CALIFORNIA STATE UNIVERSITY
LONG BEACH

Homework #1

CECS 378 – Spring 2020 Cappel

Due: Thursday, February 6 prior to class (5 PM)

Homework #1 is focused on classical cryptography. 20 total solutions all worth 4 points (100 total) & 4 extra credit solutions all worth 4 pts. (16 total).

This assignment will introduce you to several instances of classical cryptography and have you encrypt, decrypt, and in some cases cryptanalyze the ciphers. **Please show all of your work!**

Note: This website will be of value when using frequency analysis or checking your work:

https://www.dcode.fr/ (Select English Version in upper left corner – lots of good tools!)

Problem 1 – Examples of Simple Substitution Ciphers

One way to form a *simple substitution cipher* is to just use a random cipher alphabet.

Consider a simple substitution cipher with the following cipher alphabet.

Plain:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher:	X	Q	K	M	D	B	P	S	E	T	C	L	O	R	U	J	V	A	F	W	Z	G	H	N	I	Y

(a) Use this cipher to encrypt A FEW WORDS ON SECRET WRITING.

(b) Decrypt WSD BXLL UB WSD SUZFD UB ZFSDA, which was formed using this cipher.

For *simple keyword substitution ciphers*, users agree upon one or more keywords for the cipher. Spaces and duplicate letters in the keyword(s) are removed, and the resulting letters are then listed in order as the ciphertext letters that correspond to the first plaintext letters in alphabetical order. The remaining alphabet letters not included in the keyword(s) are then listed in alphabetical order to correspond to the remaining plaintext letters in alphabetical order.

Consider a simple keyword substitution cipher with the keyword GILLIGAN.

(c) Use this cipher to encrypt A TALE OF A FATEFUL TRIP.

(d) Decrypt RGQUNJ WNJLD GUAETEOMNA BOR KGRY GMM, which was formed using this cipher.

For *keyword columnar substitution ciphers*, users again agree upon one or more keywords, and remove spaces and duplicate letters in the keyword (s). The resulting letters are then listed in

order in a row, with the alphabet letters not included in the keyword (s) listed in order in successive rows of the same size beneath the keyword letters. The cipher alphabet is then obtained by taking the columns of the resulting array of letters in order starting from the left, and placing these columns as rows under the plaintext letters.

Consider a keyword columnar substitution cipher with the keywords MARSHAL DILLON.

(e) Use this cipher to encrypt CAPTAIN KIRK WAS IN ONE EPISODE.

(f) Decrypt MGA HWDKCZ DLYUF MLLCMZCA VYIZ KWHCD, which was formed using this cipher.

Considering the number of possible cipher alphabets, substitution ciphers seem impossible to break. With 26 letters, there are more than 4×10^{26} possible cipher alphabets. To test them all would be infeasible. However, as it turns out, most simple substitution ciphers are fairly easy to break through the use of *frequency analysis*. In fact, inadequate security of substitution ciphers has even altered the course of history. For example, the breaking of a substitution cipher led to the execution of Mary, Queen of Scots in 1587.

In languages like English, it is known that certain letters and combinations of letters occur more often than others. In ordinary English, the letters that naturally occur the most often are, in order, E, T, A, O, I, N, and S. The frequency with which each of the 26 letters in our alphabet occurs in ordinary English is well known.

Common digraphs (letter pairs), trigraphs (letter triples), and repeated letters in ordinary English are also known. The most common digraphs are TH, ER, ON, AN, RE, HE, IN, ED, and ND. The most common trigraphs are THE, AND, THA, ENT, ION, TIO, FOR, NDE, HAS, and NCE. The most common repeated letters are LL, EE, SS, TT, OO, MM, and FF. A thorough analysis of common letter sequences in ordinary English can be found here.

Leveraging frequency analysis, cryptanalyze the following ciphertexts, which were formed using substitution ciphers.

(g) ZVR XIELR PD QALLRQQ EQ VGIU SPIO, URUELGZEPH ZP ZVR FPC GZ VGHU, GHU ZVR URZRINEHGZEPH ZVGZ SVRZVRI SR SEH PI WPQR, SR VGJR GXXWERU ZVR CRQZ PD PAIQRWJRQ ZP ZVR ZGQO GZ VGHU.

Hint: The two most common letters in the ciphertext correspond to the two most common letters in ordinary English.

(h) IES QJDEVFMRF MVY FIY WQTLMC MVFT FE TEHQYFN? Q UYYC TFVERBCN FIMF FIY WQTLMC MVFT MVY EU WMTF MRO QRHMCHLCMACY QJDEVFMRHY. EU HELVTY Q HELCO AY DVYZLOQHYO. Q MJ M WQTLMC MVF.

Hint: The most common letter in the ciphertext corresponds to the plaintext letter A.

Problem 2 – A More Complex Substitution Cipher

While simple substitution ciphers are not very secure, not all ciphers based on substitution alone are easy to break. The Navajo code, a cipher famously created by Native Americans, primarily from the Navajo Nation that occupies a large region of Utah, Arizona, and New Mexico, and used effectively by the Americans throughout the Pacific Campaign during World War II, was essentially a substitution cipher.

Read the World War II fact sheet covering the Navajo Code Talkers at the following link:

https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/n/code-talkers.html

Leverage the Full Navajo code dictionary at the following link to solve (a) and (b):

https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/n/navajo-code-talker-dictionary.html

For the following plaintext, use the full Navajo code dictionary to encrypt the plaintext, and give the literal English translation of the resulting ciphertext.

(a) TANK AMMUNITION DEPLETED.

For the following ciphertext, which was formed using the Navajo code, use the full Navajo code dictionary to give the literal English translation, and decrypt the ciphertext.

(b) AL-TAH-JE-JAY DIBEH SHI-DA GAH TKIN NA-HASH-CHID WOL-LA-CHEE MOASI TSE-GAH YEH-HES AH-DI HA-YELI-KAHN

Problem 3 – Examples of Transposition Ciphers

Transposition ciphers, like substitution ciphers, are not very secure, but have a rich history of being used. The scytale cipher used in ancient Greece was a transposition cipher. Transposition ciphers have also been included as parts of larger ciphers, such as the ADFGX and ADFGVX ciphers used by Germany during World War and the Data and Advanced Encryption Standards, both of which were selected in recent years by the National Institute of Standards and Technology to serve as Federal Information Processing Standards.

For columnar transposition ciphers, users agree upon some prescribed number of columns, and then the actual plaintext letters (with spaces and punctuation removed) are used to form an array of letters, similar to the array used in keyword columnar substitution ciphers, with this

number of columns. The ciphertext is obtained by taking the columns of the resulting array in some specified order and placing the letters in these columns in a row.
For *simple columnar transposition ciphers*, the ciphertext is obtained by taking the columns of the array in order, starting from the left, and placing the letters in these columns in a row.

Consider a simple columnar transposition cipher with five columns.

(a) Use this cipher to encrypt LAKE PLACID IS IN UPSTATE NEW YORK.

(b) Decrypt IGOIA UNNOU RCNST RSOKT HGANM AEEDD OI, which was formed using this cipher

For a simple columnar transposition cipher, the only key is the number of columns in the array. Thus, for a ciphertext formed using a simple columnar transposition cipher, the cipher can usually be broken by a brute force attack, meaning we would try arrays with various numbers of columns (in some systematic fashion) until obtaining the correct plaintext.

EXTRA CREDIT: Cryptanalyze the following two ciphertexts, which were formed using simple columnar transposition ciphers.

(c) AOANS BUYTE NBIEB ELNDA REVBL DDEAL

(d) DMAIN TATLR EITVE SBXJS SHEDK AXANM INBEL X

For *keyword columnar transposition ciphers*, users agree upon one or more keywords, and remove spaces in the keyword(s). However, unlike for keyword substitution ciphers, for keyword transposition ciphers duplicate letters are not removed from the keyword (s). The number of columns in the array is then equal to the number of keyword letters, with the keyword letters placed in order as labels on the columns, and the ciphertext obtained by taking the columns of the array (not including the keyword letter labels) in alphabetical order by the keyword letter labels, and placing the letters in these columns in a row. If the keyword(s) contain any duplicate letters, then columns with identical keyword letter labels are taken in order starting from the left. Also, to make decryption easier, users can choose to include extra characters at the end of a message so that each column in the array will contain the same number of letters. This is called *padding* the message.

Consider a keyword columnar transposition cipher with the keyword MAYBERRY.

(e) Use this cipher to encrypt THE ANDY GRIFFITH SHOW WAS SET IN RURAL MAYBERRY NORTH CAROLINA, padded with Xs (if necessary) so each column in the array will have the same number of letters.

(f) Decrypt NTUAP FRYWT TRRYS NAHAM XAEOW SNEHO IETAX OFRII YXDON SIORM MYNOB X, which was formed using this cipher.

Because keyword columnar transposition ciphers do not necessarily take the columns of the cipher array in order, cryptanalysis can be more difficult than it is for simple columnar transposition ciphers. To break a keyword columnar transposition cipher by a brute force attack, not only must arrays with various numbers of columns be considered, but various ways

to order the columns of these arrays must be considered as well. The cryptanalysis process can be simplified, however, if a crib (i.e., a part of the plaintext) longer than the keyword(s) is known.

The following ciphertexts were formed using keyword columnar transposition ciphers.

EXTRA CREDIT: Cryptanalyze each of the two ciphertexts with the given crib.

(g) UAODI HRNNI AODSE FSOUI CWLAI HSTHO HIBYF TROTI TVRDE LRETF ENEL, with the crib CIVIL WAR

(h) IDHTE NCLEX MECEH ACLHX AHPAO OAROA NTABF HDEFB SSAKT POATL IUESR OSBRL, with the crib PEACH BASKET

Problem 4 – Example of a Shift Cipher

For shift ciphers, users agree upon an order for the alphabet letters, like for instance the natural order A, B, C, …, Z of letters in our alphabet, and then encrypt each plaintext letter by replacing it with the letter some agreed-upon number of positions to the right in the alphabet, wrapping from the end of the alphabet to the start whenever necessary.

The Roman Emperor Julius Caesar described a shift cipher with a shift of three positions to the right for encryption in his writings on the Gallic Wars. However, shift ciphers are not just something from the distant past. Shift ciphers were used by the Russian military as recently as 1915, and the modern *ROT13* cipher (whose name stands for "rotate 13 positions") is just a shift cipher with our alphabet letters in the natural order and a shift of 13 positions to the right for encryption. Caesar's cipher was likely secure in its day, given that most of his enemies were illiterate or unfamiliar with his language. On the other hand, the shift ciphers used by the Russian military were easily broken by the Germans and Austrians. ROT13, despite not being secure, is still widely used to give a casual disguise to things that users do not want to just state in the clear, such as puzzle answers, movie or television spoilers, and potentially offensive statements.

Consider Caesar's cipher with our alphabet letters in the natural order.

(a) Use this cipher to encrypt ET TU, BRUTE.

(b) Decrypt HASHU LHQFH LVWKH WHDFK HURID OOWKL QJV, which was formed using this cipher.

(c) Use ROT13 to encrypt BOB SACAMANO.

(d) Decrypt SENAX YVAQR YNABE BZNAB JFXV, which was formed using ROT13.

Shift ciphers are no harder to break than substitution ciphers, of course, because they are substitution ciphers. In fact, shift ciphers are much easier to break than substitution ciphers in which the correspondences between plaintext and ciphertext letters are assigned randomly or

via a keyword, since with a shift cipher, if the correspondence between one plaintext letter and one ciphertext letter is known, the rest of the correspondences follow. This makes a brute force attack effective against a shift cipher, and often allows a short ciphertext formed using a shift cipher to be cryptanalyzed much more easily than if it had been formed using a non-shift substitution cipher.

For a message written using our alphabet letters and encrypted with a shift cipher, the ciphertext could be the result of a maximum of only 25 distinct shifts (assuming that a shift of zero positions is not used). A brute force attack could be done by simply trying to decrypt the ciphertext assuming each of these 25 possible encryption shifts one at a time and stopping when the correct plaintext is revealed. It would almost certainly be known immediately when the correct plaintext was revealed, since of the results of the various attempts at decryption, it is almost certain that only the letters in the correct plaintext would make sense when strung together. In addition, it may be possible to save a significant amount of time in cryptanalysis by trying to decrypt just a small portion of the ciphertext, and then decrypting the full ciphertext only after the correct shift is determined.

The following ciphertexts were formed using shift ciphers with our alphabet letters in the natural order. For each, use a brute force attack to cryptanalyze the ciphertext.

(e) ESPOZ RDCLY BFTNV WJ

(f) OAOBG UCHHC YBCKV WGZWA WHOHW CBG