Quiz 4

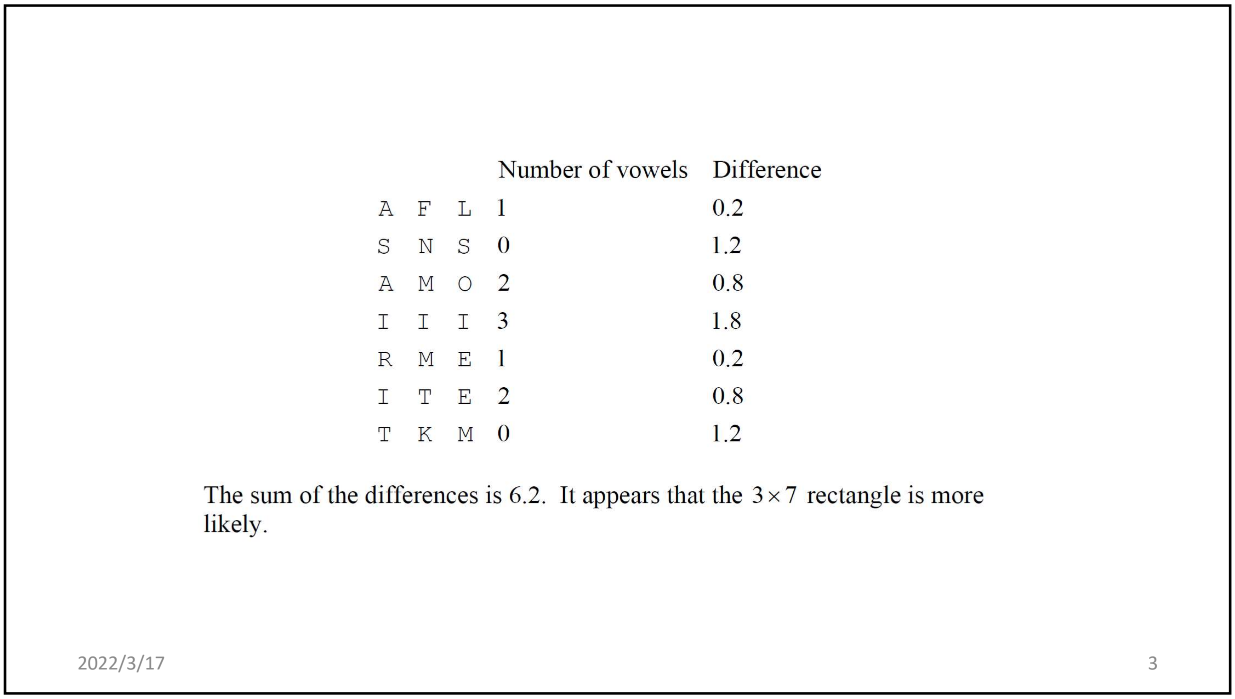
- In this assignment, we will learn using Markov chain methods to attack classical columnar transposition ciphers automatically.
- The steps to solve it are as follows:

1. Using the number of vowels to detect ciphertext rectangles (In English approximately 40% of plaintext consists of vowels).
2. Using plaintext bigrams and trigrams to calculate conditional probabilities for Markov decision processing (MDP).
3. Using MDP to recover columnar transposition ciphers.

Transposition Columnar Transposition Diffusion

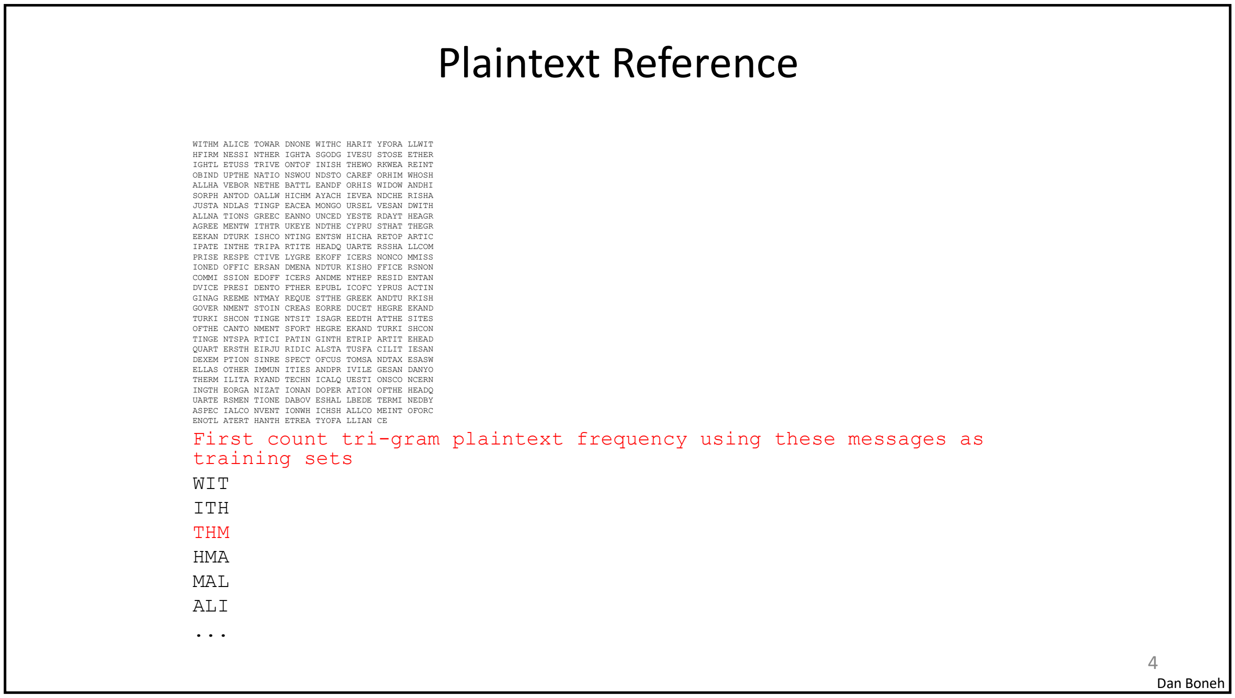
ECDTM ECAER AUOOL
EDSAM MERNE
NASSO DYTNR VBNLC
RLTIQ
LAETR IGAWE BAAEI
HOR

9



			Number of vowels	Difference
A	F	L	1	0.2
S	N	S	0	1.2
A	M	O	2	0.8
I	I	I	3	1.8
R	M	E	1	0.2
I	T	E	2	0.8
T	K	M	0	1.2

The sum of the differences is 6.2. It appears that the 3 × 7 rectangle is more likely.



Plaintext Reference

```
WITHM ALICE TOWAR DNONE WITHC HARIT YFORA LLWIT
HFIRM NESSI NTHER IGHTA SGODG IVESU STOSE ETHER
IGHTL ETUSS TRIVE ONTOF INISH THEWO RKWEA REINT
OBIND UPTHE NATIO NSWOU NDSTO CAREF ORHIM WHOSH
ALLHA VEBOR NETHE BATTL EANDF ORHIS WIDOW ANDHI
SORPH ANTOD OALLW HICHM AYACH IEVEA NDCHE RISHA
JUSTA NDLAS TINGP EACEA MONGO URSEL VESAN DWITH
ALLNA TIONS GREEC EANNO UNCED YESTE RDAYT HEAGR
AGREE MENTW ITHTR UKEYE NDTHE CYPRU STHAT THEGR
EEKAN DTURK ISHCO NTING ENTSW HICHA RETOP ARTIC
IPATE INTHE TRIPA RTITE HEADQ UARTE RSSHA LLCOM
PRISE RESPE CTIVE LYGRE EKOFF ICERS NONCO MMISS
IONED OFFIC ERSAN DMENA NDTUR KISHO FFICE RSNON
COMMI SSION EDOFF ICERS ANDME NTHEP RESID ENTAN
DVICE PRESI DENTO FTHER EPUBL ICOFC YPRUS ACTIN
GINAG REEME NTMAY REQUE STTHE GREEK ANDTU RKISH
GOVER NMENT STOIN CREAS EORRE DUCET HEGRE EKAND
TURKI SHCON TINGE NTSIT ISAGR EEDTH ATTHE SITES
OFTHE CANTO NMENT SFORT HEGRE EKAND TURKI SHCON
TINGE NTSPA RTICI PATIN GINTH ETRIP ARTIT EHEAD
QUART ERSTH EIRJU RIDIC ALSTA TUSFA CILIT IESAN
DEXEM PTION SINRE SPECT OFCUS TOMSA NDTAX ESASW
ELLAS OTHER IMMUN ITIES ANDPR IVILE GESAN DANYO
THERM ILITA RYAND TECHN ICALQ UESTI ONSCO NCERN
INGTH EORGA NIZAT IONAN DOPER ATION OFTHE HEADQ
UARTE RSMEN TIONE DABOV ESHAL LBEDE TERMI NEDBY
ASPEC IALCO NVENT IONWH ICHSH ALLCO MEINT OFORC
ENOTL ATERT HANTH ETREA TYOFA LLIAN CE
```

First count tri-gram plaintext frequency using these messages as training sets

WIT
ITH
THM
HMA
MAL
ALI
...

Tri-gram plaintext to calculate conditional probability

WORD	Frequency
THE	***A*** like 5 times
THA	***B*** like 2 times
CAR	***C***
CAN	***D***

Weight (THE)=
Log Pc(THE/TH)
=log (***A*** / ***A***+***B***)
= log 5/7

WORD	Frequency
THE	***A*** ***5***
THA	***B*** ***2***
CAR	***C***
CAN	***D***

W(THE)=
Log Pc(THE/TH) / Random
=log (***A / A***+***B***)/(1/26)
= log 26*(5/7)

L	A	S			
A	M	S			
E	M	O			
T	E	D			
R	R	Y			
I	N	T			
G	E	N			
A	N	R			
W	A	V			

We can use Markov chain methods to attack classical columnar transposition ciphers automatically for our assignment last week. That is a supervised learning approaches.

Then, Write a program to solve these transposition using a supervised learning approach- Markov chain methods

EOEYE GTRNP SECEH
HETYH SNGND DDDET
OCRAE RAEMH
TECSE USIAR WKDRI
RNYAR ANUEY ICNTT
CEIET US

Hint: the first three letters of the plaintext message are **GRE** ….