVFOSYAVONKUKVSZVOVKYAOMVORQVKXJBMNXQXIUQVZSMNQOEQVCEZANKXKSNOEEVZARQAPJKRVAN
QVKXJRONVMXKVAPCUKEHMEVQXVQGAVOEAAQVFOFJOUXKPKNIANKBBQVZOPAMXJANVZAZAJIAQXKXOVZA
NGOGAXVJOUXUAXVKPQSAKRVANQVXADANOXSASOXEQJANQXIZOUQXVZAUONPJEZAUKEVOIAVOMVKIKQXV
ZANKBBQVZOPAUAXVEVNKQIZVOXPQYAKVMXXAPRONEOGAUKCKXJVZAXJQFFAJEMJJAXPCJOUXEOEMJJAX
PCVZKVKPQSAZKJXOVKGOGAXVVOVZQXYKBOMVEVOFFQXIZANEAPRBARONAEZAROMXJZANEAPRRKPPQXIJ
OUXKDANCJAAFUAPPAQVZANVZAUAPPUKEDANCJAAFONEZARAPPDANCEPOUPCRONEZAZKJFPAXVCORVQGA
KEEZAUAXVJOUXVOPOOYKBOMVZANKXJVOUOXJANUZKVUKEIOQXIVOZKFFAXXALVRQNEVEZAVNQAJVOPOO
YJOUXKXJGKYAOMVUZKVEZAUKESOGQXIVOBMVQVUKEVOOJKNYVOEAAKXCVZQXIVZAXEZAPOOYAJKVVZAE
QJAEORVZAUAPPKXJXOVQSAJVZKVVZACUANARQPPAJUQVZSMFBOKNJEKXJBOOYEZAPDAEZANAKXJVZANA
EZAEKUGKFEKXJFQSVMNAEZMXIMFOXFAIEEZAVOOYJOUXKHKNRNOGOXAORVZAEZAPDAEKEEZAFKEEAJQV
UKEPKBAPPAJONKXIAGKNGKPKJABMVVOZANINAKVJQEKFFOQXVGAXVQVUKEAGFVCEZAJQJXOVPQYAVOJN
OFVZAHKNRONRAKNORYQPPQXIEOGABOJCEOGKXKIAJVOFMVQVQXVOOXAORVZASMFBOKNJEKEEZARAPPFK
EVQVUAPPVZOMIZVKPQSAVOZANEAPRKRVANEMSZKRKPPKEVZQEQEZKPPVZQXYXOVZQXIORVMGBPQXIJOU
XEVKQNEZOUBNKDAVZACPPKPPVZQXYGAKVZOGAUZCQUOMPJXVEKCKXCVZQXIKBOMVQVADAXQRQRAPPORR
VZAVOFORVZAZOMEAUZQSZUKEDANCPQYAPCVNMA
```