Math 1350 **The Art of Secret Writing** **Fall 2012**

Review for Exam 1

Skills to practice:

- Encipher/decipher with known keyword.
  - Shift cipher
  - Railfence
  - columnar transpositions
  - ADFGVX
  - Vigenere
  - affine/decimation
  - general substitution
- Modular arithmatic
  - Reducing numbers modulo m
  - Addition and Subtraction modulo m
  - Multiplication modulo m
  - Finding multiplicative inverses modulo m and testing for relative primeness.
  - Solving pairs of linear equations modulo m
- Frequency analysis
  - Finding likely keys for shift / affine ciphers
  - Finding an initial guess for some letters in general substitution cipher.
  - Finding most likely keys for affine substitutions (this is the only cryptanalysis step you will be asked to do on the affine cipher on the exam.)
- Cryptanalysis
  - Known word attack columnar transposition cipher.
  - For mono alphabetic substitution ciphers with word breaks preserved using a knowledge of English to make initial observations such as noticing repeated words, single letter words, common prefixes or suffixes.

Concepts to be applied:

- Advantages and limits of frequency analysis.
- Dependence of frequency analysis on sample size and content.
- Relative strengths of ciphers, especially related to number of possible keys.
- Functions and inverses and how they relate to ciphers.
- Vocabulary of cryptology.

Practice problems:

Task 1. *Encipher the word* `Hooligan` *in the various ciphers using the following key information:*

- *Shift cipher,* $b = 9$
- *Railfence*
- *columnar transpositions, keyword "mate."*
- *ADFGVX, keyword "mate."*
- *Vigenere, auto key primed with "Q."*
- *affine/decimation,* $a = 3, b = 4$
- *general substitution, use alphabet:*
  QWERTYUIOPASDFGHJKLZXCVBNM[1]

Task 2. *Decipher the following messages using the same keys as in Task 1: Accidents don't just happen of themselves.*

- `JLLRM` *Shift cipher*
- `ETDNS` *Railfence*
- `NJOUT` *columnar transpositions*
- `AFXXVGXDXXFGXAFX` *ADFGVX*
- `ETY` *Vigenere*
- `ZQOG` *affine/decimation*
- `SCTL` *general substitution,*

String the plaintexts together to get a message.

[1] Yes, you know where this substitution came from.

Task 3. *Compute the following:*

- $-6 \mod 5$ $\quad$ $162 \mod 26$ $\quad$ $125 \mod 11.$
  $4, 4, 4$
- $17 + 22 \mod 26$ $\quad$ $5 - 13 \mod 26$ $\quad$ $6 + 5 \mod 11.$
  $13, 18, 0$
- $7 \times 3 \mod 11$ $\quad$ $-4 \times 16 \mod 10$ $\quad$ $18 \times 14 \mod 26.$
  $1, 6, 18$
- *What numbers* $1, \ldots, 25$ *are relatively prime to* 26*?*
  2,3,4,6,7,8,9,11,12,13,14,16,17,18,19,21,22,23,24
  What numbers $1, \ldots, 27$ *are relatively prime to* 28*?*
  2,4,5,6,7,8,10,11,13,14,16,17,19,20,22,23,25,26 *What numbers* $1, \ldots, 28$ *are relatively prime to* 29*?*
  2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28
- $7^{-1} \mod 11$ $\quad$ 8
  $17^{-1} \mod 26$ $\quad$ 23
  $28^{-1} \mod 29.$ $\quad$ 28
- $\begin{cases} 7a + b \equiv 8 \mod 19 \\ 3a + b \equiv 17 \mod 19 \end{cases}$ $\quad$ $\begin{cases} 4a + b \equiv 4 \mod 19 \\ 15a + b \equiv 15 \mod 19 \end{cases}$ $\quad$ $\begin{cases} 18a + b \equiv 1 \mod 19 \\ 13a + b \equiv 16 \mod 19 \end{cases}$
  $(13, 16), (7, 0), (4, 2)$

Task 4. *Using frequency analysis on the following messages enciphered using a shift cipher the two most likely possibilities for what the shift was. (Anna Karenina)*

- *B lxx t ftg pah atl lxkbhnl bgmxgmbhgl, matm'l Exobg; tgw B lxx t ixtvhvd, ebdx mabl yxtmaxkaxtw, pah'l hger tfnlbgz abflxey. I see a man who has serious intentions, that's Levin; and I see a peacock, like this featherhead, who's only amusing himself. – 19*
- *Wkh kljkhvw Shwhuvexuj vrflhwb lv hvvhqwldoob rqh: lq lw hyhubrqh nqrzv hyhubrqh hovh, hyhubrqh hyhq ylvlwv hyhubrqh hovh. The highest Petersburg society is essentially one: in it everyone knows everyone else, everyone even visits everyone else. – 3*
- *Ftqdq ime azxk azq odqmfgdq uz ftq iadxp ita oagxp oazoqzfdmfq rad tuy mxx ftq ndustfzqee mzp yqmzuzs ar xurq. There was only one creature in the world who could concentrate for him all the brightness and meaning of life. – 12*

Task 5. *Using frequency analysis on the following messages enciphered using an affine cipher the two most likely possibilities for what the a, b were. (Nevil Shute)*

- *Qme oib w fmezdi dmb ml bvmezdiy krij qme oib ijowoif, zeb qme oib bri ridd ml w dmb gmvi lej. You get a double lot of troubles when you get engaged, but you get the hell of a lot more fun. – 3,22*
- *R bfsfufre ofuji, ufpl r gyrzrifb byfifb, fd zlyluh r hjnev zre xaj fd ijj urmh ij xjyp qjy r ufsfev. A civilian pilot, like a dramatic critic, is merely a young man who is too lazy to work for a living. – 5,17*
- *Jqipgby qi smho ty nlmqz mzh iqsnlo nognlo lqeo gwbioldoi, hgqzc pjo toip ko amz kqpj omaj xgt mi qp agsoi mlgzc. History is made by plain and simple people like ourselves, doing the best we can with each job as it comes along. – 7,12*

Task 6. *The following messages were enciphered using keyword columnar transpositions. You know each message has a known word that is given and has five columns. Decipher the messages. (Isaac Azimov)*

- *(inaction) bynangriilueotmonjhboonoomicofrmtrmitgcaangmaatouueruanwanohoaieanhhtlhbter A robot may not injure a human being or, through inaction, allow a human being to come to harm. – Powel*
- *(conflict) rmbditmixwsrwcitfloueevbanchudoochiaotosnhbsprhrlfwhsvbsyreyngeeceunttrwatorgiueeteosdliet A robot must obey orders given it by human beings except where such orders would conflict with the First Law. – VIPTR*
- *(existence) otesxnlspcdofwhselbstteesahennnttrsdouointagctosochirnatpcoicosrtotlietcarmrtwsenuoiecitfoow A robot must protect its own existence as long as such protection does not conflict with the First or Second Law. – Stone*

Task 7. *These messages were enciphered using a general substitution cipher. Word divisions have been preserved. Make for each message at least three observations about each message that you could use to help decipher it. (No need to completely decipher the message, unless you are bored). (Frank Herbert)*

- *anym bp qen zbqqzn-dnyqe qeyq rmbhgp qjqyz jrzbqnmyqbjh. b ubzz ayfn cw anym. b ubzz knmcbq bq qj kypp jtnm cn yhd qemjsge cn. YRFDNAGEBIOZCHJKLMPQSTUVWX – Fear is the little-death that brings total obliteration. / I will face my fear. / I will permit it to pass over me and through me.*
- *ivq ftav sp tic mova dicp s fszz pgkv pta svvak ana po caa spc dipt. ftaka pta raik tic mova ptaka fszz xa voptsvm. ovzn s fszz kabisv. ixwqarmtslyzbvodukcpgjfhne – And when it has gone past I will turn the inner eye to see its path. / Where the fear has gone there will be nothing. / Only I will remain.*
- *mrkq e oajwaqhpajrko ypw kdokndi jtakqwajw jwewkj wrew jcgkwraqh aj scjjaydk, rk aj edgcjw tknweaqdi nahrw. mrkq rk jwewkj wrew jcgkwraqh aj agscjjaydk, rk aj lkni sncyeydi mncqh. eytokzhravbdgqcsxnjwplmfiu – When a distinguished but elderly scientist states that something is possible, he is almost certainly right. When he states that something is impossible, he is very probably wrong.*

Task 8. *You may also be asked questions about the vocabulary we have encountered in the course especially to see if you can explain the differences between them or are able to identify what they refer to.*