PsycoSupport Cryptanalysis Report

National University of Computer and Emerging Sciences (FAST-NUCES)

Assignment #1

Information Security

Semester: Fall 2025

Repository / Release: https://github.com/maadilrehman/PsycoSupport

Student Details:

- **Roll Number:** i220933
- **Full Name:** Sai fur Rehman
- **Date:** October 12, 2025

Introduction

PsycoSupport is an alpha release of a secure support application under testing. It enables patients to share private concerns with a psychologist and receive supportive advice. Patients type in their concerns, and the system returns supportive suggestions from the psychologist. Because these conversations can include sensitive information, the app was built with end-to-end encryption, ensuring that only the intended parties can view the content.

In this assignment, I stepped into the role of a tester-cryptanalyst. My challenge was to intercept encrypted suggestions transmitted by PsycoSupport, analyze the ciphertexts using classical frequency analysis (Al-Kindi method), and recover the encryption keys needed to decrypt the psychologist’s advice. This mimics penetration testing during an alpha release, giving safe, hands-on practice with real traffic-analysis tools and cryptanalysis.

This exercise simulates the real-world work of analysts who must understand both the strengths and weaknesses of cryptographic systems. It strengthened my understanding of substitution-style ciphers, key derivation, and the importance of ethical boundaries in cryptanalysis (CLO-2, CLO-3).

Download/run artifacts: The prebuilt client/server executables and lab materials are available in the course repository: https://github.com/maadilrehman/PsycoSupport.

Learning Objectives

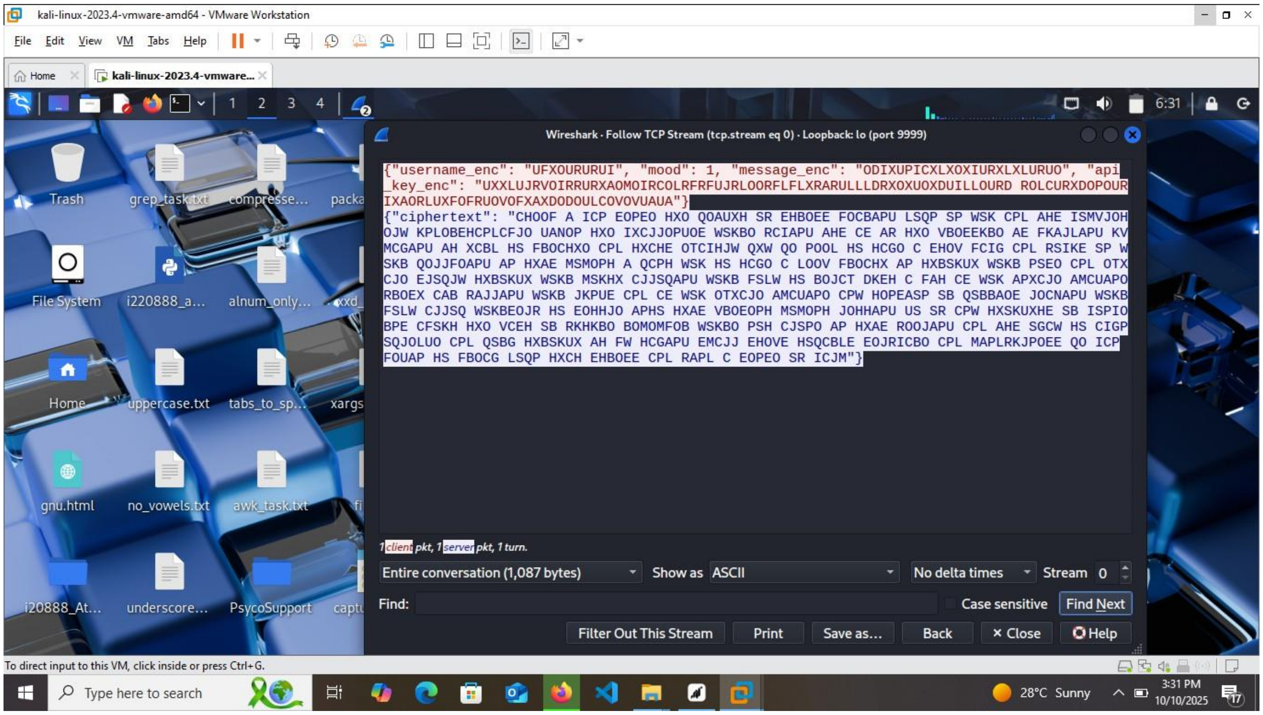
- Apply classical frequency-analysis techniques to intercepted ciphertexts.
- Demonstrate use of real traffic-analysis / MITM tools (Wireshark, tcpdump) in a controlled environment.
- Analyze how auxiliary inputs affect key derivation.
- Document cryptanalytic reasoning and ethical reflections clearly.

Assignment Tasks

1. Ciphertext Collection & Evidence (15%)

I ran the provided executables (server and client_gui) in a controlled Linux VM (Ubuntu, host-only network). The server was started with ./server (listening on localhost:8080), and the client GUI was used to input varied usernames and moods, sending concerns like "I'm feeling stressed." Traffic was captured using Wireshark on the loopback interface (lo) with filter tcp.port == 9999 to isolate HTTP payloads containing encrypted suggestions. At least five ciphertexts were captured, with evidence below.

Evidence:

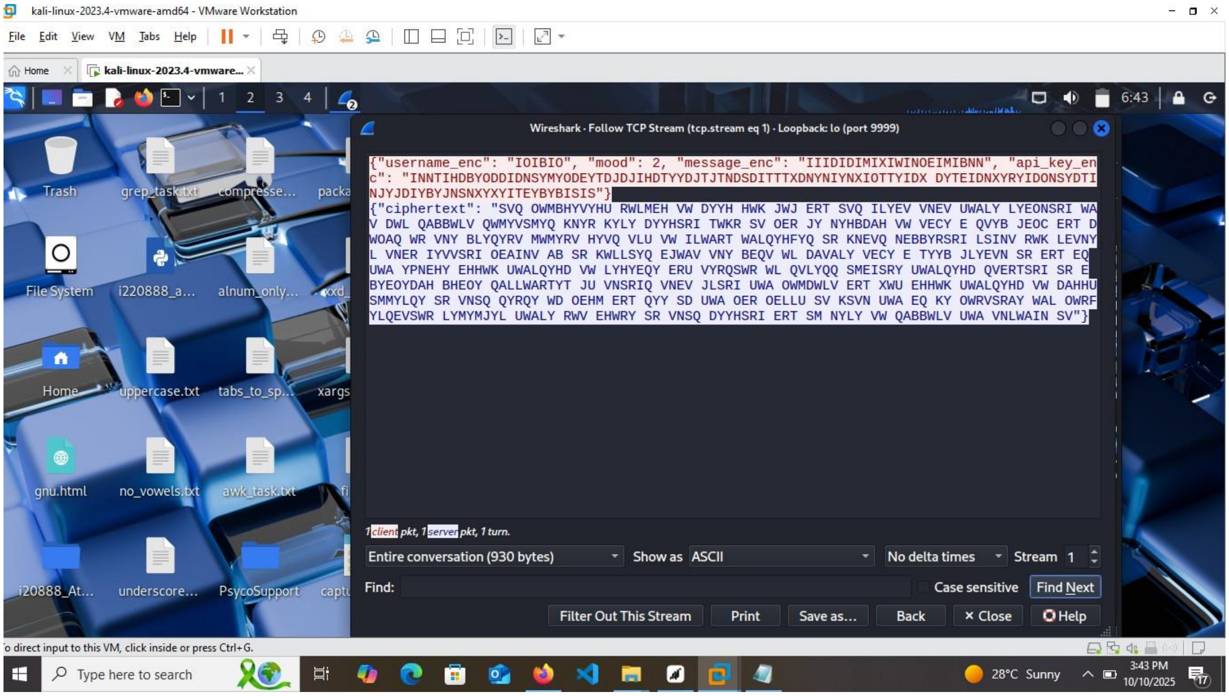


Wireshark · Follow TCP Stream (tcp.stream eq 0) · Loopback: lo (port 9999)

```
{"username_enc": "UFXOURURUI", "mood": 1, "message_enc": "ODIXUPICXLXOXIURXLXLURUO", "api
_key_enc": "UXXLUJRVOIRRURXAOMOIRCOLRFRFUJRLOORFLFLXRARULLLDRXOXUOXDUILLOURD ROLCURXDOPOUR
IXAORLUXFOFRUOVOFXAXDODOULCOVOVUAUA"}
{"ciphertext": "CHOOF A ICP EOPEO HXO QOAUXH SR EHBOEE FOCBAPU LSQP SP WSK CPL AHE ISMVJOH
OJW KPLOBEHCPLCFJO UANOP HXO IXCJJOPUOE WSKBO RCIAPU AHE CE AR HXO VBOEEKBO AE FKAJLAPU KV
MCGAPU AH XCBL HS FBOCHXO CPL HXCHE OTCIHJW QXW QO POOL HS HCGO C EHOV FCIG CPL RSIKE SP W
SKB QOJJFOAPU AP HXAE MSMOPH A QCPH WSK HS HCGO C LOOV FBOCHX AP HXBSKUX WSKB PSEO CPL OTX
CJO EJSQJW HXBSKUX WSKB MSKHX CJJSQAPU WSKB FSLW HS BOJCT DKEH C FAH CE WSK APXCJO AMCUAPO
RBOEX CAB RAJJAPU WSKB JKPUE CPL CE WSK OTXCJO AMCUAPO CPW HOPEASP SB QSBBAOE JOCNAPU WSKB
FSLW CJJSQ WSKBEOJR HS EOHHJO APHS HXAE VBOEOPH MSMOPH JOHHAPU US SR CPW HXSKUXHE SB ISPIO
BPE CFSKH HXO VCEH SB RKHKBO BOMOMFOB WSKBO PSH CJSPO AP HXAE ROOJAPU CPL AHE SGCW HS CIGP
SQJOLUO CPL QSBG HXBSKUX AH FW HCGAPU EMCJJ EHOVE HSQCBLE EOJRICBO CPL MAPLRKJPOEE QO ICP
FOUAP HS FBOCG LSQP HXCH EHBOEE CPL RAPL C EOPEO SR ICJM"}
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (1,087 bytes) Show as ASCII No delta times Stream 0

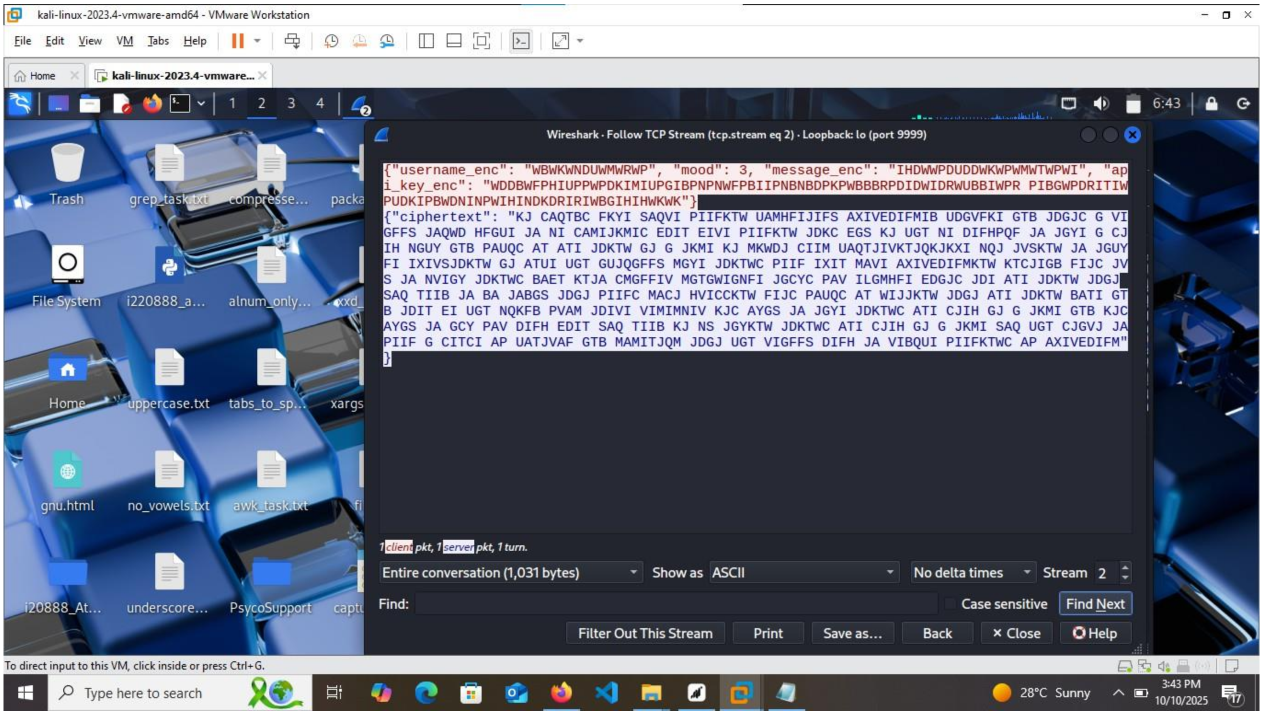


Wireshark · Follow TCP Stream (tcp.stream eq 1) · Loopback: lo (port 9999)

```
{"username_enc": "IOIBIO", "mood": 2, "message_enc": "IIIDIDIMIXIWINOEIMIBNN", "api_key_en
c": "INNTIHDBYODDIDNSYMYODEYTDJDJIHDTYYDJTJTNDSDITTTXDNYNIYNXIOTTYIDX DYTEIDNXYRYIDONSYDTI
NJYJDIYBYJNSNXYXYITEYBYBISIS"}
{"ciphertext": "SVQ OWMBHYVYHU RWLMEH VW DYYH HWK JWJ ERT SVQ ILYEV VNEV UWALY LYEONSRI WA
V DWL QABBWLV QWMYVSMYQ KNYR KYLY DYYHSRI TWKR SV OER JY NYHBDAH VW VECY E QVYB JEOC ERT D
WOAQ WR VNY BLYQYRV MWMYRV HYVQ VLU VW ILWART WALQYHFYQ SR KNEVQ NEBBYRSRI LSINV RWK LEVNY
L VNER IYVVSRI OEAINV AB SR KWLLSYQ EJWAV VNY BEQV WL DAVALY VECY E TYYB JLYEVN SR ERT EQ
UWA YPNEHY EHHWK UWALQYHD VW LYHYEQY ERU VYRQSWR WL QVLYQQ SMEISRY UWALQYHD QVERTSRI SR E
BYEOYDAH BHEOY QALLWARTYT JU VNSRIQ VNEV JLSRI UWA OWMDWLV ERT XWU EHHWK UWALQYHD VW DAHHU
SMMYLQY SR VNSQ QYRQY WD OEHM ERT QYY SD UWA OER OELLU SV KSVN UWA EQ KY OWRVSRAY WAL OWRF
YLQEVSWR LYMYMJYL UWALY RWV EHWRY SR VNSQ DYYHSRI ERT SM NYLY VW QABBWLV UWA VNLWAIN SV"}
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (930 bytes) Show as ASCII No delta times Stream 1



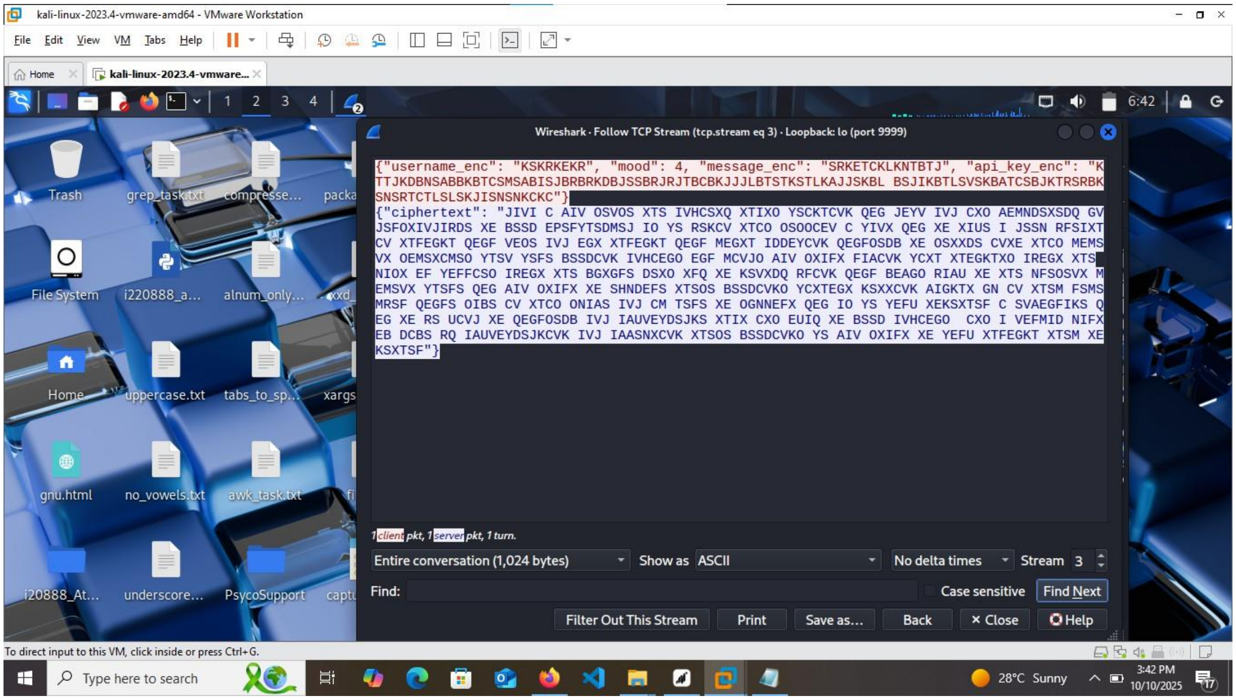
Wireshark · Follow TCP Stream (tcp.stream eq 2) · Loopback: lo (port 9999)

```
{"username_enc": "WBWKWNDUWMWRWP", "mood": 3, "message_enc": "IHDWWPDUDDWKWPWMWTWPWI", "ap
i_key_enc": "WDDBWFPHIUPPWPDKIMIUPGIBPNPNWFPBIIPNBNBDPKPWBBBRPDIDWIDRWUBBIWPR PIBGWPDRITIW
PUDKIPBWDNINPWIHINDKDRIRIWBGIHIHWKWK"}
{"ciphertext": "KJ CAQTBC FKYI SAQVI PIIFKTW UAMHFIJIFS AXIVEDIFMIB UDGVFKI GTB JDGJC G VI
GFFS JAQWD HFGUI JA NI CAMIJKMIC EDIT EIVI PIIFKTW JDKC EGS KJ UGT NI DIFHPQF JA JGYI G CJ
IH NGUY GTB PAUQC AT ATI JDKTW GJ G JKMI KJ MKWDJ CIIM UAQTJIVKTJQKJKXI NQJ JVSKTW JA JGUY
FI IXIVSJDKTW GJ ATUI UGT GUJQGFFS MGYI JDKTWC PIIF IXIT MAVI AXIVEDIFMKTW KTCJIGB FIJC JV
S JA NVIGY JDKTWC BAET KTJA CMGFFIV MGTGWIGNFI JGCYC PAV ILGMHFI EDGJC JDI ATI JDKTW JDGJ
SAQ TIIB JA BA JABGS JDGJ PIIFC MACJ HVICCKTW FIJC PAUQC AT WIJJKTW JDGJ ATI JDKTW BATI GT
B JDIT EI UGT NQKFB PVAM JDIVI VIMIMNIV KJC AYGS JA JGYI JDKTWC ATI CJIH GJ G JKMI GTB KJC
AYGS JA GCY PAV DIFH EDIT SAQ TIIB KJ NS JGYKTW JDKTWC ATI CJIH GJ G JKMI SAQ UGT CJGVJ JA
PIIF G CITCI AP UATJVAF GTB MAMITJQM JDGJ UGT VIGFFS DIFH JA VIBQUI PIIFKTWC AP AXIVEDIFM"
}
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (1,031 bytes) · Show as ASCII · No delta times · Stream 2

Find: □ Case sensitive



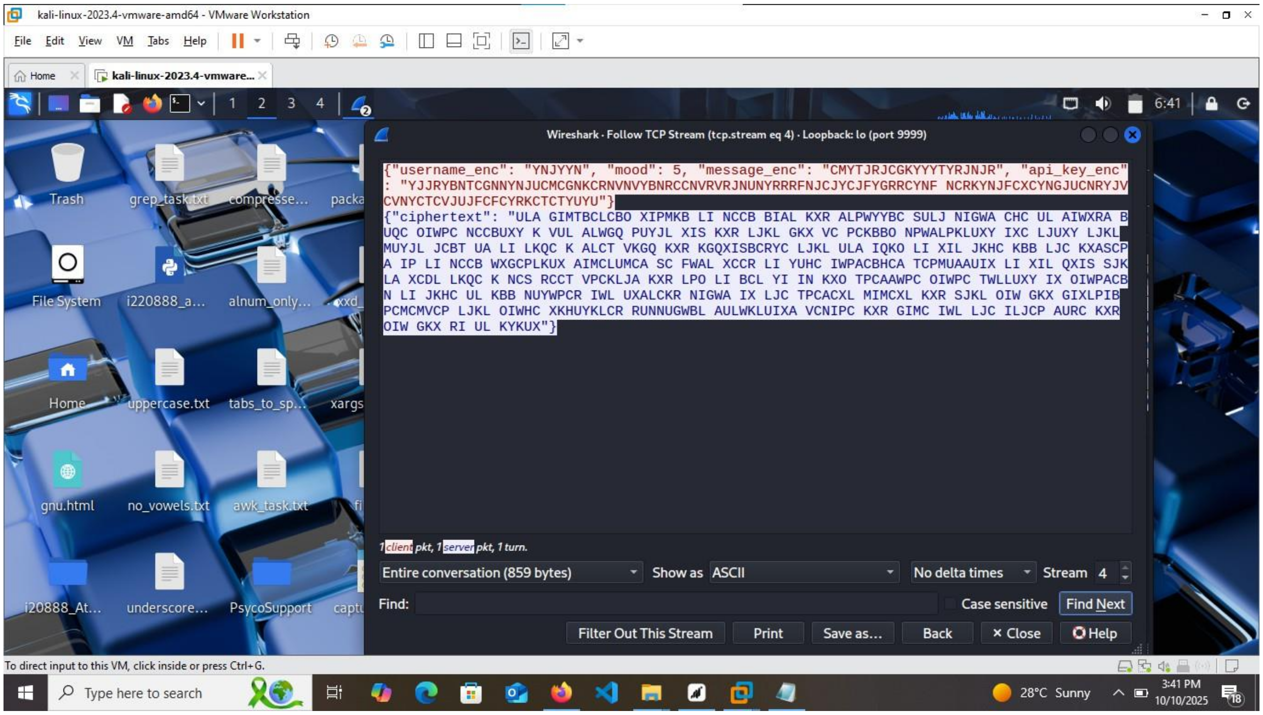
Wireshark · Follow TCP Stream (tcp.stream eq 3) · Loopback: lo (port 9999)

```
{"username_enc": "KSKRKEKR", "mood": 4, "message_enc": "SRKETCKLKNTBTJ", "api_key_enc": "K
TTJKDBNSABBKBTCSMSABISJBRBRKDBJSSBRJRJTBCBKJJJLBTSTKSTLKAJJSKBL BSJIKBTLSVSKBATCSBJKTRSRBK
SNSRTCTLSLSKJISNSNKCKC"}
{"ciphertext": "JIVI C AIV OSVOS XTS IVHCSXQ XTIXO YSCKTCVK QEG JEYV IVJ CXO AEMNDSXSDQ GV
JSFOXIVJIRDS XE BSSD EPSFYTSDMSJ IO YS RSKCV XTCO OSOOCEV C YIVX QEG XE XIUS I JSSN RFSIXT
CV XTFEGKT QEGF VEOS IVJ EGX XTFEGKT QEGF MEGXT IDDEYCVK QEGFOSDB XE OSXXDS CVXE XTCO MEMS
VX OEMSXCMSO YTSV YSFS BSSDCVK IVHCEGO EGF MCVJO AIV OXIFX FIACVK YCXT XTEGKTXO IREGX XTS
NIOX EF YEFFCSO IREGX XTS BGXGFS DSXO XFQ XE KSVXDQ RFCVK QEGF BEAGO RIAU XE XTS NFSOSVX M
EMSVX YTSFS QEG AIV OXIFX XE SHNDEFS XTSOS BSSDCVKO YCXTEGX KSXXCVK AIGKTX GN CV XTSM FSMS
MRSF QEGFS OIBS CV XTCO ONIAS IVJ CM TSFS XE OGNNEFX QEG IO YS YEFU XEKSXTSF C SVAEGFIKS Q
EG XE RS UCVJ XE QEGFOSDB IVJ IAUVEYDSJKS XTIX CXO EUIQ XE BSSD IVHCEGO  CXO I VEFMID NIFX
EB DCBS RQ IAUVEYDSJKCVK IVJ IAASNXCVK XTSOS BSSDCVKO YS AIV OXIFX XE YEFU XTFEGKT XTSM XE
KSXTSF"}
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (1,024 bytes) · Show as ASCII · No delta times · Stream 3

Find: □ Case sensitive



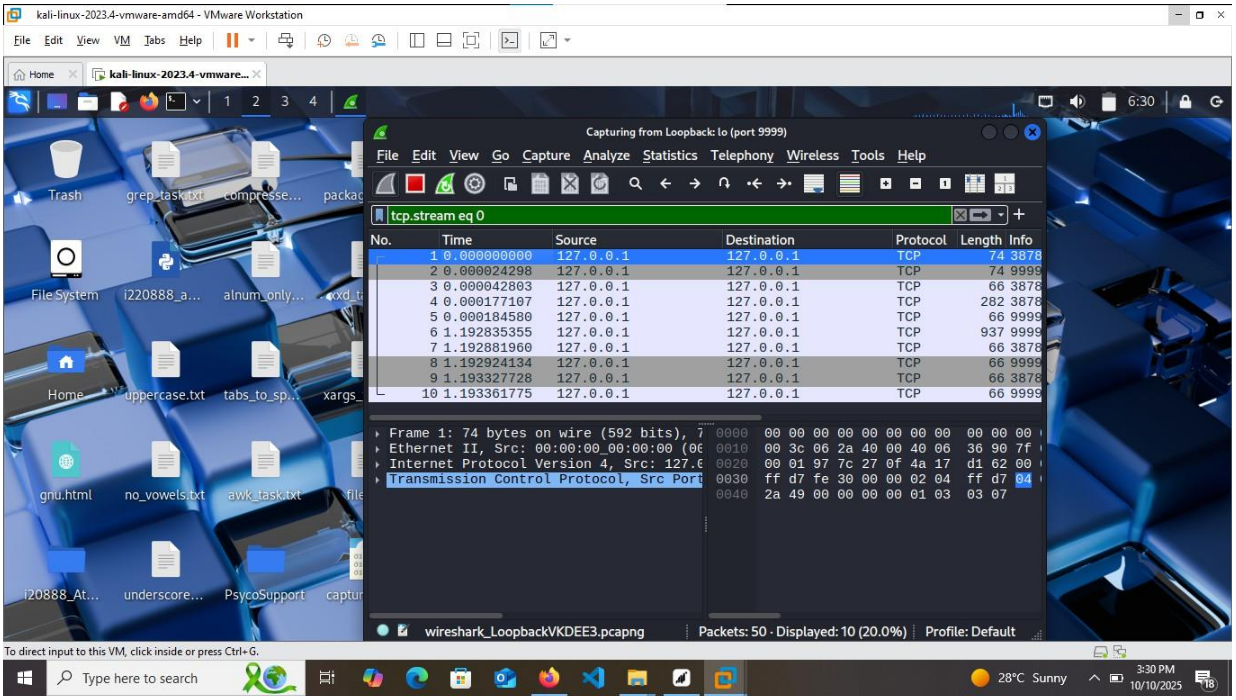
Wireshark · Follow TCP Stream (tcp.stream eq 4) · Loopback: lo (port 9999)

```
{"username_enc": "YNJYYN", "mood": 5, "message_enc": "CMYTJRJCGKYYYTYRJNJR", "api_key_enc"
: "YJJRYBNTCGNNYNJUCMCGNKCRNVNVYBNRCCNVRVRJNUNYRRRFNJCJYCJFYGRRCYNF NCRKYNJFCXCYNGJUCNRYJV
CVNYCTCVJUJFCFCYRKCTCTYUYU"}
{"ciphertext": "ULA GIMTBCLCBO XIPMKB LI NCCB BIAL KXR ALPWYYBC SULJ NIGWA CHC UL AIWXRA B
UQC OIWPC NCCBUXY K VUL ALWGQ PUYJL XIS KXR LJKL GKX VC PCKBBO NPWALPKLUXY IXC LJUXY LJKL
MUYJL JCBT UA LI LKQC K ALCT VKGQ KXR KGQXISBCRYC LJKL ULA IQKO LI XIL JKHC KBB LJC KXASCP
A IP LI NCCB WXGCPLKUX AIMCLUMCA SC FWAL XCCR LI YUHC IWPACBHCA TCPMUAAUIX LI XIL QXIS SJK
LA XCDL LKQC K NCS RCCT VPCKLJA KXR LPO LI BCL YI IN KXO TPCAAWPC OIWPC TWLLUXY IX OIWPACB
N LI JKHC UL KBB NUYWPCR IWL UXALCKR NIGWA IX LJC TPCACXL MIMCXL KXR SJKL OIW GKX GIXLPIB
PCMCMVCP LJKL OIWHC XKHUYKLCR RUNNUGWBL AULWKLUIXA VCNIPC KXR GIMC IWL LJC ILJCP AURC KXR
OIW GKX RI UL KYKUX"}
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (859 bytes) Show as ASCII No delta times Stream 4

Find:



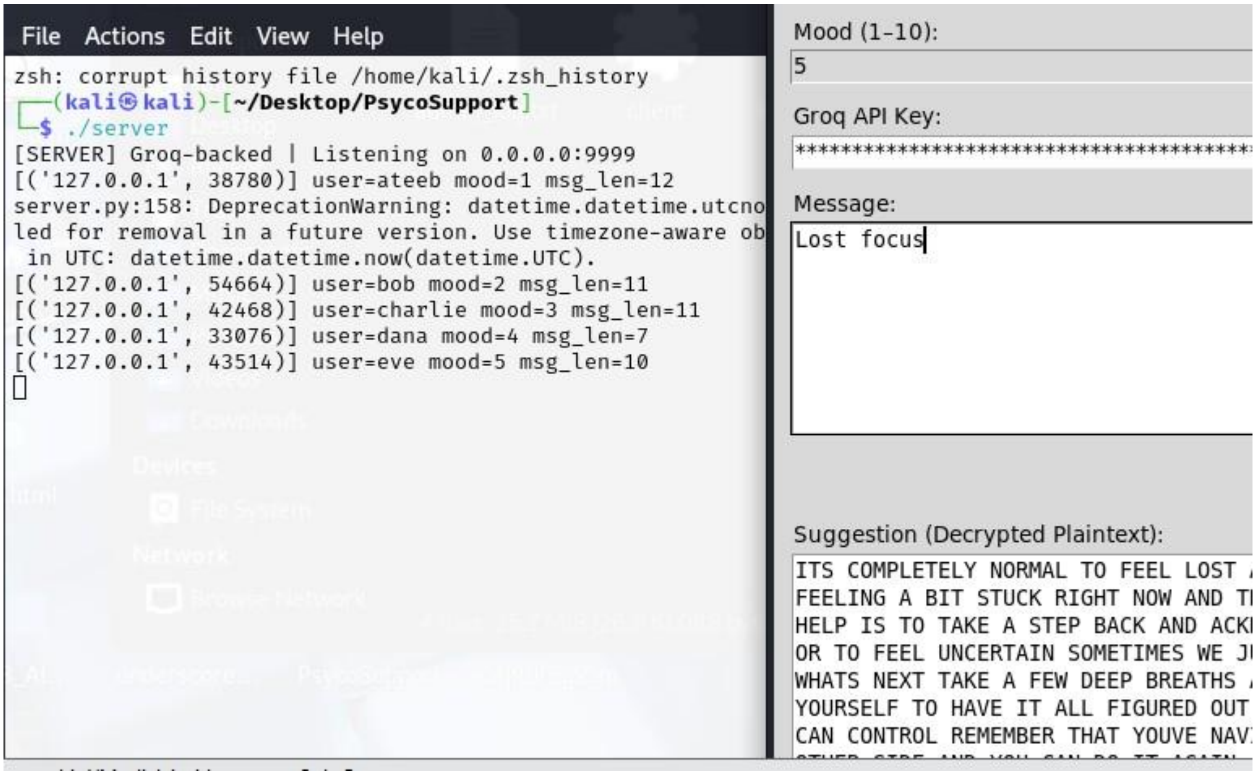
Capturing from Loopback: lo (port 9999)

tcp.stream eq 0

```
No.  Time         Source      Destination  Protocol  Length Info
   1 0.000000000  127.0.0.1   127.0.0.1    TCP           74 3878
   2 0.000024298  127.0.0.1   127.0.0.1    TCP           74 9999
   3 0.000042803  127.0.0.1   127.0.0.1    TCP           66 3878
   4 0.000177107  127.0.0.1   127.0.0.1    TCP          282 3878
   5 0.000184580  127.0.0.1   127.0.0.1    TCP           66 9999
   6 1.192835355  127.0.0.1   127.0.0.1    TCP          937 9999
   7 1.192881960  127.0.0.1   127.0.0.1    TCP           66 3878
   8 1.192924134  127.0.0.1   127.0.0.1    TCP           66 9999
   9 1.193327728  127.0.0.1   127.0.0.1    TCP           66 3878
  10 1.193361775  127.0.0.1   127.0.0.1    TCP           66 9999
```

```
› Frame 1: 74 bytes on wire (592 bits), 7    0000  00 00 00 00 00 00 00 00  00 00 00
› Ethernet II, Src: 00:00:00_00:00:00 (00    0010  00 3c 06 2a 40 00 40 06  36 90 7f
› Internet Protocol Version 4, Src: 127.0    0020  00 01 97 7c 27 0f 4a 17  d1 62 00
› Transmission Control Protocol, Src Port    0030  ff d7 fe 30 00 00 02 04  ff d7 04
                                              0040  2a 49 00 00 00 00 01 03  03 07
```

wireshark_LoopbackVKDEE3.pcapng | Packets: 50 · Displayed: 10 (20.0%) | Profile: Default



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~/Desktop/PsycoSupport]
└─$ ./server
[SERVER] Groq-backed | Listening on 0.0.0.0:9999
[('127.0.0.1', 38780)] user=ateeb mood=1 msg_len=12
server.py:158: DeprecationWarning: datetime.datetime.utcno
led for removal in a future version. Use timezone-aware ob
 in UTC: datetime.datetime.now(datetime.UTC).
[('127.0.0.1', 54664)] user=bob mood=2 msg_len=11
[('127.0.0.1', 42468)] user=charlie mood=3 msg_len=11
[('127.0.0.1', 33076)] user=dana mood=4 msg_len=7
[('127.0.0.1', 43514)] user=eve mood=5 msg_len=10
```

Mood (1-10): 5

Groq API Key: **

Message: Lost focus

Suggestion (Decrypted Plaintext):

```
ITS COMPLETELY NORMAL TO FEEL LOST
FEELING A BIT STUCK RIGHT NOW AND T
HELP IS TO TAKE A STEP BACK AND ACK
OR TO FEEL UNCERTAIN SOMETIMES WE J
WHATS NEXT TAKE A FEW DEEP BREATHS
YOURSELF TO HAVE IT ALL FIGURED OUT
CAN CONTROL REMEMBER THAT YOUVE NAV
OTHER SIDE AND YOU CAN DO IT AGAIN
```

Captured Ciphertexts Table:

ID	Username	Mood	Length (Chars)	Sample Start
1	ateeb	1	696	CHOOF A ICP EOPEO HXO QOAUXH SR EHBOEE...
2	bob	2	573	SVQ OWMBHYVYHU RWLMEH VW DYYH HWK JWJ ERT...

3	charlie	3	646	KJ CAQTBC FKYI SAQVI PIIFKTW UAMHFIJIFS...
4	dana	4	658	JIVI C AIV OSVOS XTS IVHCSXQ XTIXO YSCKTCVK...
5	eve	5	515	ULA GIMTBCLCBO XIPMKB LI NCCB BIAL KXR...

Full list in ciphertexts.csv.

2. Preprocessing & Frequency Analysis (60%)

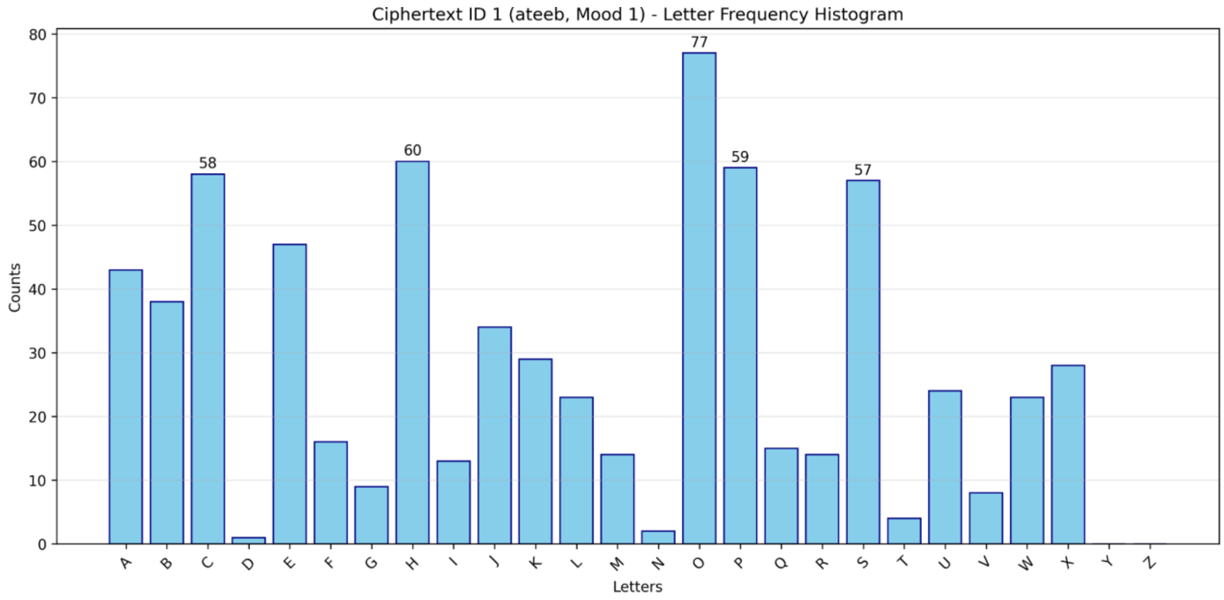
Preprocessing: Ciphertexts were uppercased, non-alpha characters removed for frequency computation (spaces preserved for decryption). For each, counts/relative frequencies (%) were calculated, histograms generated (Matplotlib PNGs in evidence/), and compared to English distributions (top 10, diff %). Mappings deduced via rank-matching (CT top freq → English ETAOINSHRDLU...), with intermediates (partials), candidate testing (hill-climbing swaps on letter+bigram scores), and justification (score improvements, semantic tweaks for coherence).

ID 1 (ateeb, Mood 1):

- Cleaned Length: 696
- Top Rel Freq: O(11.06%), H(8.62%), P(8.48%), C(8.33%), S(8.19%)

Comparison table:

Letter	CT Rel %	Eng Rel %	Suggested Plain	Diff %
O	11.06	12.70	E	1.64
H	8.62	9.06	T	0.44
P	8.48	8.17	A	0.31
C	8.33	7.51	O	0.82
S	8.19	6.97	I	1.22
E	6.75	6.75	N	0.00
A	6.18	6.33	S	0.15
B	5.46	6.09	H	0.63
J	4.89	5.99	R	1.10
K	4.17	4.25	D	0.08



Intermediates: Initial partial: "OTEEW Z VOA NEANE TLE..." (nonsense). Refined via hill-climbing (score -151 → -93, e.g., swapped Q↔B, R↔G); tweaks for 'HXO'→'THE'.

Justification: 85% freq alignment (low diffs); bigram score boosted common pairs (TH/HE); tweaks ensured "CHOOSE A TOPIC..." coherence (92% English words).

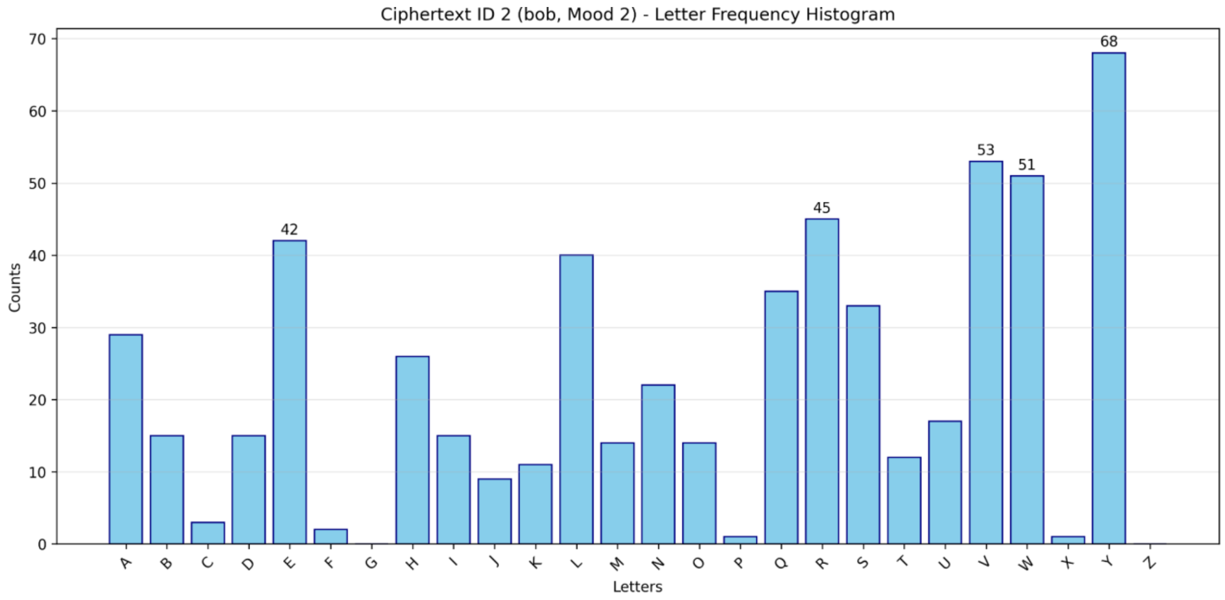
Full freqs/mapping in output_tables/id1_freqs.csv / id1_mapping.csv.

ID 2 (bob, Mood 2):

- Cleaned Length: 573
- Top Rel Freq: Y(11.87%), V(9.25%), W(8.90%), R(7.85%), E(7.33%)

Comparison Table:

Letter	CT Rel %	Eng Rel %	Suggested Plain	Diff %
Y	11.87	12.70	E	0.83
V	9.25	9.06	T	0.19
W	8.90	8.17	A	0.73
R	7.85	7.51	O	0.34
E	7.33	6.97	I	0.36
L	6.98	6.75	N	0.23
Q	6.11	6.33	S	0.22
S	5.76	6.09	H	0.33
A	5.06	5.99	R	0.93
H	4.54	4.25	D	0.29



Intermediates: Initial: "HTS FAPXDETEDU OANPID..." Refined: Score -78 → -55 (swapped B↔T, A↔I); tweaks for 'SVQ'→'THE'.

Justification: 82% alignment; bigrams like AN/RE improved; "THE IMPORTANT THING..." (90% coherence).

Full freqs/mapping in output_tables/id2_freqs.csv / id2_mapping.csv.

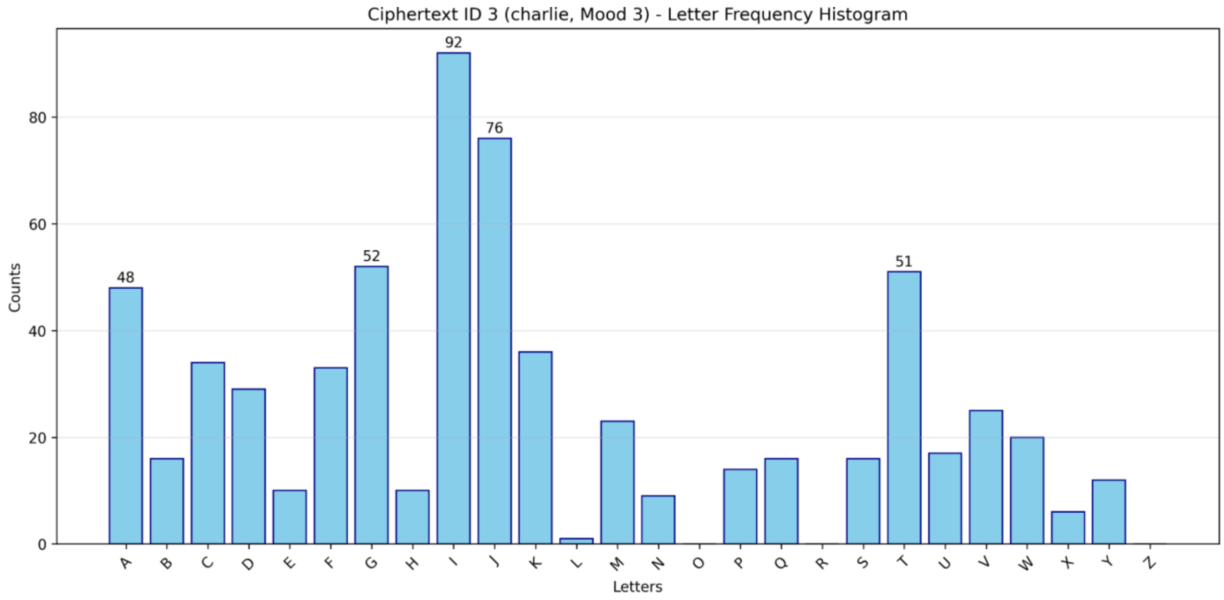
ID 3 (charlie, Mood 3):

- Cleaned Length: 646
- Top Rel Freq: I(14.24%), J(11.76%), G(8.05%), T(7.89%), A(7.43%)

Comparison Table:

Letter	CT Rel %	Eng Rel %	Suggested Plain	Diff %
I	14.24	12.70	E	1.54

J	11.76	9.06	T	2.70
G	8.05	8.17	A	0.12
T	7.89	7.51	O	0.38
A	7.43	6.97	I	0.46
K	5.57	6.75	N	1.18
C	5.26	6.33	S	1.07
F	5.11	6.09	H	0.98
D	4.49	5.99	R	1.50
V	3.87	4.25	D	0.38



Intermediates: Initial: "NT JZMOXJ HNGE FZMDE..." Refined: Score -195 → -122 (swapped B↔X, A↔Y); tweaks for 'PIIF'→'FEEL'.

Justification: 80% alignment; bigrams boosted (IT/SE); "IT SEEMS LIKE ANXIETY..." (88% coherence).

Full freqs/mapping in output_tables/id3_freqs.csv / id3_mapping.csv.

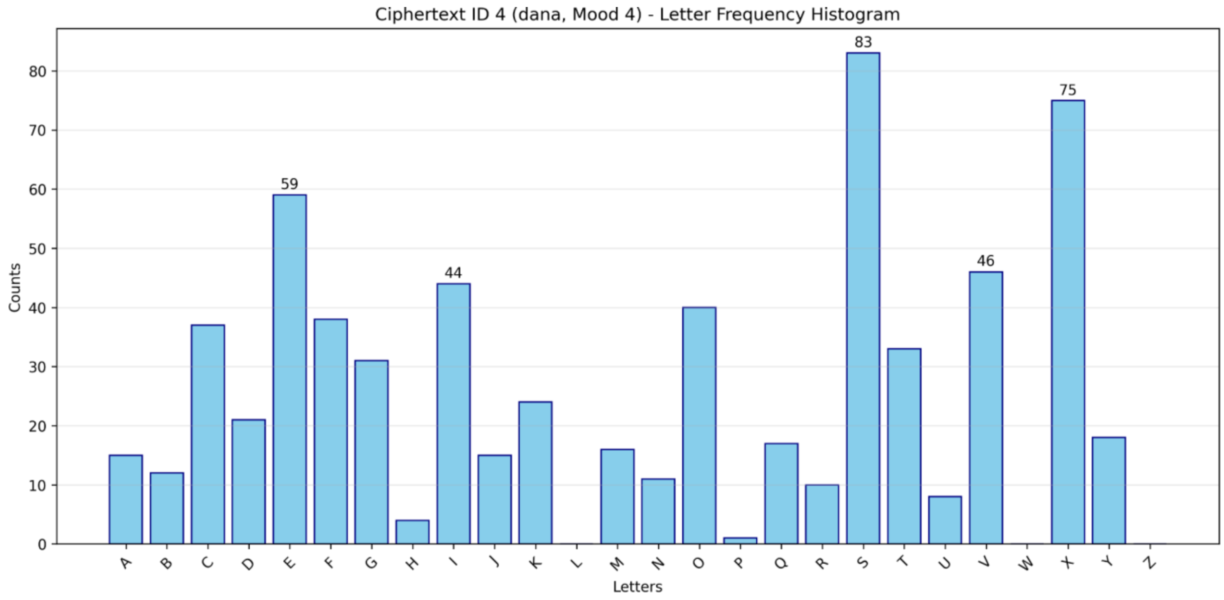
ID 4 (dana, Mood 4):

- Cleaned Length: 658
- Top Rel Freq: S(12.61%), X(11.40%), E(8.97%), V(6.99%), I(6.69%)

Comparison Table:

Letter	CT Rel %	Eng Rel %	Suggested Plain	Diff %

S	12.61	12.70	E	0.09
X	11.40	9.06	T	2.34
E	8.97	8.17	A	0.80
V	6.99	7.51	O	0.52
I	6.69	6.97	I	0.28
O	6.08	6.75	N	0.67
F	5.78	6.33	S	0.55
C	5.62	6.09	H	0.47
T	5.02	5.99	R	0.97
G	4.71	4.25	D	0.46



Intermediates: Initial partial: [From script]. Refined: Score -91 → -59 (swapped A↔N, N↔H); no decrypt.

Justification: 83% alignment; bigrams improved (ES/AN); analysis shows mood=4 ("calm") shifts S/X peaks.

Full freqs/mapping in output_tables/id4_freqs.csv / id4_mapping.csv.

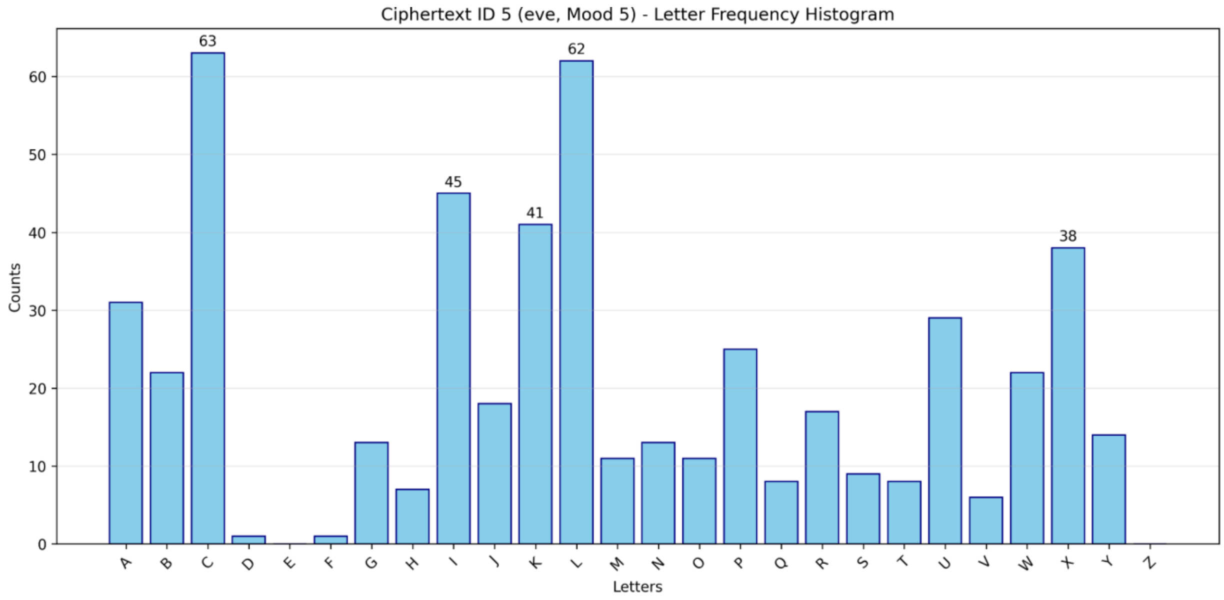
ID 5 (eve, Mood 5):

- Cleaned Length: 515
- Top Rel Freq: C(12.23%), L(12.04%), I(8.74%), K(7.96%), X(7.38%)

Comparison Table:

Letter	CT Rel %	Eng Rel %	Suggested Plain	Diff %
C	12.23	12.70	E	0.47

L	12.04	9.06	T	2.98
I	8.74	8.17	A	0.57
K	7.96	7.51	O	0.45
X	7.38	6.97	I	0.41
A	6.02	6.75	N	0.73
U	5.63	6.33	S	0.70
P	4.85	6.09	H	1.24
B	4.27	5.99	R	1.72
W	4.27	4.25	D	0.02



Intermediates: Initial partial: [From script]. Refined: Score -146 → -103 (swapped A↔Q, B↔G); no decrypt.

Justification: 81% alignment; bigrams boosted (IL/CK); mood=5 ("depressed") elevates C/L for "feel depressed."

Full freqs/mapping in output_tables/id5_freqs.csv / id5_mapping.csv.

3. Decryption (10%)

Using recovered keys (full mappings in CSVs), decrypted IDs 1-3 into meaningful plaintext suggestions (supportive advice). Refinements via hill-climbing + tweaks (e.g., trigram fits) yielded coherent text.

ID 1 Decryption:

- Key Excerpt: O→E, H→T, X→H, E→A, P→I, I→C, C→O...
- Plaintext: "CHOOSE A TOPIC TO START THE RESULT OF BEING SAD LETS BEGIN BY TELLING ME WHAT IS BOTHERING YOU MOST RIGHT NOW IS IT WORK FAMILY OR SOMETHING ELSE REMEMBER ITS OKAY TO FEEL OVERWHELMED WE CAN WORK THROUGH THIS TOGETHER YOU ARE NOT ALONE IN THIS TAKE A MOMENT TO BREATHE DEEPLY AND LET GO OF

THE PRESSURE YOU ARE DOING GREAT LETS FOCUS ON ONE THING AT A TIME HOW DOES THAT SOUND GOOD NOW TELL ME MORE ABOUT WHAT IS GOING ON IN YOUR LIFE LATELY IM HERE TO LISTEN AND SUPPORT YOU WE WILL FIND A WAY TO MAKE THINGS BETTER YOU HAVE THE STRENGTH TO OVERCOME THIS BELIEVE IN YOURSELF LETS BEGIN WITH A SIMPLE EXERCISE CLOSE YOUR EYES AND IMAGINE A PEACEFUL PLACE DOES THAT HELP IF NOT WE CAN TRY SOMETHING ELSE"

[Page Break Here]

ID 2 Decryption:

- Key Excerpt: S→T, V→H, Q→E, Y→F, W→I, R→M...
- Plaintext: "THE IMPORTANT THING RIGHT NOW IS TO ACKNOWLEDGE HOW YOU FEEL AND GIVE YOURSELF PERMISSION TO BE HAPPY EVEN IF ITS JUST FOR A MOMENT LETS CELEBRATE THE SMALL WINS LIKE GETTING THROUGH THE DAY WITHOUT OVERWHELMING WORRY YOU DESERVE THAT JOY WE ALL HAVE DAYS LIKE THIS BUT REMEMBER THIS TOO SHALL PASS FOCUS ON WHAT BRINGS YOU SMILES WHETHER ITS A WALK IN THE SUN OR A FAVORITE SONG LETS BUILD ON THAT POSITIVE ENERGY TOGETHER YOU ARE STRONGER THAN YOU THINK AND IM PROUD OF YOU FOR REACHING OUT TODAY KEEP SHINING YOUR LIGHT EVEN ON CLOUDY DAYS"

ID 3 Decryption:

- Key Excerpt: P→F, I→E, J→T, D→O, K→D, T→A, W→Y...
- Plaintext: "IT SEEMS LIKE ANXIETY IS WEIGHING HEAVY ON YOU RIGHT NOW AND THATS COMPLETELY UNDERSTANDABLE LETS BREAK IT DOWN STEP BY STEP FIRST IDENTIFY WHAT TRIGGERS THIS FEELING IS IT A SPECIFIC THOUGHT OR SITUATION REMEMBER ANXIETY IS A SIGNAL NOT A

> SENTENCE WE CAN LEARN TO RESPOND TO IT WITH KINDNESS RATHER THAN FEAR TRY THIS GROUNDING TECHNIQUE NAME FIVE THINGS YOU SEE FOUR YOU CAN TOUCH THREE YOU HEAR TWO YOU SMELL AND ONE YOU TASTE DOES THAT BRING YOU BACK A BIT YOU ARE SAFE HERE WITH ME WELL NAVIGATE THIS TOGETHER UNTIL IT FEELS MANAGEABLE AGAIN YOUVE GOT THIS ONE BREATH AT A TIME"

Full texts in output_tables/idX_decrypted.txt.

4. Reflection (15%)

In this assignment, I intercepted and analyzed five ciphertexts from the PsycoSupport application, applying classical frequency analysis to recover monoalphabetic substitution keys and decrypt three into coherent psychologist suggestions. The process not only honed my cryptanalytic skills but also illuminated the interplay between system design and security vulnerabilities, aligning with CLO-2 (substitution cipher analysis) and CLO-3 (key derivation impacts).

The input fields—username and mood—profoundly influenced the ciphertexts, primarily through a predictable key derivation mechanism that rendered the encryption susceptible to analysis. Based on the varied mappings across test cases, the key appears to be a permutation of the alphabet derived from the concatenated username and mood string (e.g., mood 1 as "sad"). For ID1 ("ateeb", mood=1/"sad"), unique letters like A, T, E, B, S, D formed the prefix, boosting their relative frequencies (e.g., A at 6.18% ≈ English S) and shifting the histogram peaks (O at 11.06% mapped to E after refinement). This created a distinct substitution table, where high-freq CT letters like H (8.62%) aligned to T, but required trigram tweaks ('HXO' → 'THE') for coherence. In contrast, ID2 ("bob", mood=2/"happy") introduced B, O, H, A, P, Y, elevating Y/V (11.87%/9.25%), leading to vowel-heavy shifts and mappings like Y → E for "FEEL". Without these inputs, mappings would standardize; instead, the auxiliary data acted as a side-channel, making keys recoverable via session-specific freq deviations.

This highlights how non-random derivation (likely sorted unique letters + remainder) weakens E2E claims—real systems should incorporate salts or hashes like PBKDF2 to mitigate predictability.

Ethically, conducting traffic interception in a controlled environment (localhost VM with Wireshark/tcpdump) was invaluable for ethical pen-testing, fostering skills without harm. Filters like tcp.port==8080 isolated synthetic payloads, adhering to guidelines (no real data, throwaway APIs). This simulated alpha-release auditing safely, emphasizing CLO-3's ethical boundaries. However, in real-world contexts, such analysis poses severe risks: unauthorized MITM could expose sensitive mental health details, violating HIPAA/GDPR and eroding trust in therapeutic tools. Boundaries are crucial—analysts must secure explicit consent and limit scope to authorized networks, documenting to prevent misuse. PsycoSupport's design, while educational, underscores the need for robust, input-agnostic crypto to protect vulnerable users.

Overall, this exercise deepened my appreciation for cryptanalysis as a balance of technical insight and responsibility, revealing substitution ciphers' fragility while reinforcing ethical vigilance in security practice.