EE 418 - Assignment 2

Total Points: 100
Autumn Quarter, 2021
Prof. Radha Poovendran
Department of Electrical and Computer Engineering
University of Washington, Seattle, WA 98195

Due: 11:59 pm (PST) on Oct 28 (Thur), 2021 via Canvas

Note:

- This homework contains both computation questions (marked as [**Com**]) which are required to do by hand calculations and programming questions (marked as [**Pro**]) which are required to write Python /MATLAB codes. Zero points will be awarded if [**Com**] questions are solved via Python/MATLAB scripts and if [**Pro**] questions are solved by hand calculations.
- Show the computation steps and/or justify your answers in all the [**Com**] questions. Failure to show any intermediate computation steps in [**Com**] questions will result zero points.
- You can use and modify the Python functions provided in the file section of the EE 418 canvas page when answering the [**Pro**] questions.
- You can discuss with others but you need to write your own computation steps, justifications and/or Python/MATLAB codes.
- **Your answers to this homework must be submitted through canvas as a single zip file containing the following:** *i*) **hand written and scanned or word or pdf answers to all the computational and discussion questions as single pdf file.** *ii*) **Python/MATLB codes for programming questions as in filename.py or filename.m respectively.**
- **Name of your submission zip file should follow the following format. "** ***#_$_EE418_HW2.zip*****", where "#" and "$" should be replaced with your first name and last name, respectively.**

1. [**Pro**] (Affine Cipher Decryption) Please answer the following questions.
   (a) (10 pts) Please write a Python/MATLAB function for affine cipher decryption. This function should take the ciphertext (Y) and key value pair (a, b) as inputs and output plaintext (x).
   (b) (5 pts) Use your function developed in part (a) to decrypt the provided cipher text file "*sampleACAD.txt*". Use the key value pair, $(a, b) = (9, -17)$.
   i) Write the decrypted text to a file name "*#_$_affine_output.txt*", where "#" and "$" should be replaced with your first name and last name, respectively.
   ii) Print the 30th to 39th ciphertext characters in the file "*sampleACAD.txt*" and their corresponding plaintext.
2. [**Com**] (Extended Euclidean Algorithm, 5 pts × 2 = 10 pts)
   (a) Using the **extended Euclidean algorithm**, compute integers x and y such that $521x+233y = 1$. Show all the steps in your calculations.
   (b) Find $521^{-1} \mod 233$ and $233^{-1} \mod 521$

3. **[Com]** (Hill and Affine Ciphers, 5 pts × 2 = 10 pts) This is an example of cascading encryption scheme with two consecutive Hill cipher encryptions followed by an affine cipher encryption.

   Consider the following cryptosystem with a smaller set of 11 English letters, i.e., a through k, which map to 0 through 10, respectively. The cryptosystem consists of hill ciphers with keys K_1 and K_2 that are both 2x2 matrices, and an affine cipher with key K_3. Suppose that $K_1 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$, $K_2 = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$, $K_3 = (7, 2)$. For example, if the plaintext is $x = (5, 8)$, then the encryption process is: First plaintext x is encrypted using Hill cipher with key K_1, then the resulting ciphertext is encrypted again using Hill cipher with key K_2, and finally, the ciphertext obtained from 2nd Hill cipher is encrypted using an Affine cipher with key K_3 to obtained the ciphertext y of plaintext x. This process is also shown in the following equations.

$$\text{First Hill Cipher: } (5,8) \cdot \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \bmod 11 = (5,1) \tag{1}$$

$$\text{Second Hill Cipher: } (5,1) \cdot \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \bmod 11 = (0,5) \tag{2}$$

$$\text{Affine Cipher: } (7 \cdot 0 + 2, 7 \cdot 5 + 2) \bmod 11 = (2,4) \tag{3}$$

   In general, the plaintext is $x = (x_1, x_2)$, and the ciphertext is $y = (y_1, y_2)$. Next, you will combine the above three ciphers with the given keys into one single cipher.

   (a) Please write down encryption rule (i.e, Find a matrix K and a scalar b such that $xK + b\mathbf{1}_{1\times 2} = y$). Simplify your answer and express the numbers in $\mathbb{Z}_{11}$ if possible.

   (b) Please write down decryption rule(i.e, Find a matrix $\bar{K}$ and a vector $\bar{b}$ such that $y\bar{K} + \bar{b} = x$). Simplify your answer and express the numbers in $\mathbb{Z}_{11}$ if possible.

4. **[Com]** (Cryptanalysis, 2.5pts × 4 = 10 pts) We use "X", "Y", and "Z" to denote Sender, Reciever, and Eavesdropper, respectively. "X" is sending a message to "Y" using one of the following cryptosystems. The plaintext of the message consists of the letter a repeated a few hundred times. "Z" knows what cryptosystem is being used, but not the key, and intercepts only the ciphertext. For systems (a), (b), (c) and (d), state how "Z" will recognize that the plaintext is one repeated letter and decide whether or not "Z" can deduce the letter and key. (Note: for system (c), the solution very much depends on the fact that the repeated letter is a, rather than $b,\ c, \ldots$)

   (a) Shift cipher

   (b) Affine cipher

   (c) Hill cipher (with a 2 × 2 matrix)

   (d) Vigenère cipher

5. **[Com]** (Stream Cipher, 10 pts) Consider a linear feedback shift register that works mod 3 instead of mod 2, so that the $(i+m)$-th element of the key stream is given by

$$z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j} \pmod 3, c_j \in \{0, 1, 2\} \tag{4}$$

   Let a recurrence of length $m = 3$ be used to generate the sequence. The initial key stream is given below

   1, 0, 1, *, 2, 0, *, 1...

   where $*$'s indicate the missing values. Determine the coefficients c_j and two missing values.

6. **[Pro]** (Stream Cipher, 5pts × 2 = 10 pts) The following sequences in part (a) and part (b) were generated by a linear feedback shift register (stream cipher). Find the coefficients of the recurrences that generate each of these sequences.

   (a) 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0,
   0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1,
   1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0,
   1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1,
   0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0,
   1, 0, 0, 0, 0

   (b) 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0,
   0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0,
   0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1,
   1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0,
   1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1,
   1, 1, 1, 1, 1

7. **[Pro]** (Substitution Cipher Cryptanalysis, 10 pts) You are given the following ciphertext generated based on the substitution cipher:

BCDCEFG BCHFIJEB KECBBCU LCGGCH JH
MNCINCE INC OCUB CFBL PJHCL KJGQRQCB
MCEC OTCGQHV FBBCI ATAAGCB INFI
RJTGU INECFICH INC BLBICP.

You are given the following plaintext/ciphertext relationship table:

Ciphertext	**Plaintext**
A	b
F	a
L	y
T	u
O	f
Q	i
U	d
J	o

Using your linguistic skills (which may include the knowledge of frequencies of occurrence of letters) and command of the English language, decode the sentence correctly. (Hint, this is about the recent senate inquiry about the fiscal policies of the us federal reserve.)
Note: please provide brief steps.

8. **[Com]** (Vigenère Cipher Cryptanalysis, 10 pts) Suppose we have a language with only three letter a, b, c, and they occur with probabilities $\frac{2}{3}$, $\frac{1}{6}$ and $\frac{1}{6}$. A message was encrypted using the Vigenère Cipher (shift of mod 3 instead of 26).

   ABCBABBBACAA

   You are given that the possible key length is either 1, 2 or 3. Find the most likely key length, and the most probable encryption key.

9. **[Pro]** (Vigenère Cipher Cryptanalysis, 5pts $\times$ 3 = 15 pts) The following ciphertexts in part (a) and part (b) are encrypted using the Vigenère cipher. Use correlation analysis to decrypt each of them, separately.

   (a) KTSVFVMHMCHJUBFDYLMGRWZXNHMVDSVNUBJOJULFZNAQILXSXOJYOROEFJTD
   XWCNERALABFMLVJFFSEFVXLUJQBORDKMLFBVGYNXLSNJQDWARDXQHAMBRHUP
   GTYXVVUYXEXHAQJVMLJEZFZBVQPBYPQMPBCUJHBUDSKQFOTVTFGKYXNPDWXJ
   QYVOWLJDUJNJHBUUFUPFOFUTCLWKFJWMKDMOLYNZSQBVBJJHWEEQHLLWTWTO
   RYZXXDYZXOVFPMIHXBMEHSSHZRZKXORYWAPSTZNURNUEFVYPWTRZAQBIWPLB
   QXLLVUNARFVNNJWHFZCBUYVOBVYVWJVMTNOWFJLVVYVVFGFZRXDXAXIRQTNT
   VHBAJRZZOBFZSCJHXAQJVXBMEHSPWUUZZRPQNUCPPDTXTWNUCJPFANUKTBPI
   WXDJTXYANSODPWFAUSRDDGSN

   (b) KSQRAUHSQGGBFDQSXOIXMRWCSYFWAAPPOSELGYQGWZGLDCXVFZZIHLCAXIL
   VRTEWGSJPFLWWCWUXAJOWNEFKGHTMUOVLHIUVBYQGLLRETIEDWETEFVHSQV
   SUREAEKZIXQEEVBRFLWWCHQVKVTETIWHFETXZLGPBEJHHPMRVLEFMPKAOEU
   SFACHTMUOHSQPSDGZRRSAICQEFKCQZELBFPEKGKSYFMLSSETIEHRPOIFAFP
   ETWJHEAXZLCAURAVBDAJEHBVURVYSBGMJLGETELAVPKWZVIWPHWJZLDILOS
   NMYKLGHTMUOWXBIDAVPYXGAVPEIHHFLFMGU

   (c) GGAMGHUMEDWXUFFAOQLYYSALSHUMEDDXPDVUMAKREIKLAZFEMJQHKKBYKQKY
   SHVRQFATXMMSFBAHZBXHXHQCGOLERXXTOPPYFBMFRPNVFPZULZWTFQBIYQTH
   LRTVCAVSKFTWKZFLJGKNXNUVFALYLFRSIXVUHOVJWHVLGOLOHSXTPQFVMQGH
   VNRQRKTQLXEVGPRCLZBKXWGZEFWFHLVPREVJRQRNWJPHAVDZBSESFFGPVZMT
   QPVERTHFBHEACKNSFEBXSUEOLWAAZWEEJFPHSSHWMIJJFJYKIYECCILZPEBS
   GAWARZATXXXJFVBMZUWJGWCKALSMMYERMPGOHFWTRDVQNYNQMBIPMKRZZQLN
   RIJBPYFBMTKGCMUPJMELSGKQUTZFAJQHGIILZNNYMCUQRHKQQUPDKQJLHWGJ
   WHGPVUATXNVXOMYLTQGYEIKLALCQGYLDWDUAOQZTEAJXFILQGYLTUXZLATXR
   IIJLQZHZWYIRJKVXBQLTJRTVCAHZTQCHKPUHCQVMECIBQKYMLYMRCIYFATKT
   YVJQULOULYSGALSJYKIYSVTXCOFMWFTIKKTAVUGHVTCPVUNOKDTIQDEHWTBH
   GDOMYLEUMDVPPDVUNRKTQIJBCLUMGITPRBETLFATHHQCGOLBTXXIJOBBNTFF
   GWKKRZSUDJXWGYEPAULMFDOYRZHZWHSAQPFBZOHRTJVBEZHFUQIIEEYLFBTW
   OXPTBYSPPFVXKQBAOQFFXWGJNAPOTQPNCAIHUOXIGDOMHALDBEISUZULTQLT
   JIJBCYLEXSXBGQUVKEYTVQTBNRPZZRSSGOAJYKIYSHAPGLTEHKXTPFACVXOJ
   WDNSVUNOTWIUWIYFJAGXXGWZGLKBKTFAGJFPUBNWIBCQULTMMNGHVERILEMP
   RDYKOLPZZNRIGDRYMMVYSGKWNAPAG