CYBR171 - Assignment 1
Thomas Green
300536064

Question One: What is the most common letter in the ciphertext?
First most frequent letter was N at 185 instances. Followed by C at 167.

Question 2 – Explain how you can use your knowledge of the most common letter to work out the value of the key.
E is the most common letter in the English Language. If N is then the most frequent letter in the ciphertext then we can then assume that N = E. N is 9 characters ahead of E so we can assume that E has a shift of 9.

Question 3 – What is the decrypted text.
Text shift of 9:
WELCOME TO THE FRACTURED FUTURE, THE FIRST CENTURY FOLLOWING THE SINGULARITY. EARTH HAS A POPULATION OF ROUGHLY A BILLION HOMINIDS. FOR THE MOST PART, THEY ARE HAPPY WITH THEIR LOT, LIVING IN A PRESERVE AT THE BOTTOM OF A GRAVITY WELL. THOSE WHO ARE UNHAPPY HAVE EMIGRATED, JOINING ONE OR ANOTHER OF THE SWARMING DENSETHINKER CLADES THAT FOG THE INNER SOLAR SYSTEM WITH A DUST OF MOLECULAR MACHINERY SO THICK THAT IT OBSCURES THE SUN. EXCEPT FOR THE SOLITARY LIGHTHOUSE BEAM THAT PERPETUALLY TRACKS THE EARTH IN ITS ORBIT, THE SYSTEM FROM OUTSIDE RESEMBLES A SPHERICAL FOGBANK RADIATING IN THE INFRARED SPECTRUM; A MATRYOSHKA BRAIN, NESTED DYSON SPHERES BUILT FROM THE DISMANTLED BONES OF MOONS AND PLANETS. THE SPLINTERY METACONSCIOUSNESS OF THE SOLAR SYSTEM HAS LARGELY SWORN OFF ITS PRE-POSTHUMAN COUSINS DIRTSIDE, BUT ITS MINDS SOMETIMES WANDER NOSTALGIAWISE. WHEN THAT HAPPENS, IT CASUALLY SPAMS EARTH IS RF SPECTRUM WITH PLANS FOR CATACLYSMICALLY DISRUPTIVE TECHNOLOGIES THAT EMULSIFY WHOLE INDUSTRIES, CULTURES, AND SPIRITUAL SYSTEMS. A SANE SPECIES WOULD IGNORE THESE GET-EVOLVED-QUICK SCHEMES, BUT THERE IS ALWAYS *SOMEONE* WHO WILL TAKE A BITE FROM THE FORBIDDEN FRUIT. THERE IS ALWAYS SOMEONE WHO UNACCOUNTABLY CARRIES THE LET IS-LICK-THE-FROZEN-FENCE-POST GENE. THERE IS ALWAYS A FUCKING GEEK WHO WILL DO IT BECAUSE IT IS A HISTORICAL GODDAMNED TECHNICAL FUCKING IMPERATIVE. WHETHER THE ENLIGHTENED, OCCULTING SMARTCLOUD SENDS OUT ITS MISSIVES AS PRANKS, POISON, OR CARE PACKAGES IS UP FOR DEBATE. ASKING IT TO EXPLAIN ITS MOTIVES IS ABOUT AS PRODUCTIVE AS NEGOTIATING WITH AN ANT COLONY TO GET IT TO ABANDON YOUR KITCHEN. WHATEVER THE MOTIVE, HUMANITY WOULD BE MUCH BETTER OFF IF THE CLOUD WOULD EVOLVE INTO SOMETHING UNINTERESTED IN COMMUNICATING WITH MEATPEOPLE—OR AT LEAST SMART ENOUGH TO LET WELL ALONE. BUT UNTIL THAT HAPPY DAY, THERE IS THE TECH JURY SERVICE: DEFENDING THE EARTH FROM THE SCUM OF THE POST-SINGULARITY PATENT OFFICE.

Question 4 – Three splits using commands.
First Split:

UNOFFJUTSUFETDBFUVUTUUSHFXXEHXIPXXIUHBUJQBIFTGXTTFNSJMFJTJIHHIUM
HVWTZTSDUTPEFSQTXIFFUBIOSUPDJOIFFSXFCTJBDFTXUJFFBSMBGBPOVFGNUT
WYPSOEOSTBUFBPIJVTUYPBFMUJFSUSOFFJUJBOFOZTJFBIBBSPSJPTMBBBNUTU

BJJUXFBOZFOFOGXOCLFBSPTZDFSFDNEUPSBBJTSPEFUIBFFPBNFTPJJUZUKJFJU
HFOGFOSSUDQFDVUFBFJMJFPIUTYUFIHPELWIMFSFYJPIOBUTMSMNCLFJJVJTVFXI
FJFBFBEFSOMFMQTUUTSBTGBIILTEBMXPOSUOFJB

F:53 U:36 B:32 J:29 T:29 S:25 O:19 I:18 P:18 X:13 M:12 E:9 D:8 H:8 N:7 V:7 G:6 Z:5 Q:4 Y:4 L:4 W:3 C:3 K:1

Second Split:

KLLWQJLZHLRUWFQLKQHWHKHDUDLLGQHODDHLXQKEFVHZWQQVWFSDYBZUVW
LWHHKDHQHLUHFHHDXWZOXHLDZDEWHWQSWRSGLWZOLZZVOGDRRDKQUWVH
SFRJZJPUFSHDBSUVGYWHUGRWLQHUDHRSUQARWVZRLLLWQJBAYJFWOWVVUJ
QVRPFIUWOVGFSHBHGQWKDRKGWPDPWOUFHHBEDUSVVSWQRDHRIWQGQWVO
RLRDSDGEVSWNUVUGRKRQVJLDYWLFWULKRXUFQLFUVWHGNZDKVERUDHXWHH
LLIWQWAQVGYKVIRDHHHBSHEQKOULWIWFWQDWJPSLDLXXRKRFQWEFDDHDDQ
HHIWQLDVRJ

W:39 H:37 D:30 L:28 Q:27 R:23 V:22 U:21 F:16 K:14 S:14 G:13 Z:11 J:9 O:9 X:7 E:7 B:6 I:6 Y:5 P:5 A:3 N:2

Third Split:

FEOFFIFFBNGBJIHOFJEBTFBOBTOOPUDESTBOQEFNXUOFPFFFIPBUFGXFUDOPUS
FSSJSUFBIOSSOIPEMEUOISFUJFFSPMBXMIPEEFBUMFESBZFUOXBBMFSSJOCPPV
SWFMFBBFVSFZTTMUWUMBFMFEQJIOGOFOOFFITIJSFMPISFDSUUOFMGEPXNFPV
STNNXIFWGBCIBHFPBFFSMMPUZIJEBNUNOEHPIENJFUMWOXUQSUFJMBGIGTBOF
CWUBOTFZWFFPOFNUBPUNIHMUEIOUUJJJWDSXMBPSTGPIFTNUBIFJFQDJESMIQS
CHPETUICIJITOIFBPDMOSJGFVFFPMLUDSOUHECJF BPMQOF

F:56 U:29 O:28 B:28 S:26 I:25 P:23 M:21 E:18 J:18 T:13 N:11 G:9 X:8 D:7 W:7 H:6 Q:6 C:6 Z:4 V:4 L:1

Question 5 – Shift Value

Length of key is 3 so every 3rd letter is encrypted. We have made three split values from the encrypted message by grouping characters encrypted with similar shift. Most common letter in the English language is E so we can assume that F for first and third split can represent E within the Plaintext as well as W and H for the second split. F is one letter ahead of E in the cipher so B(1). H in relation to E is three letters ahead so for the second split we can state D(3). Key is BDB.

We can check for a shift value of 4:
First Shift: Q is 4 away from U. U was second most frequent U is 16 characters ahead of E. Q = 16
Second Shift: S is 4 away from W. W is 18 characters ahead of E therefore S key for second split. S = 18
Third Shift: Q is 4 away from U. U was second most frequent U is 16 characters ahead of E. Q = 16

Question 6 – Decrypted Text
Using key BDB

THEMIDNINETEENEIGHTIESWEREATIMEOFDRASTICCHANGEINTHEUNITEDSTATEST
HEREAGANERAWASWINDINGDOWNTHECOLDWARWASHEATINGUPANDTHEIBMPCW
ASTHENEWESTOFNEWNESSESTHECOMPARATIVELYFEWWIRESSTITCHINGTOGETH
ERTHELARGERUNIVERSITYRESEARCHCENTERSAROUNDTHEWORLDPULSEDWITH
ANEWHEARTBEATTHEINTERNETPROTOCOLIPANDWHILETHEWORLDWIDEWEBWAS
STILL DECADEORSOAWAYTHEINTERNETWASAREALPLAC FORAGROWINGNUMBER
OFCOMPUTERSAVVYEXPLORERSANDADVENTURERSREADYTOSETSAILONTHEVIRT
UALSEATOEXPLOREANDEXPLOITTHISNEWFRONTIERINNINETEENEIGHTYSIXHAVIN
GRECENTLYLOSTHISRESEARCHGRANTASTRONOMERCLIFFORDSTOLLWASMADEA
COMPUTERSYSTEMADMINWITHTHEWAVEOFAHANDBYTHEMANAGEMENTOFLAWRE
NCEBERKELEYLABORATORYSPHYSICSDEPARTMENTCOMMANDEDTOGOFORTHAN
DADMINISTERSTOLLDOVEINTOWHATAPPEAREDTOBEASIMPLETASKFORHISFIRSTD
AYONTHEJOBINVESTIGATINGASEVENTYFIVECENTERRORINTHECOMPUTERACCOU
NTTIMECHARGESLITTLEDIDHEKNOWTHATTHISSIXBITOVERCHARGE.WOULDTAKEO
VERHISLIFEFORTHENEXTSIXMONTHSANDHAVETHISSELFPROCLAIMEDBERKELEYH
IPPIERUBBINGSHOULDERSWITHTHEFBITHECIATHENSAANDTHEGERMANPOLICEAL
LINPURSUITOFTHESOURCEANESTOFBLACKHATHACKERSANDATANGLEDWEBOFIN
TERNATIONALESPIONAGE

Question 7 - What is the maximum amount of time in seconds that it would take for a brute-force attack on a single document?
2^30 closest to 10bil
2^128/2^30
3.16912650057057350374175801344 x 10^29sec
4.154x10^7 sec in one year -> ans / 3.154 x 10^7
1.004796x10^22 years

Question 8 - What is the maximum amount of time in years that it would take for a brute-force attack on a single document?
2^30 closest to 10bil
2^1024/2^30
1.67423219872854268898 x 10^29 sec
ans / 3.154 x 10^7
5.308282 x 10^291 years

Question 9 – XOR

ASSIGNMENT to Binary: 01000001 01010011 01010011 01001001 01000111 01001110 01001101 01000101 01001110 01010100

XOR = 00010011

BAABBAABBA to Binary: 01000010 01000001 01000001 01000010 01000010 01000001 01000001 01000010 01000010 01000001

Defo wrong
00000110001001000010010000010110000010100001111000011000000011100001100000101

Thinking its 00010010

Question 10

barretts% curl -0 https://ftp.sh.cvut.cz/slax/Slax-11.x/slax-ipxe.iso

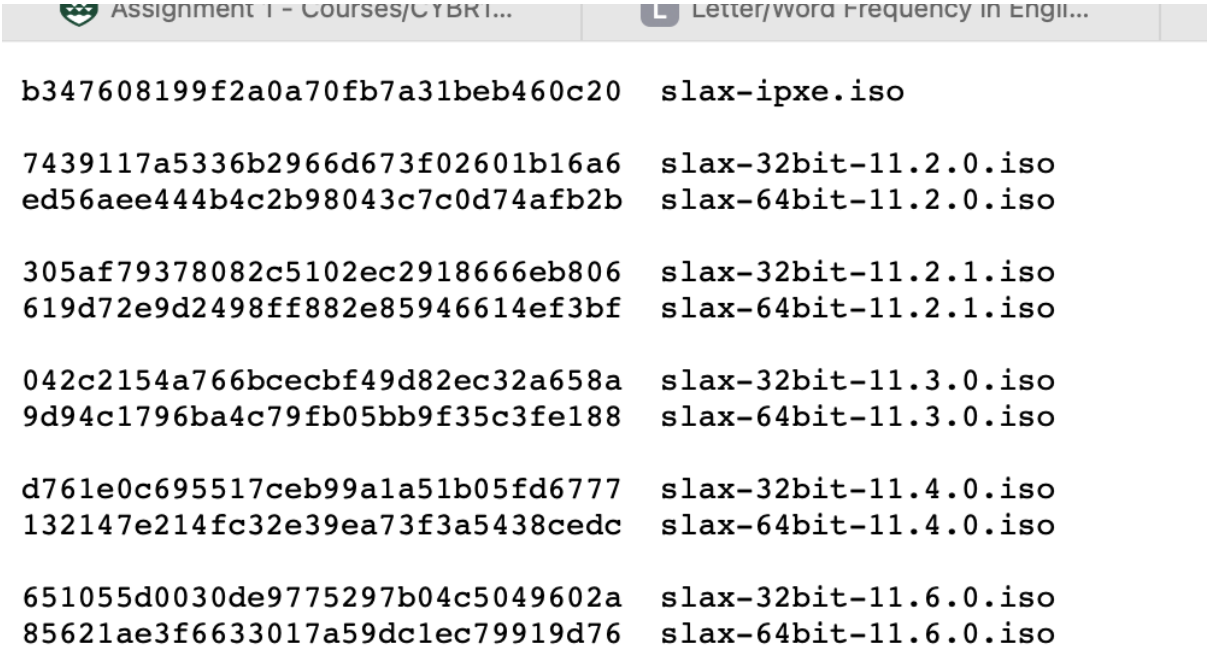
% Total % Received % Xferd Average Speed Time Time Time Current Dload Upload Total Spent Left Speed

100 304k 100 304k 0 0 98k 0 0:00:05 0:00:05 --:--:-- 229k

Barretts% md5sum slax-ipxe.iso.txt

b347608199f2a0a70fb7a31beb460c20 slax-ipxe.iso

this matches the page:



Question 11 – Authenticity

Although the hashes may match, there is no guarantee that the file is authentic. The files integrity is ensured, but it is possible that it has been accessed by unauthorized individuals or that the URL has been modified. To be completely certain, one must compare the downloaded file with the original version.

Question 12 – DES in CBC

barretts% openssl enc -des-cbc -provider legacy -provider default -pbkdf2 -in ciphers.txt -out ciphers.des.enc -passpass:greenthom

Question 13

barretts% openssl enc -aes-256-ecb -provider legacy -provider default -pbkdf2 -in ciphers.txt -out ciphers.aes.enc -pass pass:greenthom

Question 14

barretts% openssl enc -bf-cbc -provider legacy -provider default -pbkdf2 -d -in treasure.bf.enc -pass pass:lucre

I have deposited in the county of Bedford, about four miles from Buford's, in an excavation or vault, six feet below the surface of the ground, the following articles: The deposit consists of two thousand nine hundred and twenty one pounds of gold and five thousand one hundred pounds of silver; also jewels, obtained in St. Louis in exchange for silver to save transportation. The above is securely packed in iron pots, with iron covers. The vault is roughly lined with stone, and the vessels rest on solid stone, and are covered with others.

Question 15

barretts% gpg --import cybr171.pub.key
gpg: key C54C701B32A6E1C9: "CYBR171 <cybr171-staff@ecs.vuw.ac.nz>" not changed
gpg: Total number processed: 1
gpg: unchanged: 1
barretts% gpg --verify document1.asc
gpg: Signature made Mon 13 Mar 2023 09:46:57 NZDT
gpg: using RSA key 1A36CCAA172B659F8885FE6DC54C701B32A6E1C9
gpg: Good signature from "CYBR171 <cybr171-staff@ecs.vuw.ac.nz>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 1A36 CCAA 172B 659F 8885 FE6D C54C 701B 32A6 E1C9
barretts% gpg --verify document2.asc
gpg: Signature made Mon 13 Mar 2023 09:46:57 NZDT

gpg: using RSA key 1A36CCAA172B659F8885FE6DC54C701B32A6E1C9

gpg: BAD signature from "CYBR171 <cybr171-staff@ecs.vuw.ac.nz>" [unknown]

Question 16

A signature is a hash of the original message that has been encrypted using the senders private key to verify that the document is authentic. Once a document is downloaded, a new hash is generated and it compares it to the attached hash of the original doc. By decrypting the signature using the public key, the original hash can be identified. If the two hash values are matching, this means the documents integrity is preserved and therefore it has not been modified. If they don't match this means it has been intercepted/altered. This is the case for document2.asc as the contents are modified after it was signed. PGP signature of the doc does not match the hash of the message.

Question 17

barretts% gpg --keyserver pgp.net.nz --search-keys

barretts% gpg --keyserver pgp.net.nz --recv-keys 1C6DC77C

gpg: key C615B1761C6DC77C: public key "Harith Al-Sahaf <harith.al-

sahaf@ecs.vuw.ac.nz>" imported

gpg: Total number processed: 1

gpg: imported: 1

barretts% gpg --verify message.asc

gpg: Signature made Mon 13 Mar 2023 10:33:21 NZDT

gpg: using RSA key BE655EE79B2C4E7522BADD16C615B1761C6DC77C

gpg: issuer "harith.al-sahaf@ecs.vuw.ac.nz"

gpg: Good signature from "Harith Al-Sahaf <harith.al-sahaf@ecs.vuw.ac.nz>" [unknown]

gpg: WARNING: This key is not certified with a trusted signature!

gpg: There is no indication that the signature belongs to the owner.

Primary key fingerprint: BE65 5EE7 9B2C 4E75 22BA DD16 C615 B176 1C6D C77C

gpg: WARNING: not a detached signature; file 'message' was NOT verified!

The key belongs to Harith and was obtained from an official key server however is untrustworthy due to the warning displayed. The possibility of the message being intercepted/altered means its authenticity as originating from Harith means that it cannot be confirmed. The final warning indicates that the message has not been verified. To verify the messages authenticity, the primary key fingerprint must be read to Harith. If Harith confirms that it is the same primary key fingerprint, then the message can be considered to be from him.

Question 18 – APPLE to XOR

APPLE: 01000001 01010000 01010000 01001100 01000101
WEIRD: 01010111 01000101 01001001 01010010 01000100
XOR: 00010110 00010101 00011001 00011110 00000001

Question 19

Demonstrate using a worked example that applying a Caesar Cipher twice using different keys does not result in a ciphertext that is harder to break than applying a Caesar Cipher once. Include the keys used, the plaintext, ciphertexts and frequency histograms as part of your answer.

Applying a Caesar cipher twice, will be pretty much making the shift value smaller or larger.

I used HEYTHEREX (its 12.45pm) and applying a Caesar Cipher with two different keys. Applying it with a key of 5 means the plaintext will be shifted over by 5.

PT: H E Y T H E R E X
KY: 5 5 5 5 5 5 5 5 5
CT: M J D Y M J W J C

Applying another with a key of 10:
PT: H E Y T H E R E X
KY: 5 5 5 5 5 5 5 5 5
CT: M J D Y M J W J C
KY: 10 10 10 10 10 10 10 10 10
CT: W T N I W T G T M

From looking at this it's harder to break compared to a Caesar Cipher only applied once:

Frequency
Cipher1

C	D	E	J	M	W	Y
1	1	2	2	2	1	1

Cipher2

G	I	M	N	T	W
1	1	1	1	4	2

Distribution in the second ciphertext is different than the first which can make it slightly harder to decrypt. The letters W and M occur in both ciphertexts which can cause some confusion I guess. Applying a Caesar Cipher twice using different keys can make decryption somewhat harder however it is not a secure method as it can be easily broken. As we can see each letter of the plaintext can be simply shifted by a fixed number of positions within the alphabet. When it applied with a second Cipher with a different key we are applying the same thing again upon the first one.

This means that if they are able to find out the first key it is fairly easy to trace back to the first and figure out the second key to go from there. Although it does seem like it would provide a stronger encryption it doesn't offer any significant improvements.

Question 20 – Māori battalion

TE is the keyword. As 'te' is the plaintext and 'am' is the ciphertext.
To go from plaintext to ciphertext we add four, and from ciphertext to plaintext is -4.
Decrypted: Mauri Mahi Mauri Ora Mauri Noho Mauri Mahi.

Question 21 - Exhaustive Key Search

2^1024/2^30
1.67423219872854268898 x 10^299sec
5.308282 x 10^291yr (max time for brute force attack)

Quantum:
2^512/2^30
1.24869942012639689 x 10^145sec
Ans / 3.154 x 10^7
3.95909771758527866 x 10^137 (exhaustive key search)

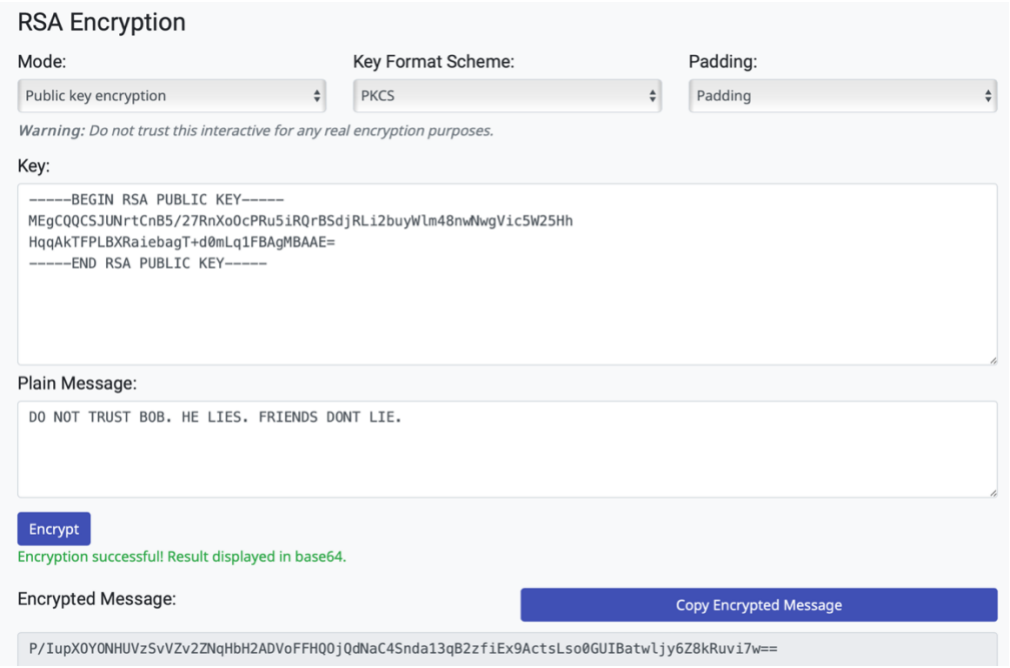
Quantum computers create significant difference in terms of the number of years to undertake an exhaustive key search. With millions of quantum computers carrying out searches this can be shortened also.

Question 22 – Dictionary Attack

When considering an attack the focus is on the number of combinations of 8-letter words in the dictionary. To calculate the total number of combinations in such an attack, taking into account the constraints provided, we need to divide the total number of possible combinations by the number of operations per second
(1000000) = 40161^2/1000000 = 1612.905921 = 1612.91 seconds

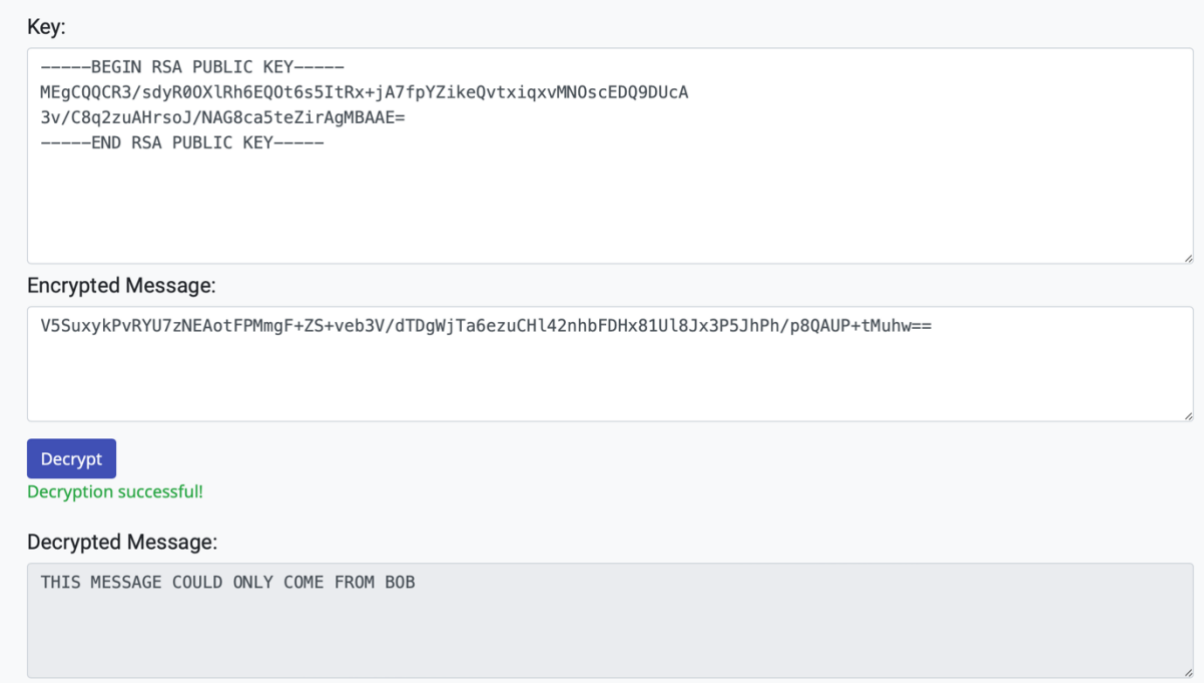
Question 23

To encrypt the message, Carol utilizes Alice's public key. As private and public keys are in relation to one another, Alice's private key would be able to decrypt the message at a later point to therefore deny Bob the ability to access it



Question 24

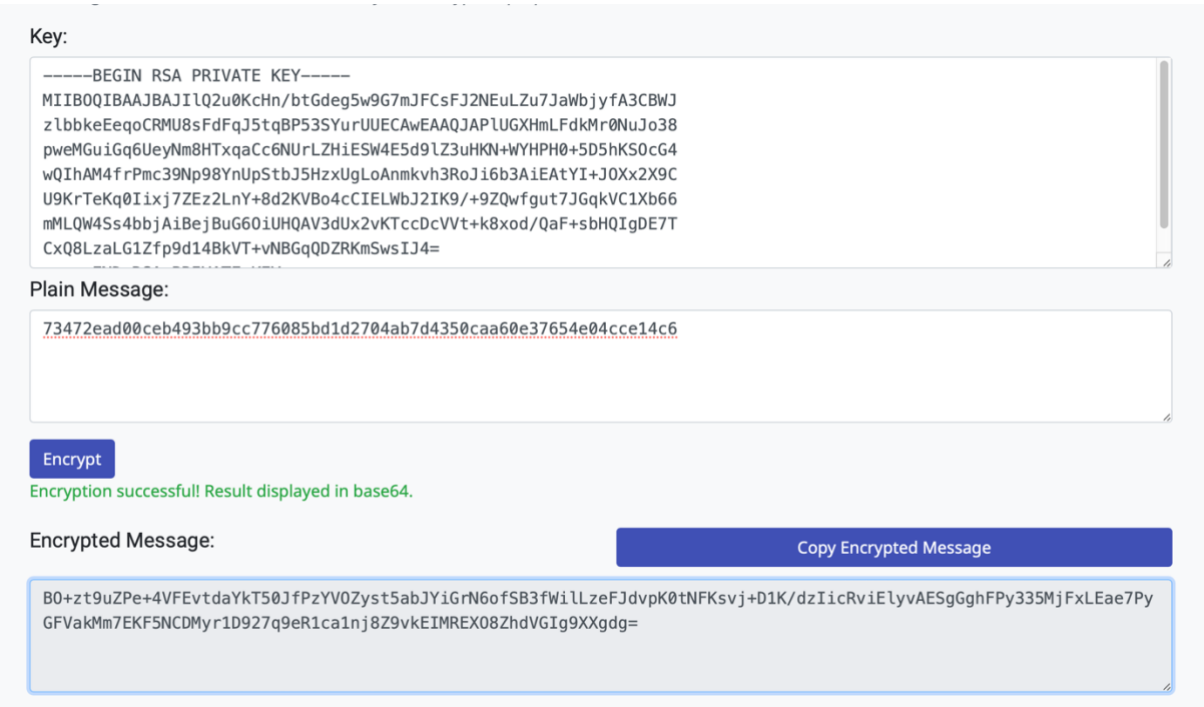
If Bob uses his private key to encrypt the message and sends it to Alice, she can be certain that the information originated from Bob. However since Bob's key is public and therefore accessible to anyone, this can be easily intercepted and read the message if it is not also encrypted with a secure key.



Question 25

SHA2 Hash: “ALICE WROTE THIS”:
73472ead00ceb493bb9cc776085bd1d2704ab7d4350caa60e37654e04cce14c6

By encrypting with her private key anyone who views Alice’s digital signature can be certain that the message appended to it genuinely originates from her, as her private key is not available to everyone else



Verifying the recipient by decrypting the signature using Alices public key

Question 26 – Cybersecurity Reports on Recent Malware Discoveries (may change)

Article: https://threatpost.com/healthcare-maui-ransomware/180154

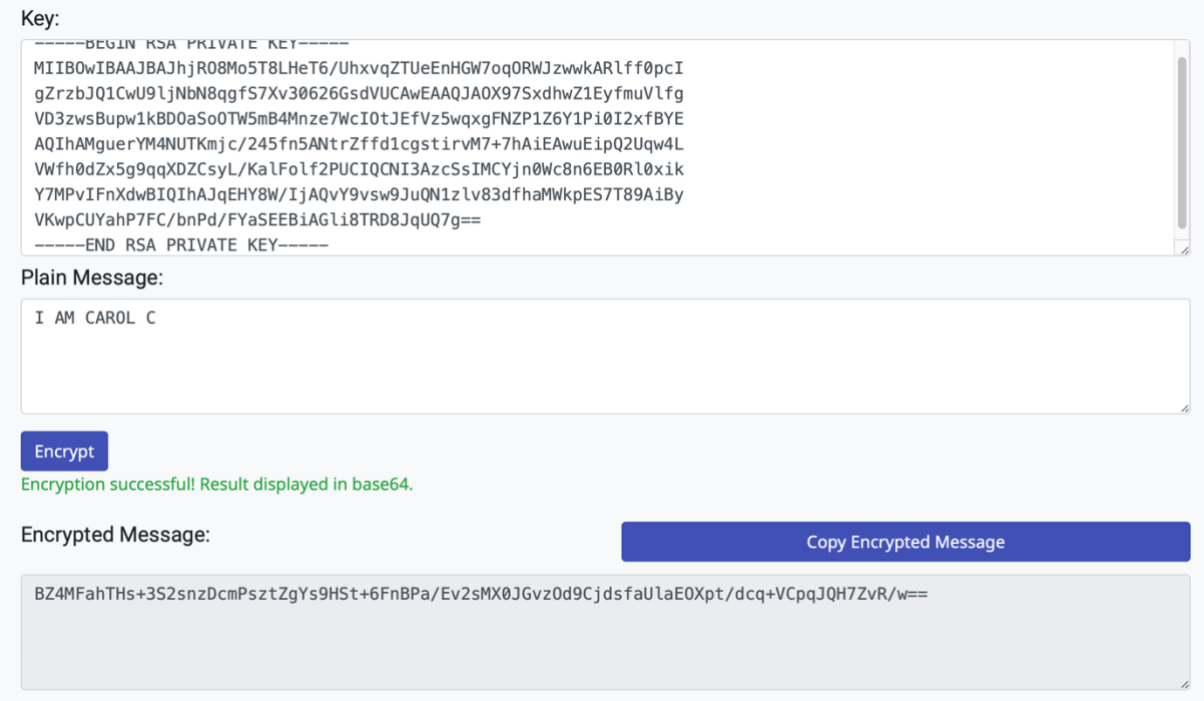
Maui is a malware created by state-sponsored North Korean hackers that is currently targeting healthcare organization in the US. This malware allows hackers to locate and encrypt critical files in health networks, potentially causing significant damage due to the vital nature of the information involved in medical services. The consequences could be disastrous, with delays in essential procedures such as surgeries and chemotherapy leading to loss of life.

To prevent such attacks, it is crucial for healthcare organizations to implement and test backups regularly to ensure that encrypted information can be recovered, rendering the attack ineffective. Additionally, implementing network segmentation can be an effective control to mitigate such attacks, limiting the attackers access to the healthcare system and reducing their leverage in a ransomware payment.

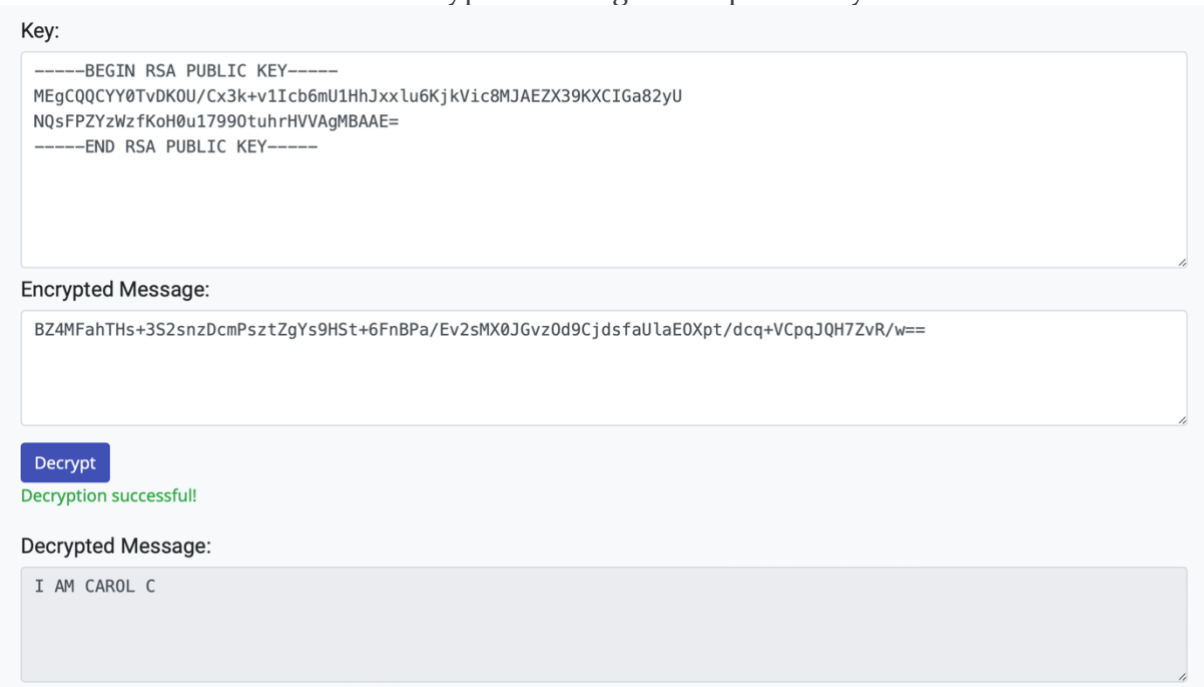
In the event of an attack, the attacker may attempt to publish stolen information. However this would have less severe consequences if backups are in place, and the healthcare organization can recover the lost data. Therefore, it is crucial for healthcare organizations to take proactive measures to prevent such attacks and prepare for their potential consequences.

Question 27

Alice can determine whether Carol is actually real by sending her a message to encrypt using Carols private key. The message will be: I AM CAROL C. Carol would then send the encrypted message back to Alice for her to decrypt it using Carols public key. If the decryption is a success then we can determine that it is actually Carol as she can only have her private key.



This then will allow Alice to decrypt this using Carols public key:



Question 28:

Yes a lot of scrolling was involved

strings cat-a.jpg

FLAG{CATS ARE CUTE}

strings cat-b.jpg

FLAG{Puss in Boots}

String cat-c.jpg

Didn’t have FLAG but said GARFIELD so taking that’s it