Classical Crypto

Q1.

a. What is Atbash?

Atbash is traditional form of Hebrew substitution cipher. It consists of replacing the original index of the letter on the alphabet with the equivalent counting from the end of the alphabet. The name Atbash originates from the substitution of the first and second letters with the last and previous of the Hebrew alphabet.

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

For example lets encrypt the following message:

Plaintext	YOU	CAN	SEE	BUT	YOU	CANT	READ	THIS	MESSAGE
Cyphertext	BKE	WZL	GUU	YEF	BKE	WZLF	HUZV	FRQG	MUGGZSU

b. What is Affine?

The Affine Cipher is a type of classical substitution cipher. It is a combination of the Caesar cipher and a simple multiplicative cipher, operating on the principles of modular arithmetic. The cipher encrypts each letter in the plaintext using a mathematical function and maps it to a corresponding letter in the ciphertext.

The Affine Cipher encrypts a letter using the formula:

$$ E(x) = (a \cdot x + b) \mod m $$

- E(x) is the encrypted value of the letter.
- x is the numeric equivalent of the plaintext letter (e.g., A=0, B=1, C=2, ..., Z=25 for the English alphabet).
- a and b are keys of the cipher, where A must be chosen such that it is coprime with m (the total number of letters in the alphabet, typically 26). This ensures that a has an inverse modulo m , which is needed for decryption. B is the amount of shift applied.
- m is the size of the alphabet (for English, m = 26).

Encryption:

Suppose we are working with the English alphabet and using a = 5 and b = 8 as our keys.

1. Choose a letter from the plaintext, say “C” (which is the 3rd letter, so x = 2).
2. Apply the encryption formula: $$ E(x) = (5 \cdot 2 + 8) \mod 26 = (10 + 8) \mod 26 = 18 $$
3. The letter corresponding to 18 is “S”. So, “C” is encrypted to “S”.

Decryption:

To decrypt, we need to reverse the encryption process using the decryption formula:

\[D(y) = a^{-1} \cdot (y - b) \mod m \]

Where:

```
  • D(y)  is the decrypted value of the ciphertext letter.
  • y  is the numeric equivalent of the ciphertext letter.
  • $$ a^{-1} $$  is the modular inverse of  a  modulo  m . The modular
inverse is the value such that $$ \( (a \cdot a^{-1}) \mod m = 1 \) $$.
```

Using the same keys a = 5 and b = 8 , and ciphertext letter “S” (which is 18):

1. Find the modular inverse of 5 modulo 26. The inverse of 5 is 21 because: \[(5 \cdot 21) \mod 26 = 1 \]
2. Apply the decryption formula: \[D(y) = 21 \cdot (18 - 8) \mod 26 = 21 \cdot 10 \mod 26 = 210 \mod 26 = 2 \]
3. The letter corresponding to 2 is “C”, so the decrypted letter is “C”.

To encrypt the message: “YOUCANTREADMYPLAINTEXT” For reference: A = 0, B = 1, C = 2, …, Z = 25. Convert each letter in the message to its numeric form.
24,14,20,2,0,13,19,17,4,0,3,12,24,15,11,0,8,13,19,4,23,19

Encryption of “You”: Y (24): \[E(24)=(5·24+8)mod26=(120+8)mod26=128mod26=24 \] Y remains Y.

O (14): \[E(14)=(5·14+8)mod26=(70+8)mod26=78mod26=0 \] O becomes A.

U (20): \[E(20)=(5·20+8)mod26=(100+8)mod26=108mod26=4 \] U becomes E.

After all the operations the we get the following cyphertext “YAESIVZPCIXQYFLIWVZCTZ”.

c. What is Playfair?

Playfair is a digraph substitution cipher that encrypts pairs of letters (digraphs) instead of single letters. To do that it makes use of a grid composed of 5 rows and 5 columns, breaks the text to encrypt into pairs of letters and swaps them according to their position in a rectangle on the grid, which makes it more secure than simple substitution ciphers like the Caesar Cipher.

This is a grid with the keyword “Diogo”, since the rules dont allow repetition we exchange the second O with A.

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

Encrypting Pairs of Letters:

The plaintext message is divided into pairs of letters (called digraphs). If there is an odd number of letters, an extra filler letter (usually X) is added to the end. The rules for encryption are: If the two letters in the pair are in the same row, each letter is replaced by the letter to its immediate right (wrapping around to the beginning of the row if needed). If the two letters are in the same column, each letter is replaced by the letter directly below it (wrapping around to the top of the column if needed). If the letters form a rectangle, each letter is replaced by the letter in the same row but in the opposite corner of the rectangle.

Example: Plaintext HELLO WORLD

Prepare the plaintext First, divide the plaintext into pairs of letters (called digraphs). If there is an odd number of letters, or if a pair contains the same letter, insert an “X” between repeated letters or at the end if necessary.

For “HELLO”: Split into digraphs: HE LX LO (we insert X between the two L's to avoid repetition).

Encrypt each pair using the key square We apply the rules of the Playfair Cipher to each digraph:

HE: H is in row 1, column 5. E is in row 2, column 3. These letters form a rectangle. Swap the corners of the rectangle: H is replaced by B (same row as H, same column as E). E is replaced by F (same row as E, same column as H). So, HE becomes BF.

LX: L is in row 3, column 2. X is in row 5, column 3. These letters form a rectangle. Swap the corners of the rectangle: L is replaced by M. X is replaced by W. So, LX becomes MW.

LO: L is in row 3, column 2. O is in row 1, column 3. These letters form a rectangle. Swap the corners of the rectangle: L is replaced by M. O is replaced by I. So, LO becomes MI.

After all the replacements we get the cyphertext “BFMWMIXIWROV”

Rules for Decryption: For each pair (digraph) in the ciphertext:

Same row: Replace each letter with the one to its immediate left (wrapping around if necessary). Same column: Replace each letter with the one directly above it (wrapping around if necessary). Rectangle (different row and column): Swap the corners of the rectangle formed by the letters, using the opposite corners in the same row.

BF:

B is at (2, 1). F is at (1, 4). These form a rectangle. Swap the corners: B becomes H. F becomes E. So, BF becomes HE. MW:

M is at (3, 3). W is at (5, 2). These form a rectangle. Swap the corners: M becomes L. W becomes X. So, MW becomes LX. MI:

M is at (3, 3). I is at (1, 2). These form a rectangle. Swap the corners: M becomes L. I becomes O. So, MI becomes LO.

In the end we get the following plaintext HELLOXWORLD and we remove the filler X and get the original plaintext HELLO WORLD.

d. What is ADFGVX?

ADFGVX is a substitution and transposition cipher used by the German army during the first World War. Name comes from the six letters A, D, F, G, V, and X, which are used as coordinates in a 6×6 polybius square to substitute letters and digits in the plaintext. The result of the cipher introduced a new method called fractionation.

Components of the Cipher: 6×6 Polybius Square:

It consists of 36 characters (26 letters and 10 digits). A keyword is used to fill the square, followed by the remaining letters of the alphabet and the digits 0-9. Each letter or digit in the plaintext is replaced by two of the letters ADFGVX, based on their row and column coordinates in the 6×6 square.
Columnar Transposition:

After substitution, the ciphertext undergoes transposition based on a second keyword, which further scrambles the text.

A 6×6 grid is used, filled with the keyword first, followed by the remaining letters and digits. Here's an example using the keyword "CIPHER":

	A	D	F	G	V	X
A	C	I	P	H	E	R
D	A	B	D	F	G	J
F	K	L	M	N	O	Q
G	S	T	U	V	W	X
V	Y	Z	0	1	2	3
X	4	5	6	7	8	9

The grid has 6 rows and 6 columns. The letters A, D, F, G, V, and X are used to label both rows and columns. The letters and digits are arranged using a keyword ("CIPHER" in this case), followed by the remaining letters of the alphabet and numbers 0-9.

Substitution Step (ADFGVX) For encryption, each letter or digit in the plaintext is replaced by its coordinates in the Polybius square. Each letter is represented by a pair of the letters ADFGVX, based on its position in the grid.

Example Encryption: plaintext "HELLO123".

Find each letter's position in the 6×6 grid: H is in row A, column G → AG E is in row A, column V → AV L is in row F, column D → FD L (again) → FD O is in row F, column X → FX 1 is in row V, column G → VG 2 is in row V, column X → VX 3 is in row X, column X → XX So, the substitution phase results in the ciphertext: AGAVFDXFXVGVXFX.

Columnar Transposition Next, we apply the transposition cipher using another keyword. Let's use the keyword "KEY".

Write the ciphertext into rows under the keyword letters:

K	E	Y

A	G	A
V	F	D
X	F	X
V	G	V
X	X	F

Sort the columns based on the alphabetical order of the keyword (KEY becomes E, K, Y):

E	K	Y
G	A	A
F	V	D
F	X	X
G	V	V
X	X	F

Read the ciphertext column by column in this new order: The final ciphertext is: GFFGXXAVVXADDX.

Decryption To decrypt the ADFGVX cipher, reverse the process:

Reverse the Transposition Knowing the keyword, first undo the columnar transposition by rearranging the ciphertext back into its original columns based on the keyword order. In our example, the keyword “KEY” gives us the column order (E, K, Y). Divide the ciphertext GFFGXXAVVXADDX into columns of the same length as the keyword:

E	K	Y
G	A	A
F	V	D
F	X	X
G	V	V
X	X	F

Then, reorder the columns back to the original order of the keyword (“KEY”):

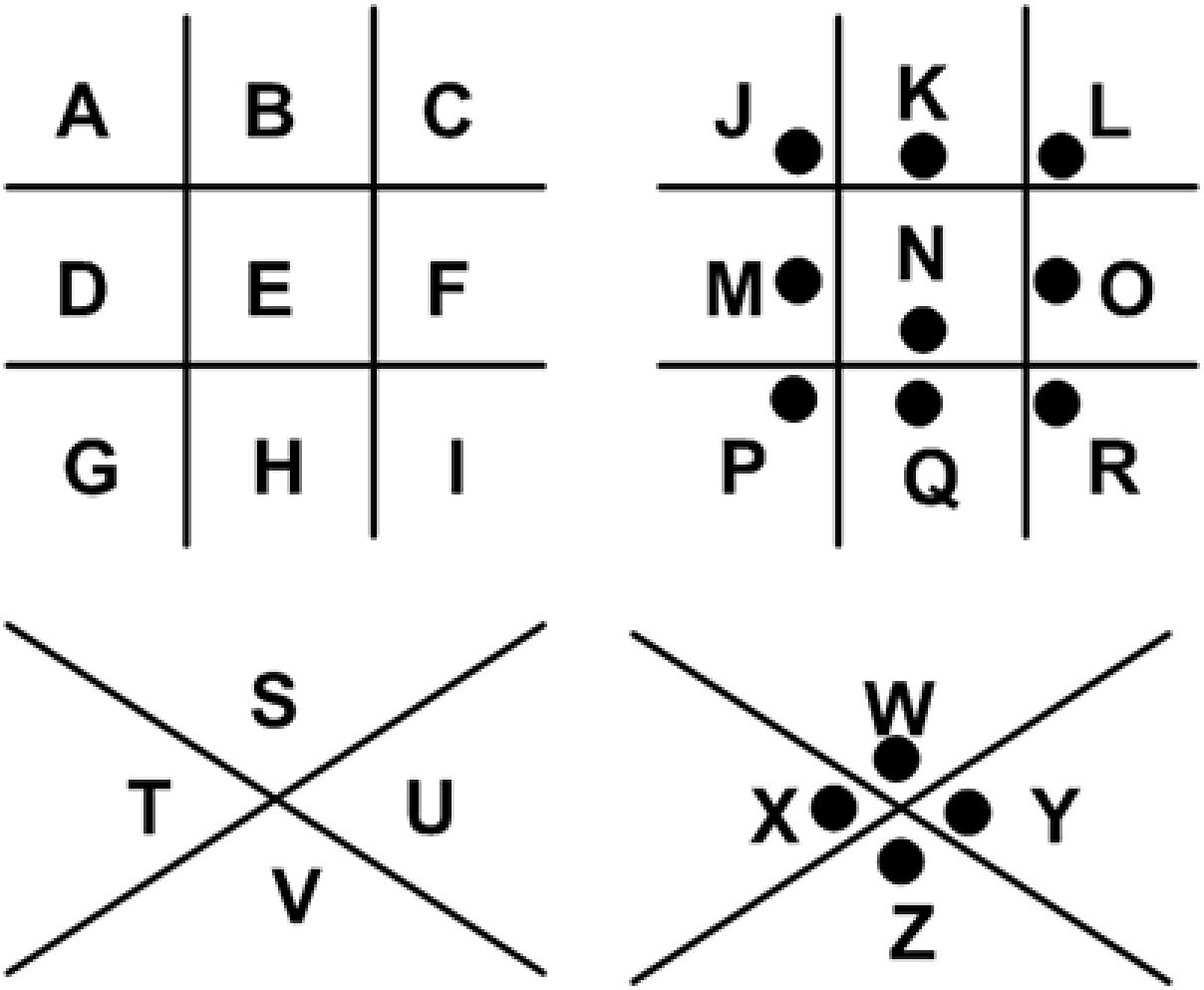
K	E	Y
A	G	A
V	F	D
X	F	X
V	G	V
X	X	F

This restores the original intermediate ciphertext: AGAVFDXFXVGVXFX.

Reverse the Substitution Now, using the Polybius square, reverse the substitution by converting the pairs of ADFGVX back into their corresponding letters and digits. AG → H AV → E FD → L FD → L FX → O VG → 1 VX → 2 XX → 3 The original plaintext is: “HELLO123”.

e. What is Pigpen?

The Pigpen cipher is part of the substitution ciphers but instead of number it uses simple geometric shapes like grids and crosses to map to the letters of the message, making it easy to recognise but harder to decipher if you're not familiar with the symbols.



The letters are described by the their place in the matrix.

Plaintext: X marks the spot Ciphertext:

Q2. Encrypt an English text of at least 80 words using the Vigenere cipher and exchange it with one of your fellow students explain your work

Message

Kqxxp orpq nsqdwqd Utle ue nk hzodzbwqp yfevmsq J trbq kpg kmhq oa sdanmqp pqosksfuzh uw geuos wtq woazxqphq sdahjphp fa ve ek ftf xdn fqbokqde pz rgd rjdvf oxbev. Itudt rr ftf xhofgsqg oubique pue krg ruop padq jzwqdqtflzs mop ztmf jz zme uo krgd aququaz uth qmejqvf fa dddow? Fiuv yqetmjqp ibe hzodzbwqp ijfk m egqqu eqosqw wqk utdf zacagk iumx hhqd guqp. Mruqu odmdwlzs fiuv fqju U gaz'f utlzw kpg zuxx imyq fdpgexqe fhhd ndfmnuzs bzb aftfd. Guasp

Process

Using the Vigenere Cipher tool I wrote my message and encrypted it using the key “DMMMBM”.

Q3. Crack the crypted text of your fellow student using the Vigenere cipher tool explain your work

This is the ciphertext I received:

```
IWBJUXHGEQHIPXNGECMCSUFYQUBJXVRJUXHGEQOIVM
AIGGRCSUMVNKDADETISKTXNPJOPWPLGCTOEHPBQNYJDLVX
E
YMAPHVIXEQOJNAXHBIKWNDMASZQODLWENVSUMALRVOFIG
M RFIEQWITJFSVTPBWRCSBEOCTDIGIAVODLTSXKLVIIAAFFVM
ETUGPKRRAXGUXXXLTQLNICBEQWXXGYGQMKOTTUGMKWIH
VP
ACTDSFKBVIHEEXEGMIHCQWNIGEQEIXRPMBPPKRRAXGSIVJ
PZCPVIHYEWPPVJIGUCRSROYCTOWERRCDYVDTUGRMSCDVO
EX
XHTBTEKRNEKEECWXNGJEPVXDTGAXHSOAQTUITPSQRVSCG
RT TRECTUTEOHPYF
```

The Index of Coincidence (IC) analysis points to the key lengths of 7 with the highest value of 0.0596. The value is closer to the typical IC for English text (around 0.065).

Upon seeing partially decrypted segments that could relate to the text’s theme (like “FLOUR” or “MILK”), I assumed that the keyword was something relevant to these ingredients. Words related to specific themes (like “RECIPE,” “BAKING,” or “PANCAKE”) were some of my logical guesses.

Using the Vigenere cipher with the key “PANCAKE” the plain text is the following

```
TWOHUNDREDFIFTYGRAMSOFFLOURFIVEHUNDREDMILI
LITERSOFMILKTWOEGGSAPINCHOFSALTATEASPOONOFOLIVE
OILPUTINABOWLANDMIXUNTILSMOOTHHEATSKILLETOVERM
EDIUMHIGHFIREPOURSOMEBATTERINTOTHESKILLETANDFLI
PTHEPANCAKEUNTILGOLDENBROWNTRYTOMAKETHEMASTHI
N
ASPOSSIBLESERVEWITHPOWDEREDCINNAMONPANCAKESYRU
PMAPLESYRUPFRUITSCHOCOLATESPREADOROTHERCONDIME
N
TSTOREANYEXCESSINTHEFRIDGEANDDONOTKEEPFORLONGE
R THANTHREEDAYS
```

4. Go through the previous two steps again, this time using a cipher of your own choosing. Do not tell your fellow student what cipher you used!

I've received the last encrypted message

> OSHL ST FMSOL YMS YSDQ TSDXLO PDL FML OPHL FMPF NLPD XDSOOLO

To decipher the text “OSHL ST FMSOL YMS YSDQ TSDXLO PDL FML OPHL FMPF NLPD XDSOOLO” first I used the online tool https://www.dcode.fr/cipher-identifier to do the initial analysis and explore assume which cipher was most likely used. After that I started looking based on the results it provided.

Using ROT-13 which was the most likely didn't where I shifted all the letters of the alphabet 13 and apply on top of it didnt achieve any english possible translation. “BFUY FG SZFBY LZF LFQD GFQKYB CQY SZY BCUY SZCS AYCQ KQFBBYB” so I went to the 2nd cipher on that list which was Caeser.

The tool gave provided me with more gibberish and the most close to english was this one after doing a extensive search. “DHWA HI UBHDA NBH NHSF IHSMAD ESA UBA DEWA UBEU CAES MSHDDAD”.

After I tried Mono-alphabetic Substitution and I got the following result.

The plaintext message is

> SOME OF THOSE WHO WORK FORCES ARE THE SAME THAT LEAR CROSSES