CYB-200-B1

SECURITY CONTROLS AGAINST FILE ENCRYPTION BASED RANSOMWARE

By: Jordyn Bostick, Jack Crane, Kevin Hubbard, and Gabrielle Turco

WHY OUR RESEARCH IS RELEVANT

- This course provides a foundational understanding of operating systems, process and memory management, file systems, and system security. Also explores how operating systems protect against security threats such as memory exploits and unauthorized access.

- Our goal was to explore the effectiveness of OS security controls against file encryption based ransomware.

ORIGINALITY & INOVATION

- We have simulated a ransomware based attack to explore how real world systems react to file encryption threats and explored other research topics related to ransomware.
- Our encryption tool uses AES-256 with Cipher Block Chaining and proper key handling and padding which is used in industry.
- We experimented with Linux system services to understand process management, race conditions, and even tried to auto kill the threat.
- We faced a race challenge between our file monitoring script and the ransomware simulation. This showed us how fast malicious processes can operate compared to detection mechanisims

RESEARCH QUESTIONS

- How does ransomware work?
- What logging and forensic artifacts are generated when ransomware interacts with OS security features?
- What ransomware techniques are most effective at bypassing built-in OS Security Controls?
- What steps should a ransomware victim take before and after attack occurs?

HOW RANSOMWARE WORKS

- Ransomware can accidentally be downloaded onto a computer by opening an email attachment, clicking advertisements, visiting a website with malicious code hidden within.
- When the code is on a computer, it will lock access to the computer itself, or data and files stored there.
- Often times, the victim is unware that their computer is infected. However it is evident when they no longer can access data, files have been modified, or a “A Ransom Note” has been left behind

RANSOMWARE LOGGING & ARTIFACTS

- System logs can reveal suspicious activity related to unusual network connections, file access patterns and process execution

- Artifacts may include but are not limited to: Encrypted Files, Ransom Notes, Executables, Scripts, Registry Modifications, Modified Timestamps

- Check the Bash History as it may reveal scripts, commands, downloads, or how the attacker gained entry.

RANSOMWARE TECHNIQUES THAT BYPASS OS SECURITY CONTROLS

- Fileless Execution via PowerShell or WMI
    - Fileless Execution runs ransomware in memory using tools like PowerShell to avoid detection
- Exploiting Unpatched OS Vulnerabilities
    - OS Exploits takes advantaged of unpatched system flaws to gain unauthorized access.
- Privilege Escalation via Token
    - Impersonation Privilege Escalation steals credentials to act as an admin and bypass security restrictions.
- Disabling or Tampering with Security Tools
    - Security tools tampering disables antivirus and defenses before encrypting files.

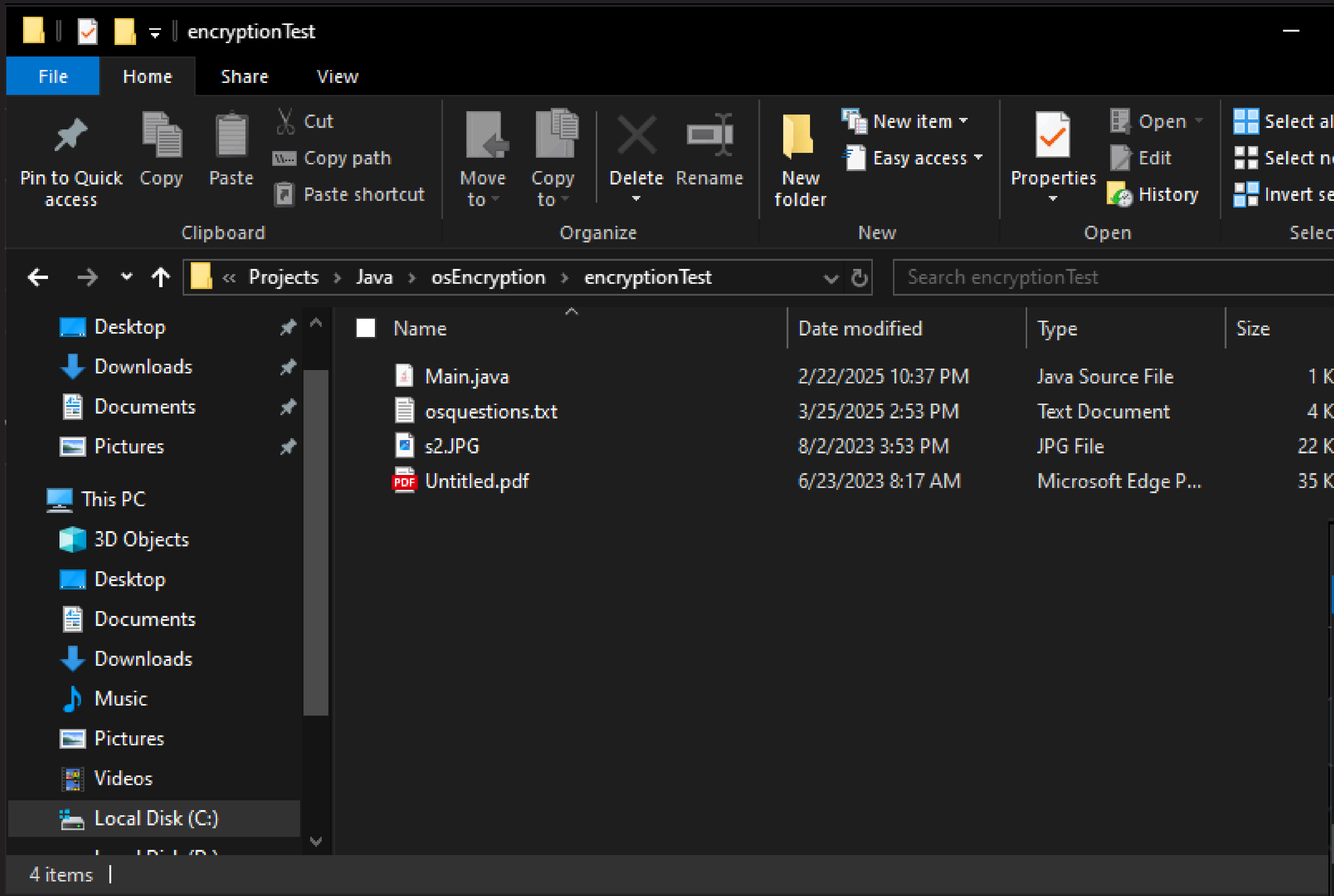
HOW TO AVOID BECOMING A RANSOMWARE VICTIM

- Keep Operating Systems, software, and applications up to date
- Set anti-virus and anti-malware to automatic update and run regular scans.
- Back up data regulary. Secure back ups and make sure they are not connected to the computers and networks they are backing up.
- Have a plan in place in case your business or organization is the victim of an attack.

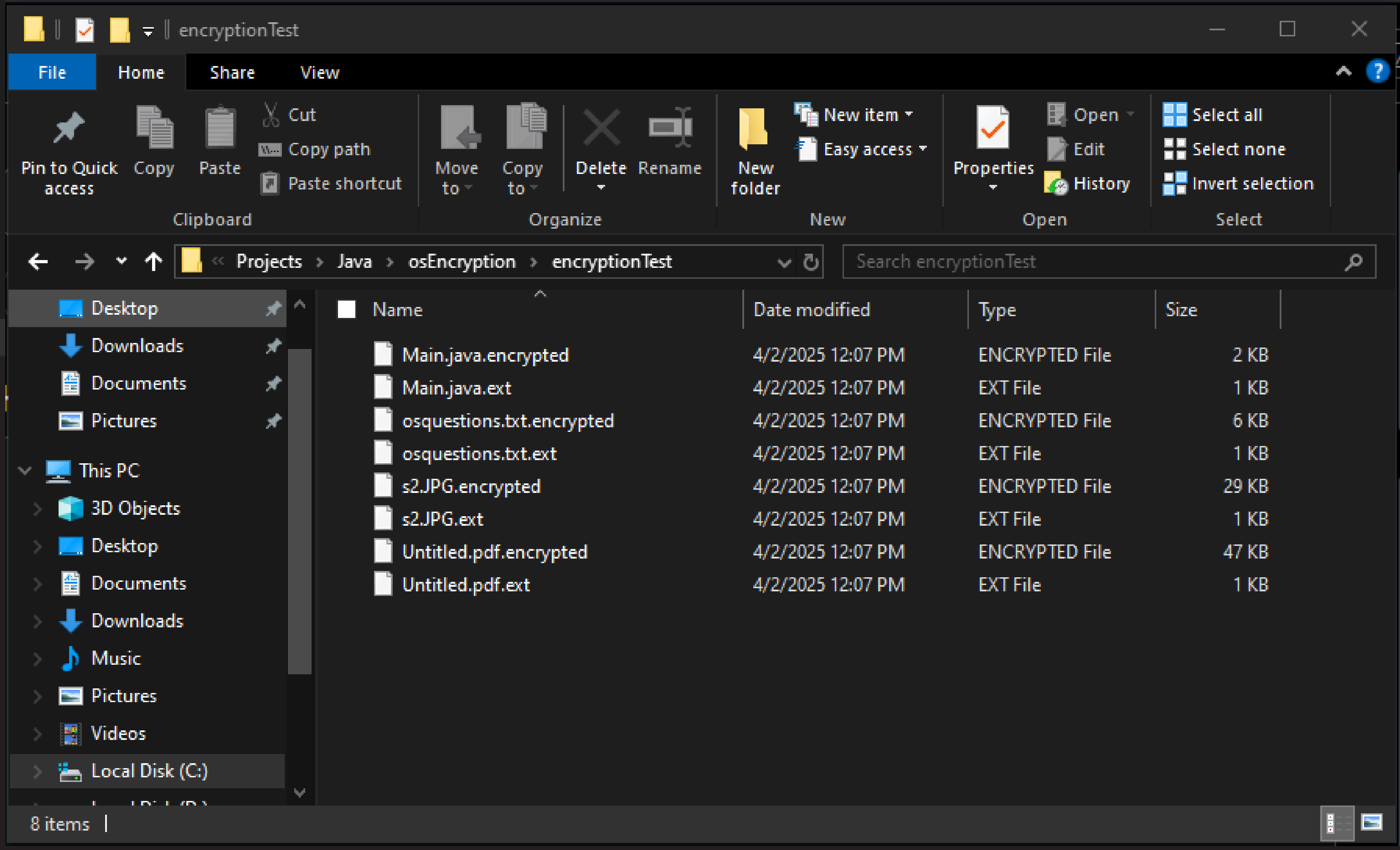
GITHUB

- https://github.com/kevinhubbard/osEncryption

ENCRYPTION METHODOLOGY

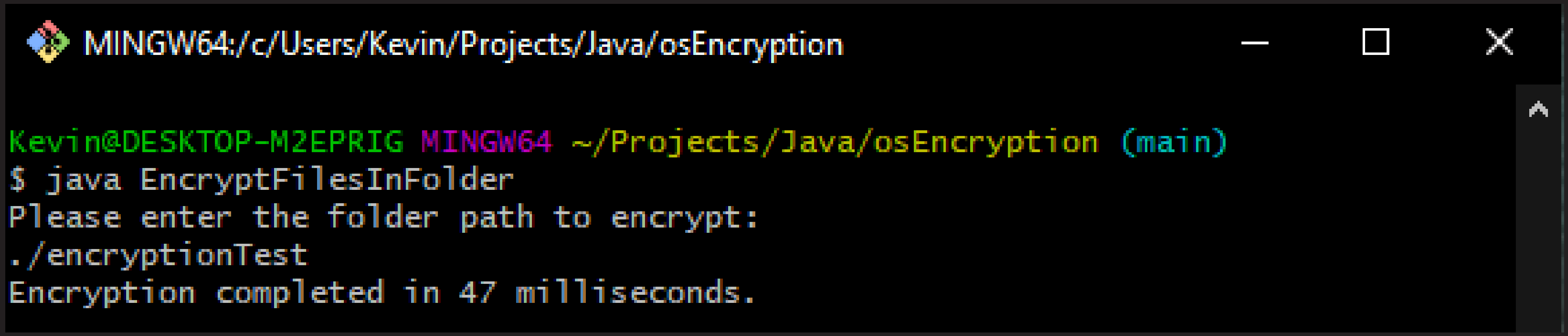


Name	Date modified	Type	Size
Main.java	2/22/2025 10:37 PM	Java Source File	1 KB
osquestions.txt	3/25/2025 2:53 PM	Text Document	4 KB
s2.JPG	8/2/2023 3:53 PM	JPG File	22 KB
Untitled.pdf	6/23/2023 8:17 AM	Microsoft Edge P...	35 KB



Name	Date modified	Type	Size
Main.java.encrypted	4/2/2025 12:07 PM	ENCRYPTED File	2 KB
Main.java.ext	4/2/2025 12:07 PM	EXT File	1 KB
osquestions.txt.encrypted	4/2/2025 12:07 PM	ENCRYPTED File	6 KB
osquestions.txt.ext	4/2/2025 12:07 PM	EXT File	1 KB
s2.JPG.encrypted	4/2/2025 12:07 PM	ENCRYPTED File	29 KB
s2.JPG.ext	4/2/2025 12:07 PM	EXT File	1 KB
Untitled.pdf.encrypted	4/2/2025 12:07 PM	ENCRYPTED File	47 KB
Untitled.pdf.ext	4/2/2025 12:07 PM	EXT File	1 KB

BEFORE VS. AFTER ENCRYPTION



```
Kevin@DESKTOP-M2EPRIG MINGW64 ~/Projects/Java/osEncryption (main)
$ java EncryptFilesInFolder
Please enter the folder path to encrypt:
./encryptionTest
Encryption completed in 47 milliseconds.
```

General Program flow

- Ask user for folder path they want encrypted
- Generate and save encryption key
- Use folder path and encryption key to encrypt the contents of the folder.
- (optional) Use a timer to compare computer processing times

Advanced Encryption Standard

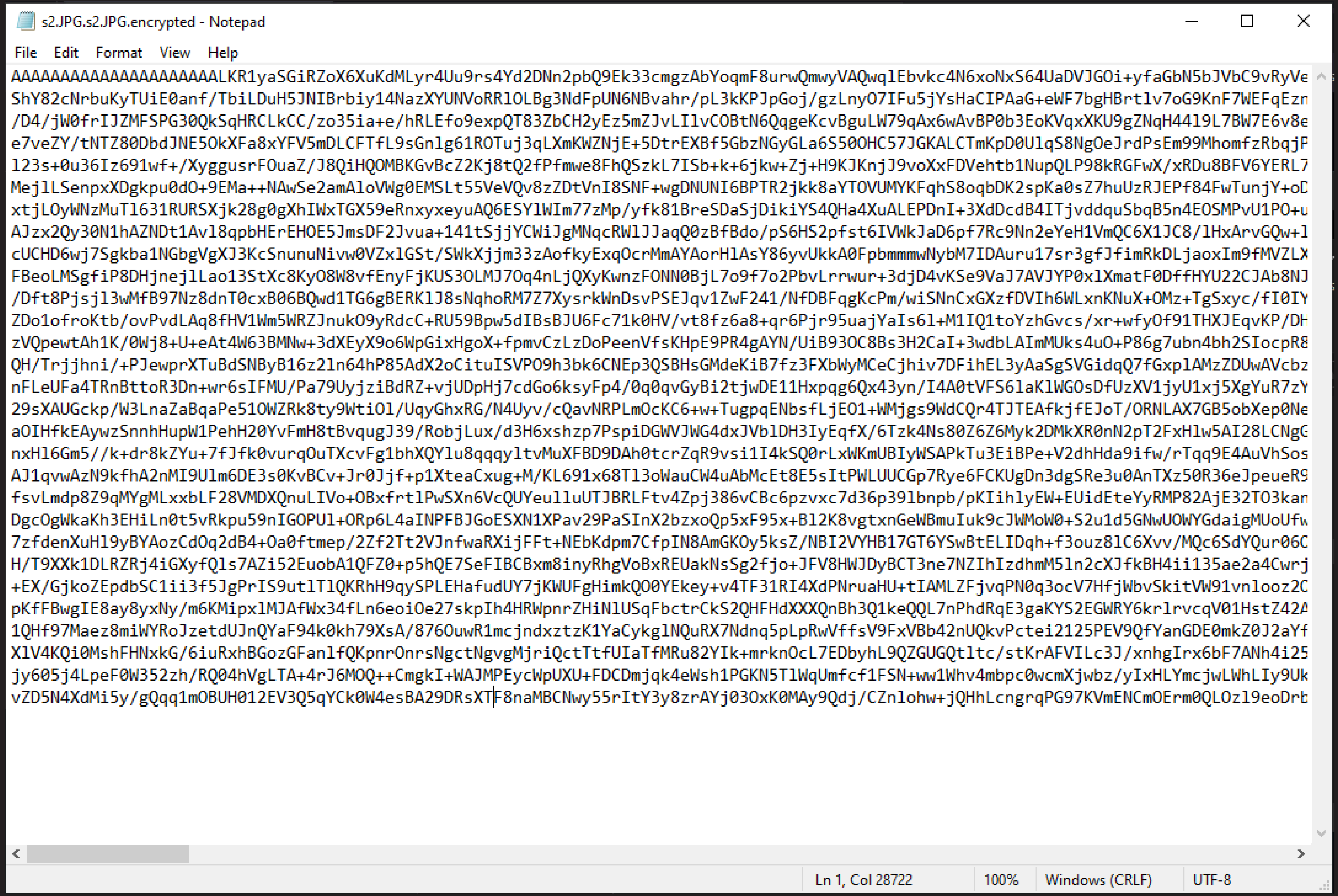
Key Generation

- Symmetric key encryption algorithm
- Uses 128, 192, or 256-bit keys
- Key size determines number of rounds (10, 12, 14)
- Encrypts data in 16-byte blocks
- Standardized by NIST in 2001
- Approved for use by the NSA

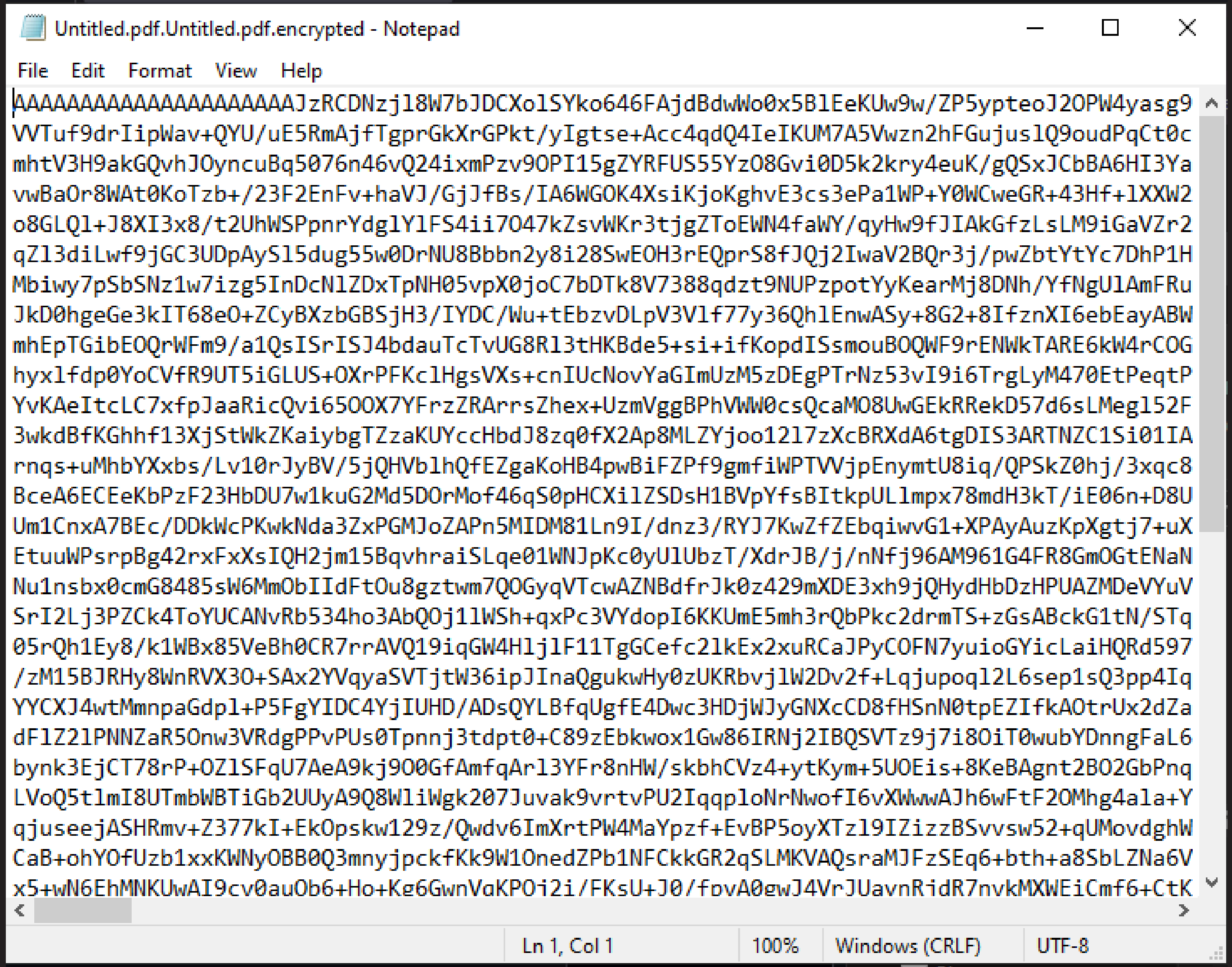
Encryption Process

- Converts plaintext to ciphertext
- Create an array of files then convert to byte array
- Start to encrypt the first 16 bytes of the file using the key and AES
- Repeats encryption block-by-block until the file is complete
- Returns an encrypted string of the file contents which is written (or saved) in place of the original file.

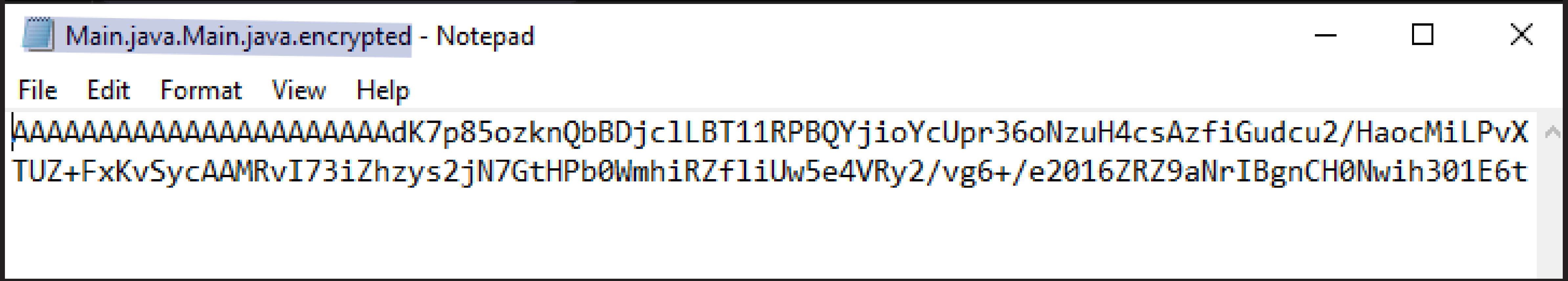
ENCRYPTED FILES



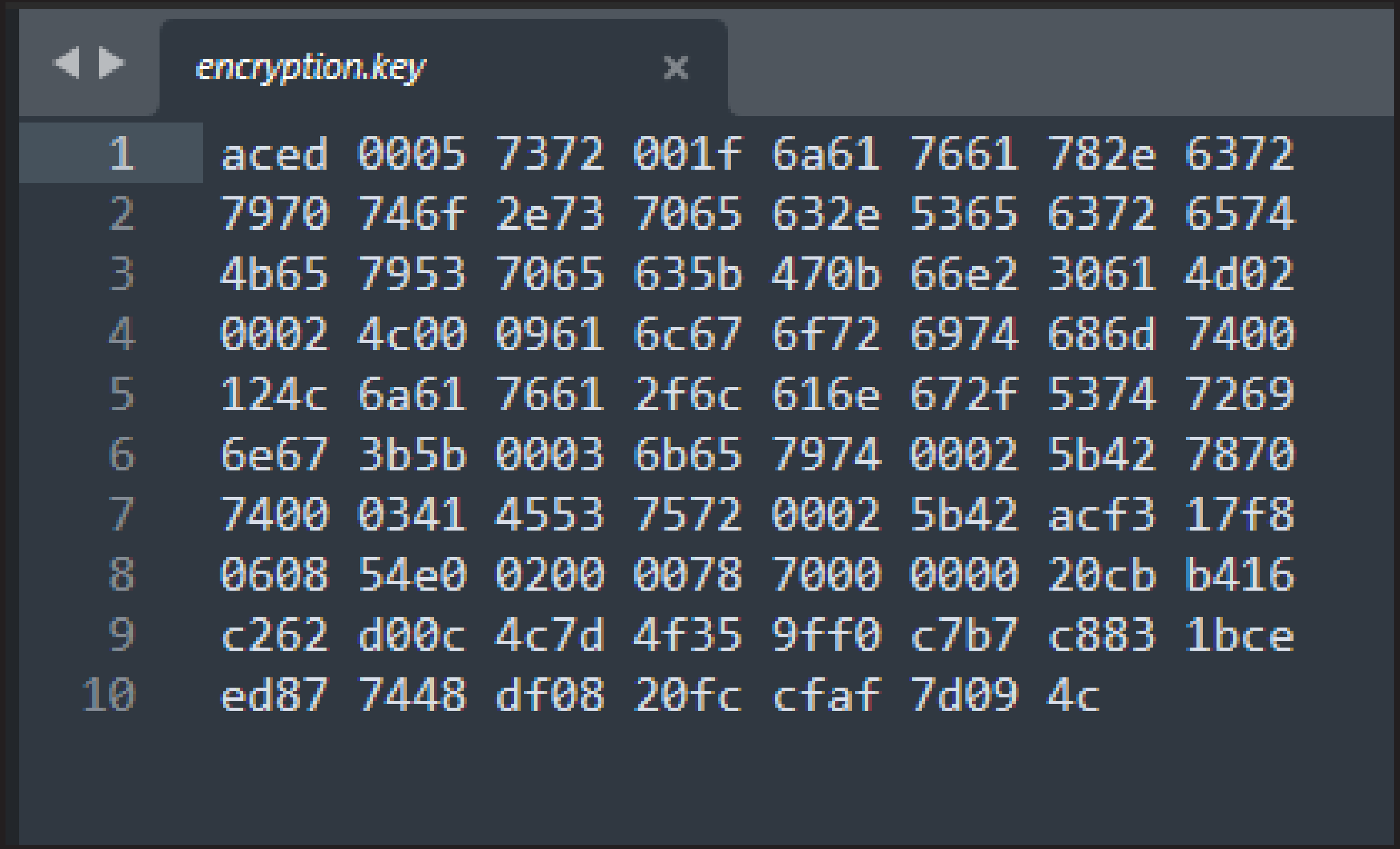
```
AAAAAAAAAAAAAAAAAAAAALKR1yaSGiRZoX6XuKdMLyr4Uu9rs4Yd2DNn2pbQ9Ek33cmgzAbYoqmF8urwQmwyVAQwqlEbvkc4N6xoNxS64UaDVJGOi+yfaGbN5bJVbC9vRyVe
ShY82cNrbuKyTUiE0anf/TbiLDuH5JNIBrbiy14NazXYUNVoRR1OLBg3NdFpUN6NBvahr/pL3kKPJpGoj/gzLnyO7IFu5jYsHaCIPAaG+eWF7bgHBrtlv7oG9KnF7WEFqEzn
/D4/jW0frIJZMFSPG30QkSqHRCLkCC/zo35ia+e/hRLEfo9expQT83ZbCH2yEz5mZJvLIlvCOBtN6QqgeKcvBguLW79qAx6wAvBP0b3EoKVqxXKU9gZNqH4419L7BW7E6v8e
e7veZY/tNTZ80DbdJNE5OkXFa8xYFV5mDLCFTfL9sGnlg61ROTuj3qLXmKWZNjE+5DtrEXBf5GbzNGyGLa6S50OHC57JGKALCTmKpD0UlqS8NgOeJrdPsEm99MhomfzRbqjP
123s+0u36Iz691wf+/XyggusrFOuaZ/J8QiHQOMBKGvBcZ2Kj8tQ2fPfmwe8FhQSzkL7ISb+k+6jkw+Zj+H9KJKnjJ9voXxFDVehtb1NupQLP98kRGFwX/xRDu8BFV6YERL7
MejlLSenpxXDgkpu0dO+9EMa++NAwSe2amAloVWg0EMSLt55VeVQv8zZDtVnI8SNF+wgDNUNI6BPTR2jkk8aYTOVUMYKFqhS8oqbDK2spKa0sZ7huUzRJEPf84FwTunjY+oD
xtjLOyWNzMuTl631RURSXjk28g0gXhIWxTGX59eRnxyxeyuAQ6ESYlWIm77zMp/yfk81BreSDaSjDikiYS4QHa4XuALEPDnI+3XdDcdB4ITjvddquSbqB5n4EOSMPvU1PO+u
AJzx2Qy30N1hAZNDt1Avl8qpbHErEHOE5JmsDF2Jvua+141tSjjYCWiJgMNqcRWlJJaqQ0zBfBdo/pS6HS2pfst6IVWkJaD6pf7Rc9Nn2eYeH1VmQC6X1JC8/lHxArvGQw+l
cUCHD6wj7Sgkba1NGbgVgXJ3KcSnunuNivw0VZxlGSt/SWkXjjm33zAofkyExqOcrMmAYAorHlAsY86yvUkkA0FpbmmmwNybM7IDAuru17sr3gfJfimRkDLjaoxIm9fMVZLX
FBeoLMSgfiP8DHjnejlLao13StXc8KyO8W8vfEnyFjKUS3OLMJ7Oq4nLjQXyKwnzFONN0BjL7o9f7o2PbvLrrwur+3djD4vKSe9VaJ7AVJYP0xlXmatF0DffHYU22CJAb8NJ
/Dft8Pjsjl3wMfB97Nz8dnT0cxB06BQwd1TG6gBERKlJ8sNqhoRM7Z7XysrkWnDsvPSEJqv1ZwF241/NfDBFqgKcPm/wiSNnCxGXzfDVIh6WLxnKNuX+OMz+TgSxyc/fI0IY
ZDo1ofroKtb/ovPvdLAq8fHV1Wm5WRZJnukO9yRdcC+RU59Bpw5dIBsBJU6Fc71k0HV/vt8fz6a8+qr6Pjr95uajYaIs6l+M1IQ1toYzhGvcs/xr+wfyOf91THXJEqvKP/DH
zVQpewtAh1K/0Wj8+U+eAt4W63BMNw+3dXEyX9o6WpGixHgoX+fpmvCzLzDoPeenVfsKHpE9PR4gAYN/UiB93OC8Bs3H2CaI+3wdbLAImMUks4uO+P86g7ubn4bh2SIocpR8
QH/Trjjhni/+PJewprXTuBdSNByB16z2ln64hP85AdX2oCituISVPO9h3bk6CNEp3QSBHsGMdeKiB7fz3FXbWyMCeCjhiv7DFihEL3yAaSgSVGidqQ7fGxplAMzZDUwAVcbz
nFLeUFa4TRnBttoR3Dn+wr6sIFMU/Pa79UyjziBdRZ+vjUDpHj7cdGo6ksyFp4/0q0qvGyBi2tjwDE11Hxpqg6Qx43yn/I4A0tVFS6laKlWGOsDfUzXV1jyU1xj5XgYuR7zY
29sXAUGckp/W3LnaZaBqaPe51OWZRk8ty9WtiOl/UqyGhxRG/N4Uyv/cQavNRPLmOcKC6+w+TugpqENbsfLjEO1+WMjgs9WdCQr4TJTEAfkjfEJoT/ORNLAX7GB5obXep0Ne
aOIHfkEAywzSnnhHupW1PehH20YvFmH8tBvqugJ39/RobjLux/d3H6xshzp7PspiDGWVJWG4dxJVblDH3IyEqfX/6Tzk4Ns80Z6Z6Myk2DMkXR0nN2pT2FxHlw5AI28LCNgG
nxHl6Gm5//k+dr8kZYu+7fJfk0vurqOuTXcvFg1bhXQYlu8qqqyltvMuXFBD9DAh0tcrZqR9vsi1I4kSQ0rLxWKmUBIyWSAPkTu3EiBPe+V2dhHda9ifw/rTqq9E4AuVhSos
AJ1qvwAzN9kfhA2nMI9Ulm6DE3s0KvBCv+Jr0Jjf+p1XteaCxug+M/KL691x68Tl3oWauCW4uAbMcEt8E5sItPWLUUCGp7Rye6FCKUgDn3dgSRe3u0AnTXz50R36eJpeueR9
fsvLmdp8Z9qMYgMLxxbLF28VMDXQnuLIVo+OBxfrtlPwSXn6VcQUYeulluUTJBRLFtv4Zpj386vCBc6pzvxc7d36p39lbnpb/pKIihlyEW+EUidEteYyRMP82AjE32TO3kan
DgcOgWkaKh3EHiLn0t5vRkpu59nIGOPUl+ORp6L4aINPFBJGoESXN1XPav29PaSInX2bzxoQp5xF95x+Bl2K8vgtxnGeWBmuIuk9cJWMoW0+S2u1d5GNwUOWYGdaigMUoUfw
7zfdenXuHl9yBYAozCdOq2dB4+Oa0ftmep/2Zf2Tt2VJnfwaRXijFFt+NEbKdpm7CfpIN8AmGKOy5ksZ/NBI2VYHB17GT6YSwBtELIDqh+f3ouz8lC6Xvv/MQc6SdYQur06C
H/T9XXk1DLRZRj4iGXyfQls7AZi52EuobA1QFZ0+p5hQE7SeFIBCBxm8inyRhgVoBxREUakNsSg2fjo+JFV8HWJDyBCT3ne7NZIhIzdhmM5ln2cXJfkBH4ii135ae2a4Cwrj
+EX/GjkoZEpdbSC1ii3f5JgPrIS9utlTlQKRhH9qySPLEHafudUY7jKWUFgHimkQO0YEkey+v4TF31RI4XdPNruaHU+tIAMLZFjvqPN0q3ocV7HfjWbvSkitVW91vnlooz2C
pKfFBwgIE8ay8yxNy/m6KMipxlMJAfWx34fLn6eoiOe27skpIh4HRWpnrZHiNlUSqFbctrCkS2QHFHdXXXQnBh3Q1keQQL7nPhdRqE3gaKYS2EGWRY6krlrvcqV01HstZ42A
1QHf97Maez8miWYRoJzetdUJnQYaF94k0kh79XsA/876OuwR1mcjndxztzK1YaCykglNQuRX7Ndnq5pLpRwVffsV9FxVBb42nUQkvPctei2125PEV9QfYanGDE0mkZ0J2aYf
XlV4KQi0MshFHNxkG/6iuRxhBGozGFanlfQKpnrOnrsNgctNgvgMjriQctTtfUIaTfMRu82YIk+mrknOcL7EDbyhL9QZGUGQtltc/stKrAFVILc3J/xnhgIrx6bF7ANh4i25
jy605j4LpeF0W352zh/RQ04hVgLTA+4rJ6MOQ++CmgkI+WAJMPEycWpUXU+FDCDmjqk4eWsh1PGKN5TlWqUmfcf1FSN+ww1Whv4mbpc0wcmXjwbz/yIxHLYmcjwLWhLIy9Uk
vZD5N4XdMi5y/gQqq1mOBUH012EV3Q5qYCk0W4esBA29DRsXTF8naMBCNwy55rItY3y8zrAYj03OxK0MAy9Qdj/CZnlohw+jQHhLcngrqPG97KVmENCmOErm0QLOzl9eoDrb
```



```
AAAAAAAAAAAAAAAAAAAAAJzRCDNzj18W7bJDCXolSYko646FAjdBdwWo0x5BlEeKUw9w/ZP5ypteoJ2OPW4yasg9
VVTuf9drIipWav+QYU/uE5RmAjfTgprGkXrGPkt/yIgtse+Acc4qdQ4IeIKUM7A5Vwzn2hFGujuslQ9oudPqCt0c
mhtV3H9akGQvhJOyncuBq5076n46vQ24ixmPzv9OPI15gZYRFUS55YzO8Gvi0D5k2kry4euK/gQSxJCbBA6HI3Ya
vwBaOr8WAt0KoTzb+/23F2EnFv+haVJ/GjJfBs/IA6WGOK4XsiKjoKghvE3cs3ePa1WP+Y0WCweGR+43Hf+lXXW2
o8GLQl+J8XI3x8/t2UhWSPpnrYdglYlFS4ii7O47kZsvWKr3tjgZToEWN4faWY/qyHw9fJIAkGfzLsLM9iGaVZr2
qZl3diLwf9jGC3UDpAySl5dug55w0DrNU8Bbbn2y8i28SwEOH3rEQprS8fJQj2IwaV2BQr3j/pwZbtYtYc7DhP1H
Mbiwy7pSbSNz1w7izg5InDcNlZDxTpNH05vpX0joC7bDTk8V7388qdzt9NUPzpotYyKearMj8DNh/YfNgUlAmFRu
JkD0hgeGe3kIT68eO+ZCyBXzbGBSjH3/IYDC/Wu+tEbzvDLpV3Vlf77y36QhlEnwASy+8G2+8IfznXI6ebEayABW
mhEpTGibEOQrWFm9/a1QsISrISJ4bdauTcTvUG8Rl3tHKBde5+si+ifKopdISsmouBOQWF9rENWkTARE6kW4rCOG
hyxlfdp0YoCVfR9UT5iGLUS+OXrPFKclHgsVXs+cnIUcNovYaGImUzM5zDEgPTrNz53vI9i6TrgLyM470EtPeqtP
YvKAeItcLC7xfpJaaRicQvi65OOX7YFrzZRArrsZhex+UzmVggBPhVWW0csQcaMO8UwGEkRRekD57d6sLMegl52F
3wkdBfKGhhf13XjStWkZKaiybgTZzaKUYccHbdJ8zq0fX2Ap8MLZYjoo12l7zXcBRXdA6tgDIS3ARTNZC1Si01IA
rnqs+uMhbYXxbs/Lv10rJyBV/5jQHVblhQfEZgaKoHB4pwBiFZPf9gmfiWPTVVjpEnymtU8iq/QPSkZ0hj/3xqc8
BceA6ECEeKbPzF23HbDU7w1kuG2Md5DOrMof46qS0pHCXilZSDsH1BVpYfsBItkpULlmpx78mdH3kT/iE06n+D8U
Um1CnxA7BEc/DDkWcPKwkNda3ZxPGMJoZAPn5MIDM81Ln9I/dnz3/RYJ7KwZfZEbqiwvG1+XPAyAuzKpXgtj7+uX
EtuuWPsrpBg42rxFxXsIQH2jm15BqvhraiSLqe01WNJpKc0yUlUbzT/XdrJB/j/nNfj96AM961G4FR8GmOGtENaN
Nu1nsbx0cmG8485sW6MmObIIdFtOu8gztwm7QOGyqVTcwAZNBdfrJk0z429mXDE3xh9jQHydHbDzHPUAZMDeVYuV
SrI2Lj3PZCk4ToYUCANvRb534ho3AbQOj1lWSh+qxPc3VYdopI6KKUmE5mh3rQbPkc2drmTS+zGsABckG1tN/STq
05rQh1Ey8/k1WBx85VeBh0CR7rrAVQ19iqGW4HljlF11TgGCefc2lkEx2xuRCaJPyCOFN7yuioGYicLaiHQRd597
/zM15BJRHy8WnRVX3O+SAx2YVqyaSVTjtW36ipJInaQgukwHy0zUKRbvjlW2Dv2f+Lqjupoql2L6sep1sQ3pp4Iq
YYCXJ4wtMmnpaGdpl+P5FgYIDC4YjIUHD/ADsQYLBfqUgfE4Dwc3HDjWJyGNXcCD8fHSnN0tpEZIfkAOtrUx2dZa
dFlZ2lPNNZaR5Onw3VRdgPPvPUs0Tpnnj3tdpt0+C89zEbkwox1Gw86IRNj2IBQSVTz9j7i8OiT0wubYDnngFaL6
bynk3EjCT78rP+OZlSFqU7AeA9kj9O0GfAmfqArl3YFr8nHW/skbhCVz4+ytKym+5UOEis+8KeBAgnt2BO2GbPnq
LVoQ5tlmI8UTmbWBTiGb2UUyA9Q8WliWgk207Juvak9vrtvPU2IqqploNrNwofI6vXWwwAJh6wFtF2OMhg4ala+Y
qjuseejASHRmv+Z377kI+EkOpskw129z/Qwdv6ImXrtPW4MaYpzf+EvBP5oyXTzl9IZizzBSvvsw52+qUMovdghW
CaB+ohYOfUzb1xxKWNyOBB0Q3mnyjpckfKk9W1OnedZPb1NFCkkGR2qSLMKVAQsraMJFzSEq6+bth+a8SbLZNa6V
x5+wN6EhMNKUwAI9cv0auOb6+Ho+Kg6GwnVqKPOi2i/FKsU+J0/fpvA0gwJ4VrJUavnRidR7nvkMXWEiCmf6+CtK
```



```
AAAAAAAAAAAAAAAAAAAAAAdK7p85ozknQbBDjclLBT11RPBQYjioYcUpr36oNzuH4csAzfiGudcu2/HaocMiLPvX
TUZ+FxKvSycAAMRvI73iZhzys2jN7GtHPb0WmhiRZfliUw5e4VRy2/vg6+/e2016ZRZ9aNrIBgnCH0Nwih301E6t
```

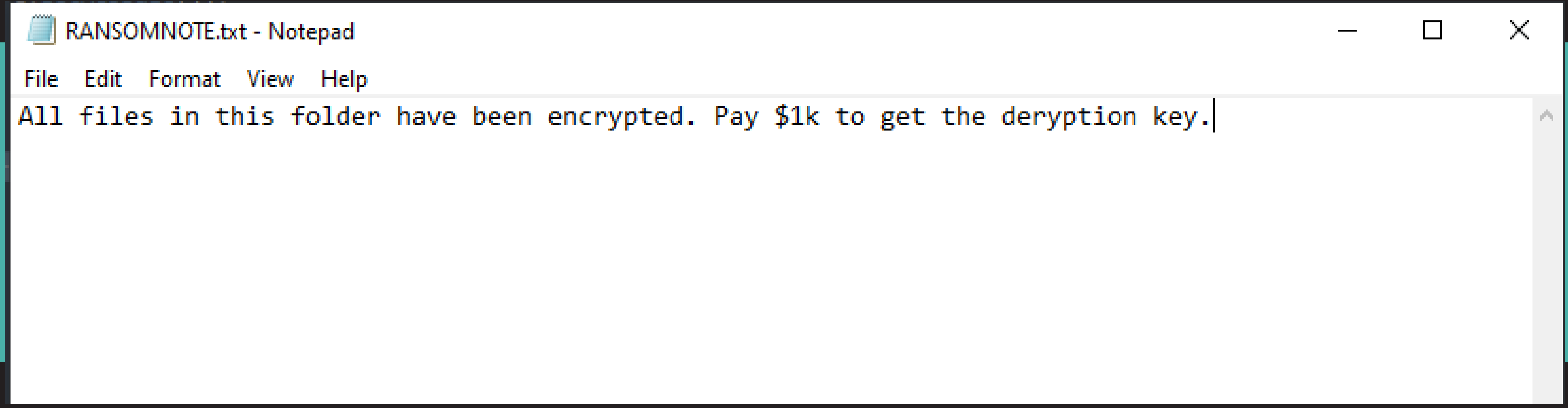


```
aced 0005 7372 001f 6a61 7661 782e 6372
7970 746f 2e73 7065 632e 5365 6372 6574
4b65 7953 7065 635b 470b 66e2 3061 4d02
0002 4c00 0961 6c67 6f72 6974 686d 7400
124c 6a61 7661 2f6c 616e 672f 5374 7269
6e67 3b5b 0003 6b65 7974 0002 5b42 7870
7400 0341 4553 7572 0002 5b42 acf3 17f8
0608 54e0 0200 0078 7000 0000 20cb b416
c262 d00c 4c7d 4f35 9ff0 c7b7 c883 1bce
ed87 7448 df08 20fc cfaf 7d09 4c
```

ENCRYTPTION KEY

- This key is randomly generated using AES (Advanced Encryption Standard) algorithm and saved as a file.
- This key is essential. Without it the encrypted files can not be restored.
- This is essentially a master key for the entire system.

RANSOM NOTE

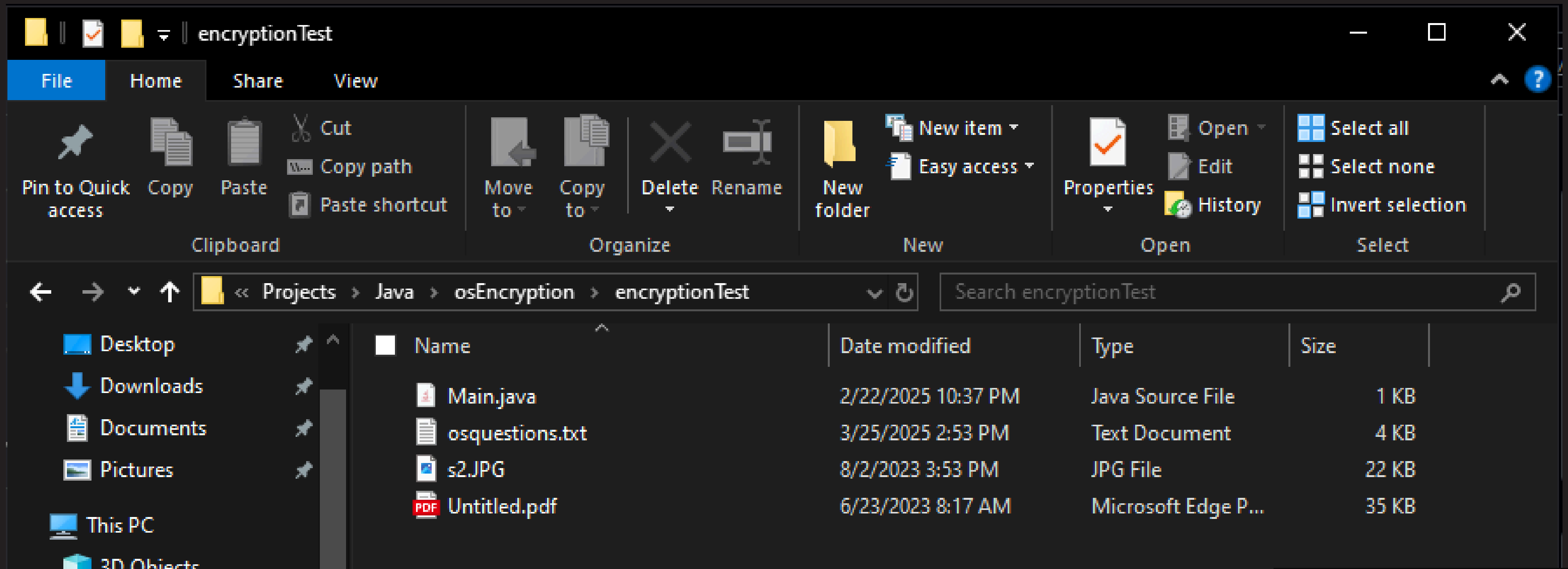


All files in this folder have been encrypted. Pay $1k to get the derytion key.

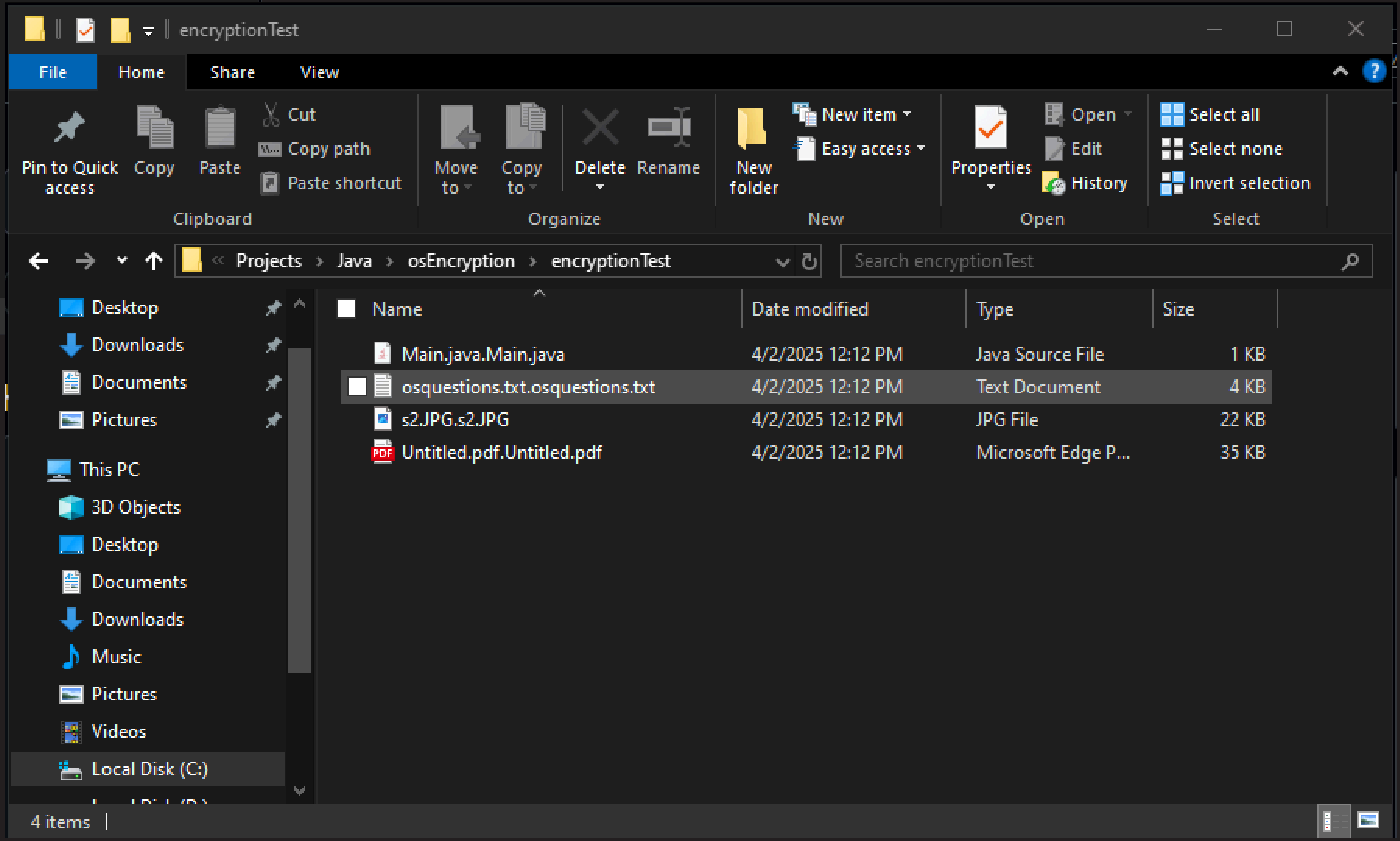
SHOULD VICTIMS PAY THE RANSOM

- The FBI does not support paying a ransom.
- Paying a ransom does not ensure that you or your organization will get any data back.
- By paying a ransom it will encourage attacks to continue to target more victims.

DECRYPTION METHODOLOGY

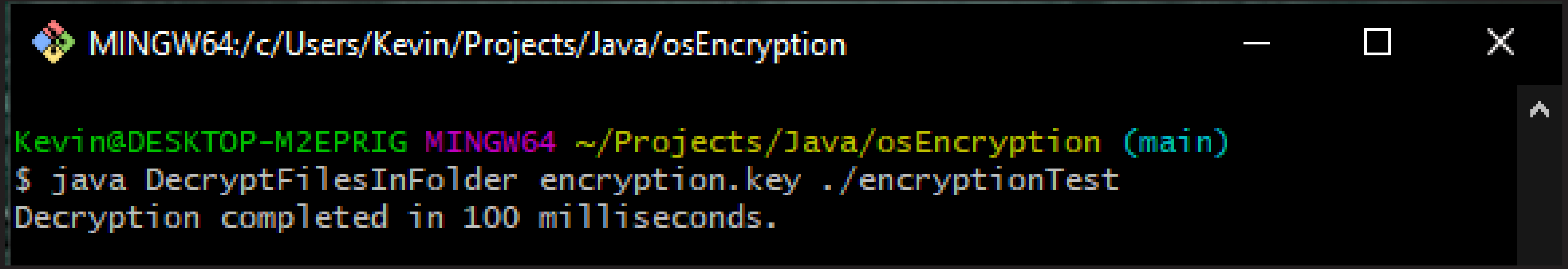


Name	Date modified	Type	Size
Main.java	2/22/2025 10:37 PM	Java Source File	1 KB
osquestions.txt	3/25/2025 2:53 PM	Text Document	4 KB
s2.JPG	8/2/2023 3:53 PM	JPG File	22 KB
Untitled.pdf	6/23/2023 8:17 AM	Microsoft Edge P...	35 KB



Name	Date modified	Type	Size
Main.java.Main.java	4/2/2025 12:12 PM	Java Source File	1 KB
osquestions.txt.osquestions.txt	4/2/2025 12:12 PM	Text Document	4 KB
s2.JPG.s2.JPG	4/2/2025 12:12 PM	JPG File	22 KB
Untitled.pdf.Untitled.pdf	4/2/2025 12:12 PM	Microsoft Edge P...	35 KB

BEFORE VS AFTER DECRYPTION

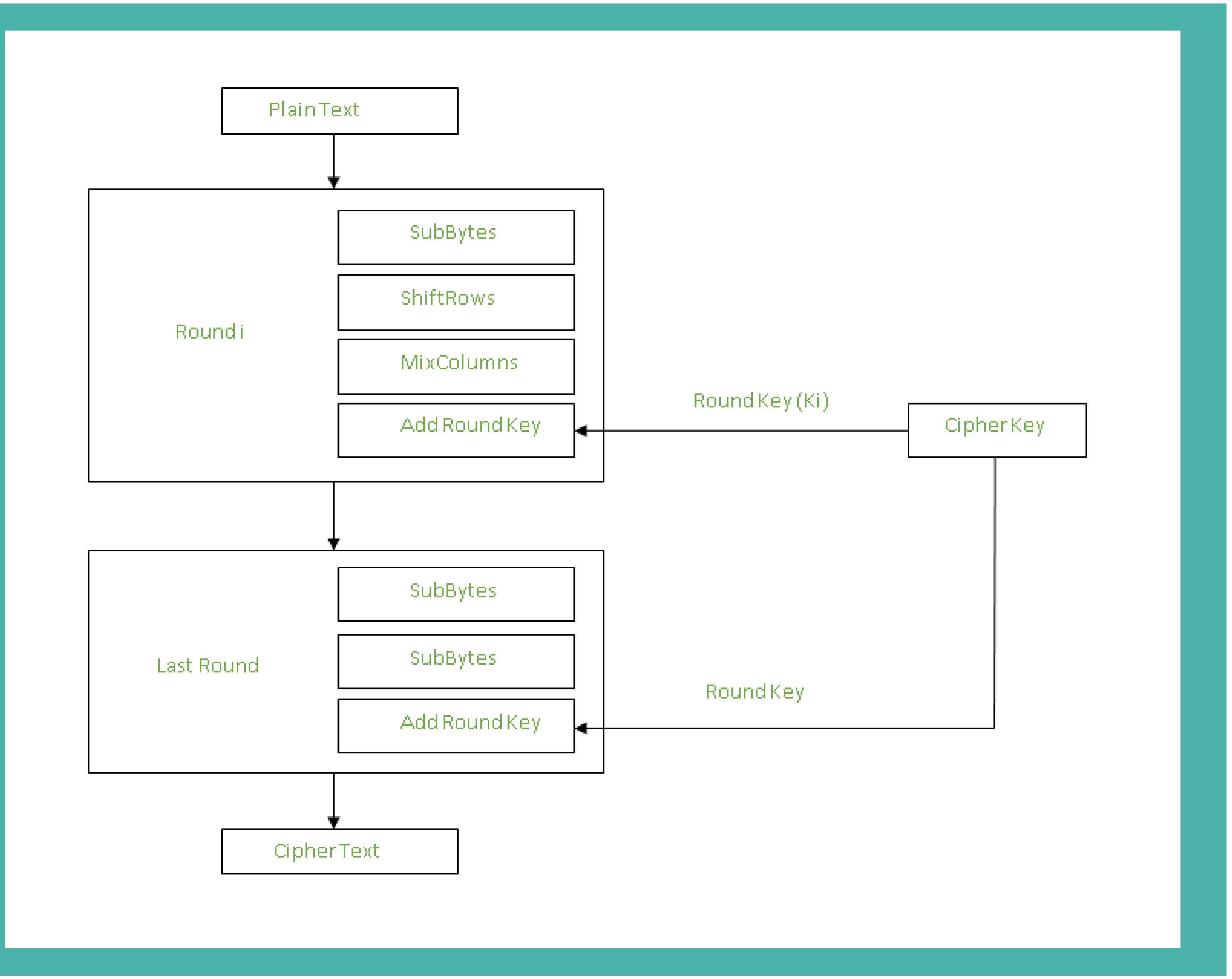


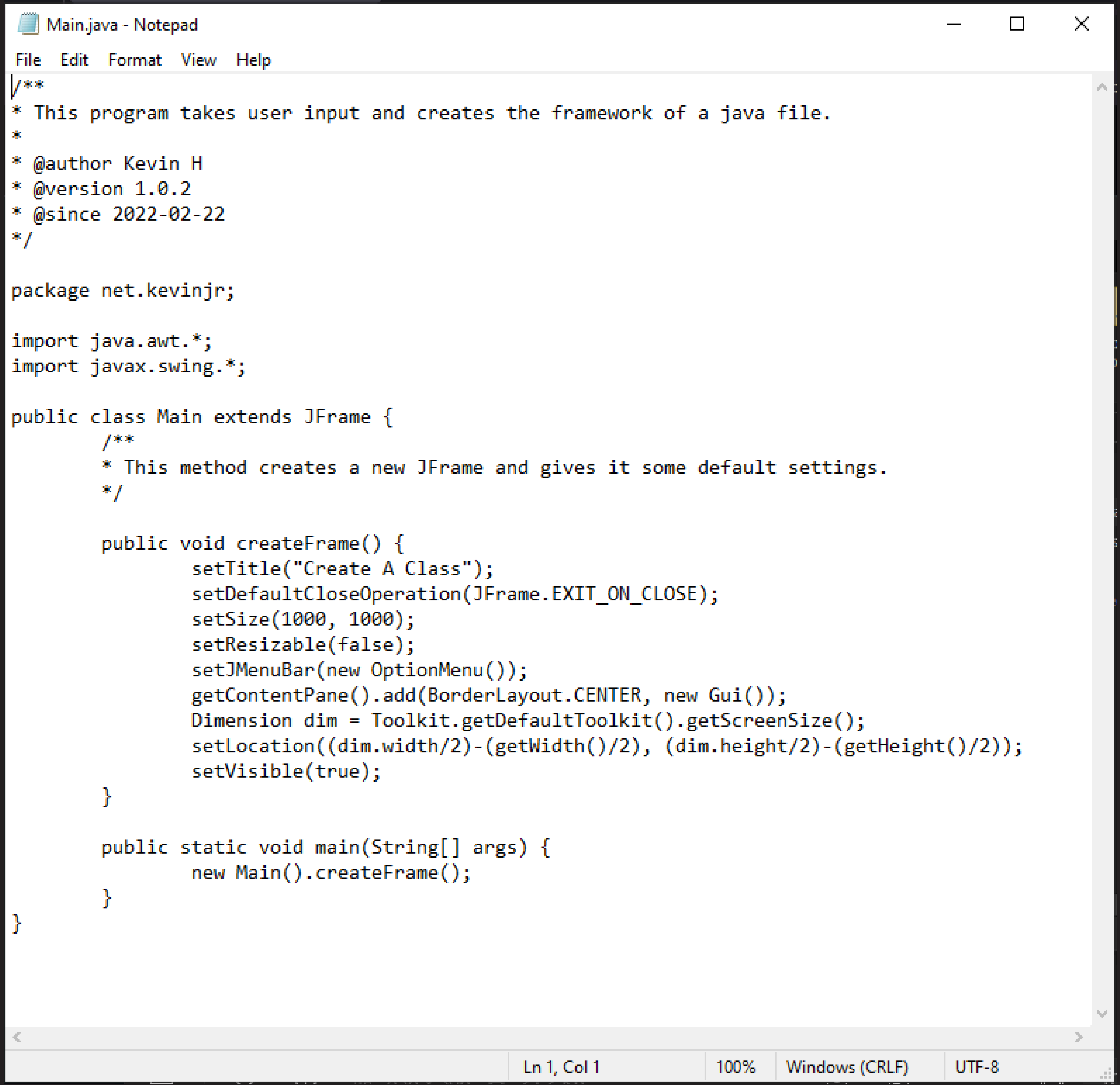
MINGW64:/c/Users/Kevin/Projects/Java/osEncryption

```
Kevin@DESKTOP-M2EPRIG MINGW64 ~/Projects/Java/osEncryption (main)
$ java DecryptFilesInFolder encryption.key ./encryptionTest
Decryption completed in 100 milliseconds.
```

General Program Flow

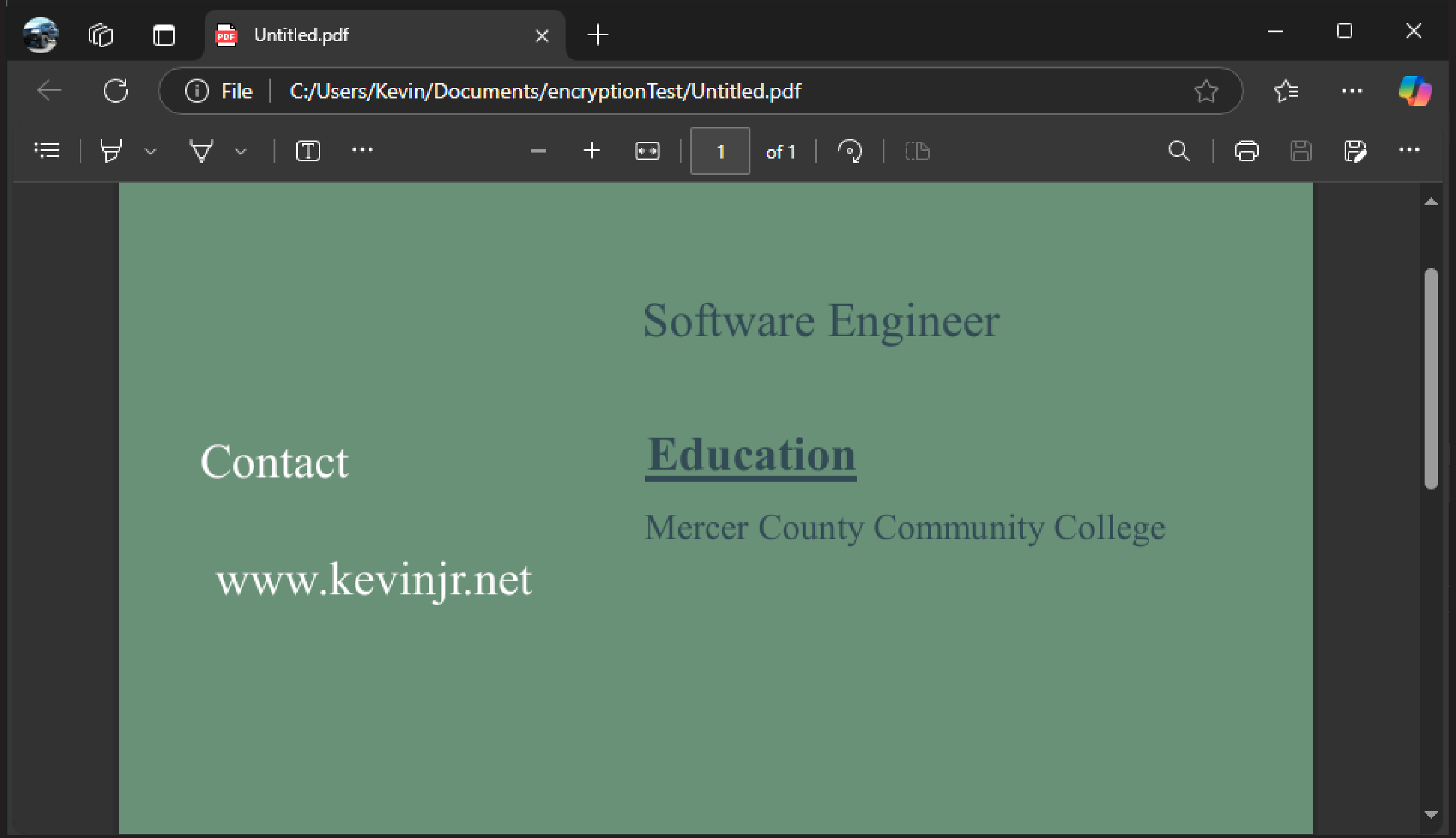
- Essentially the same algorithm as the encryption process
- To decrypt enter the folder as an argument to the java program
- We reuse the same key to decrypt each 16 byte block of data
- Once the file is decrypted reuse the original filename
- Delete ransom note
- (optional) Compare run time on various PC’s and OS’s





```
/**
* This program takes user input and creates the framework of a java file.
*
* @author Kevin H
* @version 1.0.2
* @since 2022-02-22
*/

package net.kevinjr;

import java.awt.*;
import javax.swing.*;

public class Main extends JFrame {
        /**
        * This method creates a new JFrame and gives it some default settings.
        */

        public void createFrame() {
                setTitle("Create A Class");
                setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);
                setSize(1000, 1000);
                setResizable(false);
                setJMenuBar(new OptionMenu());
                getContentPane().add(BorderLayout.CENTER, new Gui());
                Dimension dim = Toolkit.getDefaultToolkit().getScreenSize();
                setLocation((dim.width/2)-(getWidth()/2), (dim.height/2)-(getHeight()/2));
                setVisible(true);
        }

        public static void main(String[] args) {
                new Main().createFrame();
        }
}
```

DECRYPTED FILES



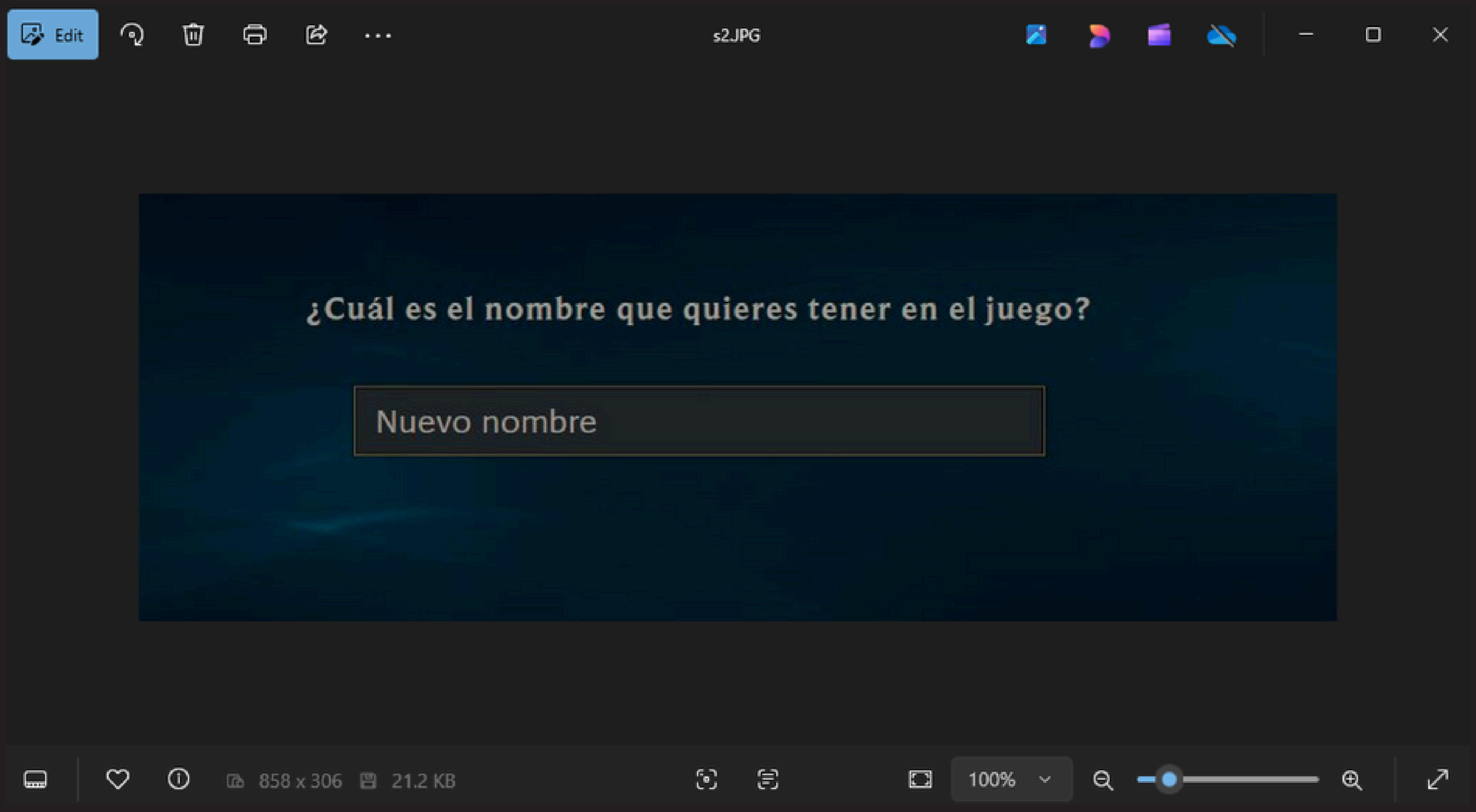
Software Engineer

Contact

www.kevinjr.net

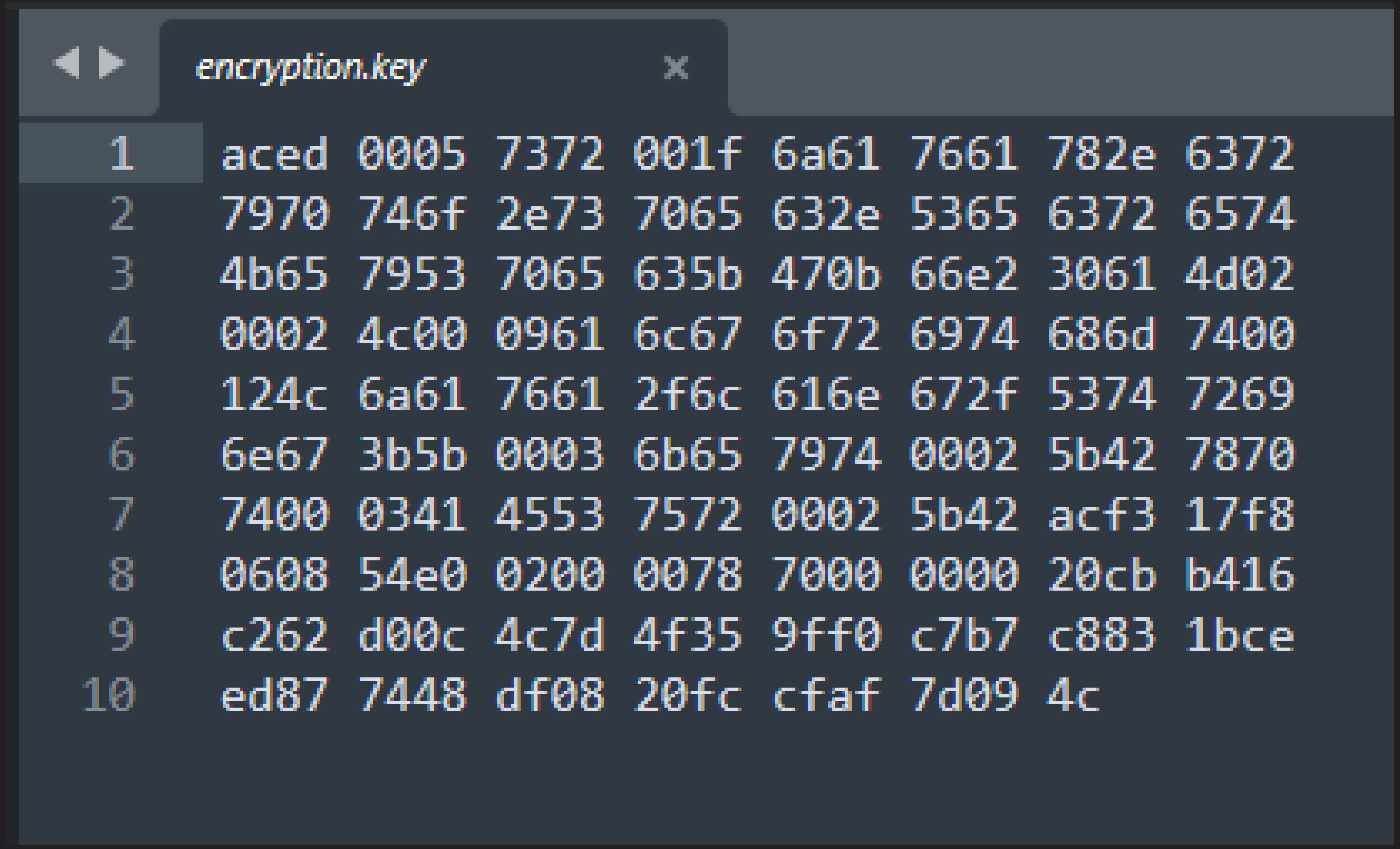
Education

Mercer County Community College



¿Cuál es el nombre que quieres tener en el juego?

Nuevo nombre



```
aced 0005 7372 001f 6a61 7661 782e 6372
7970 746f 2e73 7065 632e 5365 6372 6574
4b65 7953 7065 635b 470b 66e2 3061 4d02
0002 4c00 0961 6c67 6f72 6974 686d 7400
124c 6a61 7661 2f6c 616e 672f 5374 7269
6e67 3b5b 0003 6b65 7974 0002 5b42 7870
7400 0341 4553 7572 0002 5b42 acf3 17f8
0608 54e0 0200 0078 7000 0000 20cb b416
c262 d00c 4c7d 4f35 9ff0 c7b7 c883 1bce
ed87 7448 df08 20fc cfaf 7d09 4c
```

DECRYPTION KEY

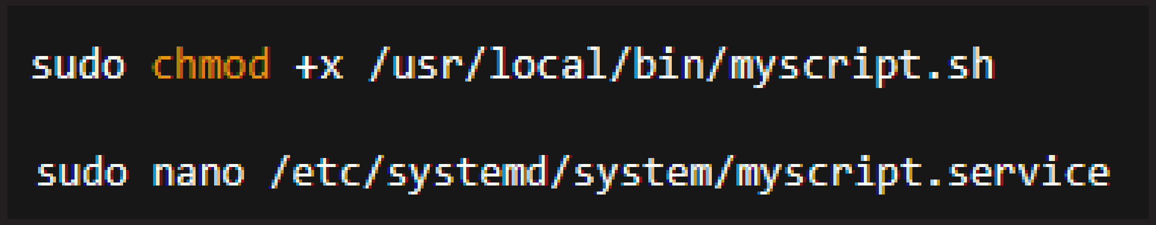
- This key is the same key that was used for encrypting the data.

PROCESS MONITORING

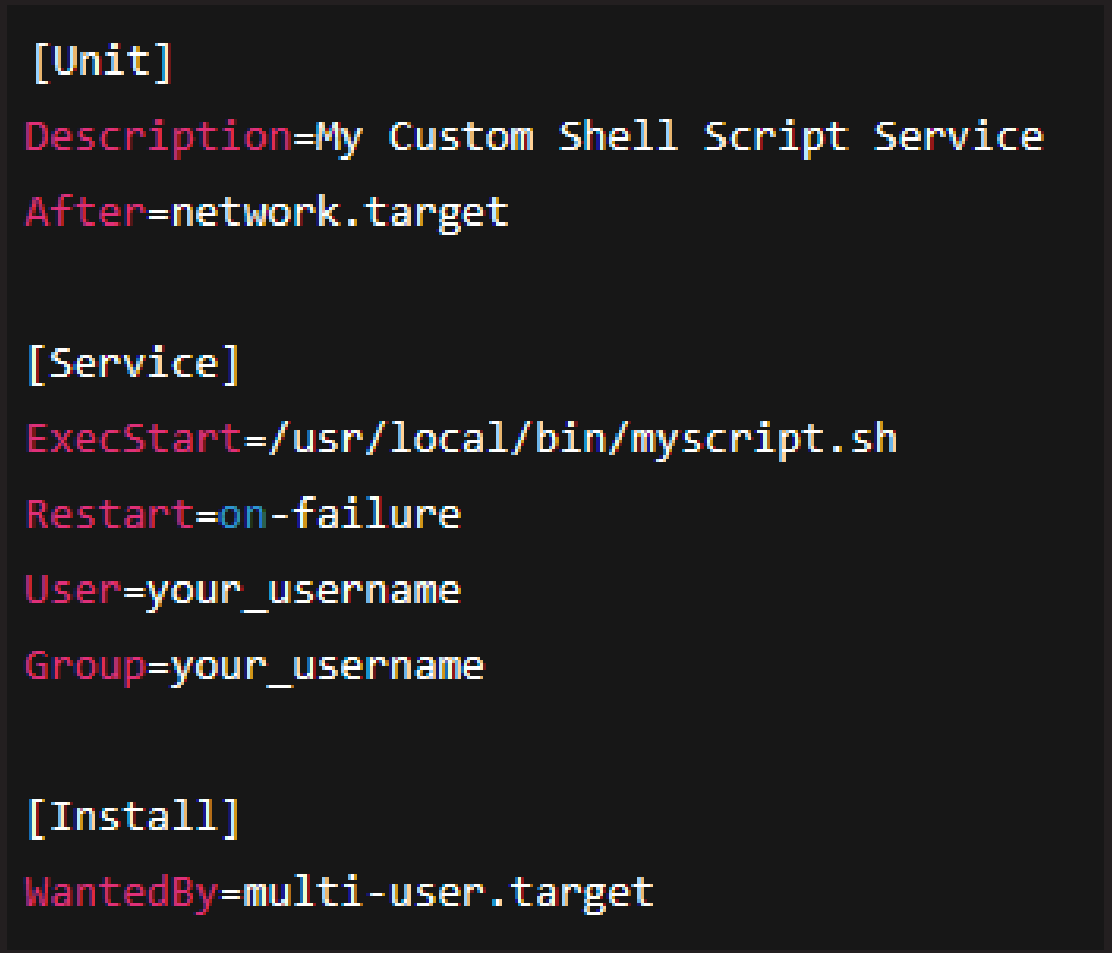
DETECTING ENCRYPTION

- Create a shell script that looks for file:
  - modifications
  - creations
  - deletions
- Within a certain folder or directory
- Process will halt
  - Asks user to terminate or continue process

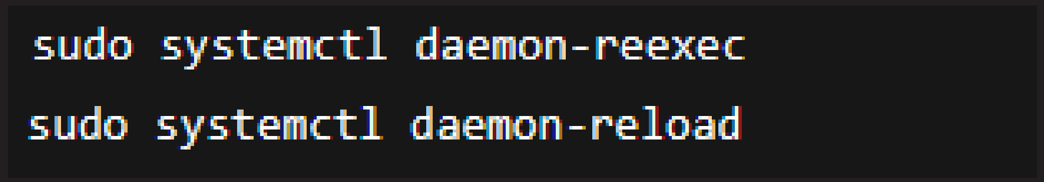
System Services



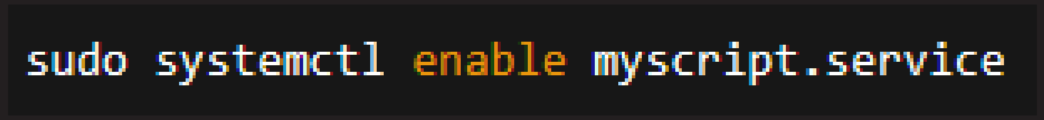
```
sudo chmod +x /usr/local/bin/myscript.sh

sudo nano /etc/systemd/system/myscript.service
```



```
[Unit]
Description=My Custom Shell Script Service
After=network.target

[Service]
ExecStart=/usr/local/bin/myscript.sh
Restart=on-failure
User=your_username
Group=your_username

[Install]
WantedBy=multi-user.target
```



```
sudo systemctl daemon-reexec
sudo systemctl daemon-reload
```



```
sudo systemctl enable myscript.service
```

STEPS RANSOMWARE VICTIMS SHOULD TAKE

- Step 1: Evaluate
  - Identify ransomware type & risks
  - Explore recovery options
  - Analyze security gaps
- Step 2: Secure
  - Isolate systems
  - Implement security measures to prevent reinfection
- Step 3: Recover
  - Restore systems
  - Ensure integrity of recovered data integrity
  - Verify security before system goes live again
- Step 4: Report
  - Provide incident reports (www.ic3.gov)
  - Assist with audits & investigations

THANK YOU

Questions?

RESOURCES

Chittooparambil, S., et al. "Ransomware Detection Using Random Forest Technique." Procedia Computer Science, vol. 170, 2020, pp. 381–388.

Continella, A., et al. "A Clever New Tool Shuts Down Ransomware Before It's Too Late." Wired, 24 July 2017, www.wired.com/story/shieldfs-ransomware-protection-tool.

FBI. Ransomware. FBI, www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware.

Oz, H., et al. "A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions." arXiv, 11 Feb. 2021, arxiv.org/abs/2102.06249.

Shaukat, M., and M. Ribeiro. "Ransomware Early Detection: A Survey." Future Generation Computer Systems, vol. 133, 2023, pp. 1–18.

Yaqoob, I., et al. "Ransomware: Recent Advances, Analysis, Challenges and Future Directions." Computers & Security, vol. 106, 2021, p. 102