3 Mechanical Methods

Notes:

1. Remember to check the types of input control or input box used for answers in multiple choice questions. If radio buttons are used it means you need to select the one best answer. If check boxes are used, then there will be more than one correct answer.

2. Some questions have extra instructions for entering your answers. This guidance is provided because Canvas is very particular about short answer questions and will only mark your answers as correct if they are an exact match for the expected answer(s). If you want Canvas to automatically grade your answers you must follow this guidance. If Canvas marks one of your answers as incorrect because you didn't follow the extra guidance, but you feel your answer is correct, you will have to send me an email so I will know to manually check your answer.

Exercises

1. Assume that you encrypt a plain text file containing 14,567 characters using a mono alphabetic cipher, which results in cipher text that we will call MAC. Next you encrypt the same plain text file using a poly alphabetic cipher which results in cipher text that we will call PAC. Which of the following will be true?
    a. MAC will contain more characters than PAC.
    b. MAC will contain fewer characters than PAC.
    c. MAC and PAC will contain the same number of characters.
    d. None of the above.

2. Assume you are encrypting a plain text message that only contains lower case letters from the English alphabet. Which of the following requires a cipher alphabet of more than 26 characters?
    a. Homophonic
    b. Mono alphabetic substitution
    c. Mono alphabetic transposition
    d. Poly alphabetic
    e. None of the above

3. Which of the following is true about the Trithemius cipher?
    a. It is a homophonic cipher.
    b. It is a mono alphabetic cipher.
    c. It is a Poly alphabetic cipher that moves through each cipher alphabet in a set order.
    d. It is Poly alphabetic cipher that uses a keyword to determine which cipher alphabets to use.
    e. None of the above

4. Which of the following is true about the Vigenère cipher?
    a. It is a homophonic cipher.
    b. It is a mono alphabetic cipher.
    c. It is a Poly alphabetic cipher that moves through each cipher alphabet in a set order.
    d. It is Poly alphabetic cipher that uses a keyword to determine which cipher alphabets to use.
    e. None of the above

5. True or False. The Vigenère cipher can provide perfect security if it used with a key word or key phrase that has as many characters as the plain text.
    a. True
    b. False

6. Assume you are encrypting several plain text messages using the Vigenère cipher. Which of the following will result in flaws in the cipher text that can be used to break the messages?
    a. Using a keyword/keyphrase that has more characters than the plain text.
    b. Using a keyword/keyphrase that has fewer characters than the plain text.
    c. Using the same keyword/keyphrase to encrypt more than one plain text message.
    d. Using a keyword/keyphrase that has the same character frequency as a normal alphabet.
    e. None of the above

7. What information needs to be exchanged to use the Vigenère cipher?
    a. Which extra cipher text characters are being used to encrypt high frequency letters such as “e” and “t”.
    b. Which characters in the cipher text are being used to indicate a shift to a new cipher text alphabet.
    c. A keyword or keyphrase that will be used to determine how to set up the initial configuration of the transposition alphabets used in the Vigenère table.
    d. A keyword or keyphrase that will be used to determine which rows in the Vigenère table to use during encryption, and the order for using the rows.

8. True or False. The use of One Time Pads provides perfect security because it eliminates the need for the sender and receiver to exchange any information besides the encrypted text.
    a. True
    b. False

9. True or False. The use of mechanical encryption machines such as Enigma or Purple provided perfect security and eliminated the need for the sender and receiver to exchange any information besides the encrypted text.
    a. True
    b. False

10. What is the name of the main encryption system used by the Germans during World War II? If you want Canvas to give you credit for this question your answer must be in all lower case. For example if the answer is Dover enter dover.

11. Which of the following made it difficult to crack encrypted messages sent by the Germans during World War II?
    a. *The number of possible initial rotor and plugboard configuration settings.
    b. *The fact that the rotor settings changed each time a character was entered.
    c. The fact that a simple test message was sent at the start of each day.
    d. The fact that the initial rotor settings, did not need to be exchanged between sender and recipients.
    e. *The fact that the initial rotor settings changed each day.
    f. None of the above

12. Assume that you are in charge of a spy operation and you are running 4 field agents. You want each of these agents to communicate with each other, as well as with you. You want to use One Time Pads (OTP) to ensure that all communication remains secret. You also want each line of communication to use a unique One Time Pad in case the agent is compromised. That is, Agent 1 will use one OTP to communicate with you, a different OTP to communicate with Agent 2, a different OTP to communicate with Agent 3, etc. How many OTPs are required to implement this system? Count each OTP pair as one OTP. For example, the OTP shared by Agent 1 and Agent 2 will count as one OTP, not two. If you want Canvas to grade your answer enter your answer as a number. For example if the answer is 1 enter 1. Do not enter one or “one”.

13. The following text has been encrypted using a Trithemius cipher. What is the first word of the plain text?
    Hint 1 – remember there are several sites on the Internet that will do this decryption for you.
    Hint 2 – The decrypted text may have the spaces removed. If this happens, look at the cipher text to determine how many characters there are in the first word.

    If you want Canvas to grade your answer enter your answer in all lower case with no quotes. For example if the answer is Tony enter tony. Do not enter Tony or “tony”.

```
Tigui ny mznooaz kxjyag, ncaoc hs gthiiut erdsahh
Ihp lh wvpzf shf fhpzml qw k amcsg slh
```

14. The following text has been encrypted using a Vigenère cipher. What is the most likely key length? Hint - there are several sites on the Internet that will do this calculation for you. If you want Canvas to grade your answer enter your answer as a number. For example if the answer is 1 enter 1. Do not enter one or “one”.

```
UEOXBHZKITRMGREKHDZWQKMEIBXCTVIBPMQOOTCZXCEVAMAUCLFRZBACIFNNBBRAKIJV
KCVCAXMWRNVAMBBARVSJNVMTWEYMKYZZOIIGBLZVZGXYXJBZNHPKKHZJBJRFFMQZFZJC
JVZPKJSKILQKUAMMLMRLTDWGYAKHJZBXOEGOPXQKTRZBTPEFFAWKCOXNVNYYOISOWHNK
EAILBLYGEXBTLECEOBXPCYEIQGFOJJPLZKKETOPXQGWEOGHPOETZZXQZFFOPXEUMEMVF
CTKRZYNGXVSDBLSLWIXMBRZFSVGYMAEDDVZDGKHZZLDXFMOPXJODIOMWEUMEMVFCTKSX
PHMRNEMMGMZKOJPTNVPAWWNRZYINIVAUIDDVZRUYINBHPORNYWKMZYYBIGDOVLYNHURV
RDVACXSOJSNLSRIGIUJKKHZZXQUCUOQHLRVDBMHPMVWVAAGTXTJVMMIFMKTTGTRBJCMK
GZLOIFNKIIIOTLJKHJUTQPVFAMKQUEJVUXQSRDDAHLGEDEIFCYDOIZHCHVGVVMMCIIOM
MMKRCCWMFKIIIKHBKKOKZXQKIVZBACVIIQIVWUWTCMBPIFMHCGGIRTDWGQOEFVKMRNVF
JCGBOEGAIMFKISPAXBKECMGIROFNWMYMXVDPZBLMRNYIYRKITCMKCBFLPBBMTRRTETPP
VFAMKQUEIIXTPZZCPTTPCRSVXKMRZFDKNQKIOAMGAXPPOMWAUDMPVBAGKIJVLYTUEQMG
GTMEIBXBGTIKPXPTFWFVHUTRSOPXHKWFZZLMTUINSMMKECMGIRGEDYMVPEGTCQLAUDMP
VBAGKIJVLBKJPDBXUNRTOPXEUMEMVFCTKHVAVJGZMZLKCIVNOTRCTTRTXMCJTOHUNLOT
AOQHLYRRZVHRGEOQMEREKHZGPCXVAOBACNVAMBHDZYEDLXYYKHVBECJKOVUXPOTANNHS
TUIIOMFKWOPVWCXJBZTBCBVDOPTRVIIQIVWUWCJUFSTZCVBBMTRNYKHLYVQPMGRRPBZQ
GEGSLZBHDXVEGGXVVIENAMFKZROPHSMYTNETQIIUXQTJZFAAZXCYFCDMMWPRMZAFYJZS
JVXTKEPVZMGGCLTMGAXPPOMWFOJCJZKCYGOILXLIVTJBAMSRSEMYDKISJVPFKIECMYGX
JTKZHNUJEYBACHZLGWYPOXHOAXLIIYKBBMTYANIEUGPSKTTWKUAFMRNGITDVTKKIIXIG
FOJTJZRZAKTCQLKKJSVOXFGJBZMGJUJTJVFYTPOABHBGPSGMTBKISVAMFKPWJZDRUNEV
SXLKECMGIROFNRPTROJEIKKWVKIJVTRZYEQMKWHRSDKECBVLZVVPEGTDWGGYRWVGMMYT
RVUUJKRNYCGQIIAHJECOEFJZFYZZOICLGTXFJZFSRRSXIEJKUCDXACXJWCQVFUWTZVKC
RPOICGGWLEFMRQLFRZFTKVCEVTBAKDIBPMQKEDVAVPGDBGMWKKJSVOXRUSOWBAYZTAIJ
XBKTRTXMCJFNGGUWAJIIOTIKPTCIMLUFNZMQAKGTWWUNUJSZALCYJONPXAGEBZANPKKH
VBGMUEEZTLCIRNMMTBZYEDZVMTMEMATROFNOWWYEVNXZRNZZOIQLSYVDDVFYTPAMMTQH
VYJVWRXRDDBBMTRLXWFKAEIXIMGUESDBLUNRTZVLSXVSOPTRULRJVEGTVBVVDYITOPVM
QGIENMVSXVIOKTLVIEQMGRYFMZWGCLIOHAGMUGIIOHLEFUMQGRKINZBMPGWFDKTRGTOA
NXCYYOKIGBSFSOQFNUITVVMJEZTNEAYZNEMMEWUETJAXAAIEJCKNKISJVTJJVVDKXQRZ
KZAFYXKPCWGCYRNYKHKVLTZZLUNZCCKHLZRIIWNPKETDZXJOMENOHTKINHMGRUWFDKBY
RJHVDXQZRROMWNAJHDVZDUIBVKDBUFRNEACXVAIMGAXPPOQHLYPSOMFGYZNOMGROFNVT
EWCVAFMGCJJOOPTRMFVZZGKKETXIGYITENAPFGKEQMKBGKADBPYTKSWCMRNZSDLXYOJA
```

IWGQZRROMKCTTRTXMGUEINUTRNRNYGHSIRNOUTLOGUGIMCSRTCXKMHCEHAMMHVSJTOYH
CEWGHLRPOIMLNKTIAQVEXFUKWYNKFPGMYMXZNNBTLIVTCMNQMFVZZGKKETDNMFKVNXZR
NZZOIBAYZRLDKXSYVSOWLCTUAHMLQGXEOWUMHZSXWFNXFMDAXBOKINBACXVTJMQNRFIO
NHPCYOZDXPLZNYABRGUDDBBMTRLGGWCYZGIQGEYVCPZXAUDPPBXPYPSOMFQOJACIKBVI
OWTXKOEMJLXPTTOHXNROEGYMLNOKEOPXZKJTZNYMXKSJNIPUXRVUFCXJWZZXEACAMTRF
KRRVJHSZMUGVXPGSIGQMGKJTCIMAUDPMWFGYVPMQOYZVIINHPSRTDWGDUIMDTEGUESJN
ICUGLZBHGTKEIBBMTRLGGBLZIOYCVCBLLIMKYHZLDBBCYRSKIKRUWARMTIKEEYMGAXPP
OQHLYPSOMFGYRRZKBNKWOMLBQGJTZZGMZAUNBYMXFNZXXPYFNJZVMSGAIGUSZWOMMOCX
POIMNQOEGOPTRKECMGIROFNNGLRKDWZIKCGIGPIUJECIQQGEOEABWEBKEABMHDYLRQMB
JRRNXMPFKIEOPXEUMEMVFCTKHVAFMXVMZIGQZFMJVBRUIIOAICUGLZBAYTVVZZUCLFRZ
QMQIIUXQTJLFRXQMGFVNNQGYJVMJKKYIPTJJXYHCEOWYPKVLTMQNXVSNBACSJEGDXQGE
DZVVPEGTDWGGYFNZWYRNVFZEMMUCSOPTRGTTPIEJEIENQLRYKHZXXPBRSDDXQAIVZQEJ
GECZAMYZVANEAGYKLZJEMCVRZLPYXUSIWPBKEPPBBRKECMGIROFNRWKIYZTNDBRGCTCI
MGZTOIBBLAVSOWPMXBAILMFGKMZIGQXVSDAMGTXGJDXPTDEIBVPKRTZLUYIBDJWKQIFD
ZQLQVVEXPTRZYEZTXAZIOIQVDXFNOQXPLFUILTROFNZNYUKSEGQXTKKHVBZMBVRIUXLZ
JEANHPZJTJKHLZIOGMGAXPPOQHLHPPMMOCTKIIOBRYGUWTBAGKIJVTLJZMKTXKKETVBB
MTZSVDBMRRTDWGMLKHZNBPYKAHMGBSVNOWYRNVCJVLROKUOQHLZYEAQKQZRMZVWKKETK
ZHRKTTNIEJSRNIMKMLVXKZXQYZOIQGARLDDVZUXZTOMGKAJIXIGBGSSOZTAZRROABKOC
AMTRAUUEDATKKRNNWYBOJSZUBLGKIIOBLLFRHIMGUEAILBBKRSDBWMKJNOUTRZVRDNBR
YTOHUNLOTAOMWGTRFJZFRNRTDAGRIFMKZXFKESDJECZFLVGICUGLZUTLEGEJXECIRNOZ
XYJRCGILQOTAGUNQOTSCMXRHLTOPTRJFENVMKKRNOPTRZYEBWOCXEMZVMAGERZAMPOTT
OPXNXFDPKMGUEOAUHXGITOPXDKUEMIEAULROATEXVEYEBRNLSOPTRIFDZQLQVVEXPPFK
EEANEGZZGVBXBGTANMBLZYEIQGCZVEIVBLKKYNKTJRVDWMKLYKEDVOBKGAMBFCTKOARN
QZZCZIUCXBEGMREXRDPIMCYKUYMGRTRMZLWYTZEGRUCXESOMBLCRNOMWRUGUWTBQNZNA
WKKGKIJVTZULTVVXLIIYKBBMTRLBWKGZYMCMAYJUEQMEMVVDWCMFKNANXKMNZBDBXBLI
OHLHGTXSJJXAGLSZBACMFVZZGKKETOZXYZVDNCVFOEFJZFYZZOIILKAEIOQHLYRKDVMM
CVAKWGQUIBJUUQGEDMMJSOIEYILNKTIVTEGIVNNMYPUDTCMLRGKEYMIYXKMZVMRUJHVZ
XGZRLDKXLYVIOEHSRUNJBZPGETCQFKXSEMVLRKZNNCXBGEDMMIPKJEIBXBHPEANLSITE
NAYSRCYVZZSKUTCIMAKESJZBLMRLBWKGZYMNQLYTLNXWGQZZTPBBMTRLQQHJGKIJVHDL
IEZLHKUWSKMXANKHZKTQKIEHIBLYXOJLEYCKOOPBQJRYRQMFYZMDTTPVIEXMWCTKHJTW
GTXIIWMFKICJCKRYGODVMCJCYECWEKSEOBRDRVTXPXPLIOHBACTZNOPVGXTUDBVMAITJ
NTNVVAGAPPUKEOPXYBRIGIUGRZTTIGBAJEJNLCILRZMGAXPPOQHLSRYMMVJGZMNWFCVF
ROQHLUWTCMIPOMAXGPCNRVZTHQZXOQMKLSVNOMYDUITNBHAUETMWECTTRTXMGUETCCLK
GPWZTEGSGLDKTRKEOOWGJEKHZNBPYKAHMGBSVNOZBENKSWCMYRJOOPXAUESOQMSZZOII
EPOXHOAHDKRCCWYSYRSKWMCTKIVTKCIZPDMGRYFFZVVPEGTDWGQHFUIBRRNVGJDXPTDE
IBFYEKRTBHBKGIXBXLIIYKBBMTRSHIDGTXUNCGQGWEWCMRNVRZIEGZPINXKCIZSZTRRN
VOKXHQOKEDBTDLFRYAIPOMAOMBLJZVDLNYRJTCMHNVFROCGGZPTJUTIKKHZULCRMENAT
DKWRJUZMBVRIUXLZJPMGBLMVYZAMFKIERQEJGCWVGLZKTRDUBLGCSRPHRGBEVLOYTKAB
MHDZVCCVHJUXYOWWMHRDOPBLMJBPBPCYYOPTWLZJAXZBDOTEZDXPEFNZAKGMYTNBHNXZ
VVKRYTUFMMXQVVEXPBLZYEIIFCUWSOWINOEGVNXUHRDVKMMXJEIKKWVKIJVBQGYUHIGP
OXHOABQYLEHWOGTXBZGHLJKHZCGGZVDNBTRKJEIKKWVKIJVBQGXLJJTJNLMVVKGMYTNQ
LQAVANIMUUKHJCLYTUFDNMCKERZXHPZWRJUMFKLNDBXBTRTDWGQUWFDKXMLKHZPBENTO
HUBQYZOIMKDUIHPUTLXZGCBLLUKENMGAXPPOQHLGEDVVHLEDIOGXLGSLZQGBOMIYCTJY
KOZFXPIZSZBACOIRDOARYKOAZXCJFMJNHNOEIJVTLJVXKZXQYZOIQGRNVDDOBRGCABMT
LJRSNCVFJVSZZOCYKRJVZNXFTZKMGUETCMKCVFRONNPZYEMMFNNRSDHXQZYAOOHTKINH
MGRYUEHIGBOEGZVVPEGTDWGZGTKYWHPYYAQMGMZUEHWGQZIAOMWRNRTXZBKOEAGWKRKI
RJZBQZLSZWYCTTRTXMGUESZZOCYRSVVBLYLPZZTZRVBVZKGKITJTTUKEFJZVCSVNOWUH
KTTDDXQOEOOPXPCFRYAPFKELVEXLLFRXMFCTKANSLDUICJUIPUDINMWCTTRTXMGUEIOL
HCYETHMTLZYAOMGAXPPOQHLOJAXBNYRCYRPTRYJTJXIGTXTCMFDXFMDVOCYKIBIMGTXT
CWLCIIIHMLYLKEMMQYSZNDVZRNVEIKKWVKIJVIMRZCDMLMLJEQMKYRTOPVMPOVSDVVJA
UIIOKSYJIVKHJUDBDIBLJZAHWKMITOKIDGYKAIIGBZYEPVBRKUSOIMCYRMIMLREZNOMK
LGKIJVTJIFNXTNBKUIIBACJZGDBTJGXEVKVCYJTJIGBAJEJNXLIIYKBBMTZSVVXLGSLZ

```
ZHDZYEMQZFZKOKZBTGTYWMVYAJEZVVPEGTDWGAGEPMWMCIKCJUFSTZCVBBMTJFMWFQVP
IIOBRIRNCMENVVOKTXQNRRZBACOIOKQGGUEWDBAMZYEMAPGZYOPBKCVIINIEQGTCZALG
TWOMUTROFNJVMFKNEWIGBUIGVVBXKNIOPHRNVRNIZYOESOQGHAJTDKXCTTRTXMGUEINB
ACXVFJZXYRJOVVXLGSLZZHDZYEMQZFZJTJNKCKUOHWYCDGRZALGUEIINHPSRTDWGYTUO
KQGGUEAILTJYFHVATLODPVKMMTKHZZBENKSOWYPKVDJUHDVVAXMYSRRSNMFZRPANAHAO
RTDWGYTUOOPXPNLMVVKGMYTNMGAXPPOQHLOJAKIKROTUGIKJETRDBBAGCTJWEDUIHPUT
LXZGCBLBKWEILXPYRCOQOGYKSVVWHULRIIEGYKSVTEMLNHJUKCRPOIQMUOKHDVVPKRSD
VZDXVQPMGAEKOKZHRKTTOPXGXJEXCKGZPAILMFGKOAWMFKISVOTGTJTPVEYCWUGANPBV
IGTTLIVNJUTRZVRRPXPKJOHMHLKIENQWCYZNOPXUUILYBACEUENMKTKJTMWGEKECMGIR
OFNJCKCTTRTXMCJTOHUNLOTAOQHLYRLGWPSYKOCIOCVIIQIVWGEDOWYPKVLTMQNXVSNW
NPYVLQMLYYYUHIGZKZNBAZMBVRIUXLZJEQMKWCYEMMAYBVDZDXJUGEYMQRXROMLBLGIY
RIRQZFMJVBRUITCMBPIZTDHXLYRNYAHGZJBZKHKKVXOZTMXUIIIKGRPIHXHPZRNOBAYZ
NECIOCYKRJVZCTTRTXMGUEANIUSRNAMSYMXGRDDTAERNYNKCKKHJCZFZRGVQGQZKHZIP
CYFMZXHUKIOABACYLRQMBJRRNXMLRGKE
```

15. The following text, including the answer you should provide for this question, has been encrypted using a Vigenère cipher. When decrypted the phrase you should enter will be obvious.
    Hint 1 – remember there are several sites on the Internet that will do this decryption for you.
    Hint 2 – The decrypted text may have the spaces removed. If this happens, look at the cipher text to determine how many characters there are in each first word.

    If you want Canvas to grade your answer enter your answer in all UPPER case with no quotes. For example if the answer is Tony enter TONY. Do not enter Tony, tony, or “tony”.

    ```
    Hye ntwkvr gu xvzs daigkibt mg KHR XMUYT GU TFZVNIC.

    Hye eokvk tb vvwmape mg eog sibkibtir zn gni Qfnfzmhltvur, plt gni
    Glpekqs Tohxx vrs fgmr khnz wsmeegp cw tuk eavnqsibks pxioke gnmg
    iitnx. Cee bl xvv azkrrdeazw wj tuk Jclrgn Eavnqsibk, wuogv jtbvw
    hye cupwte nth ckhrx kcmeetqset nmibks sxsa jenxgvznt aw ci ohx
    tffprxxm nignsik "peufoslr ieije" gu fscirbi hyag ci vrvr isadigzir
    r ceoqs.
    ```