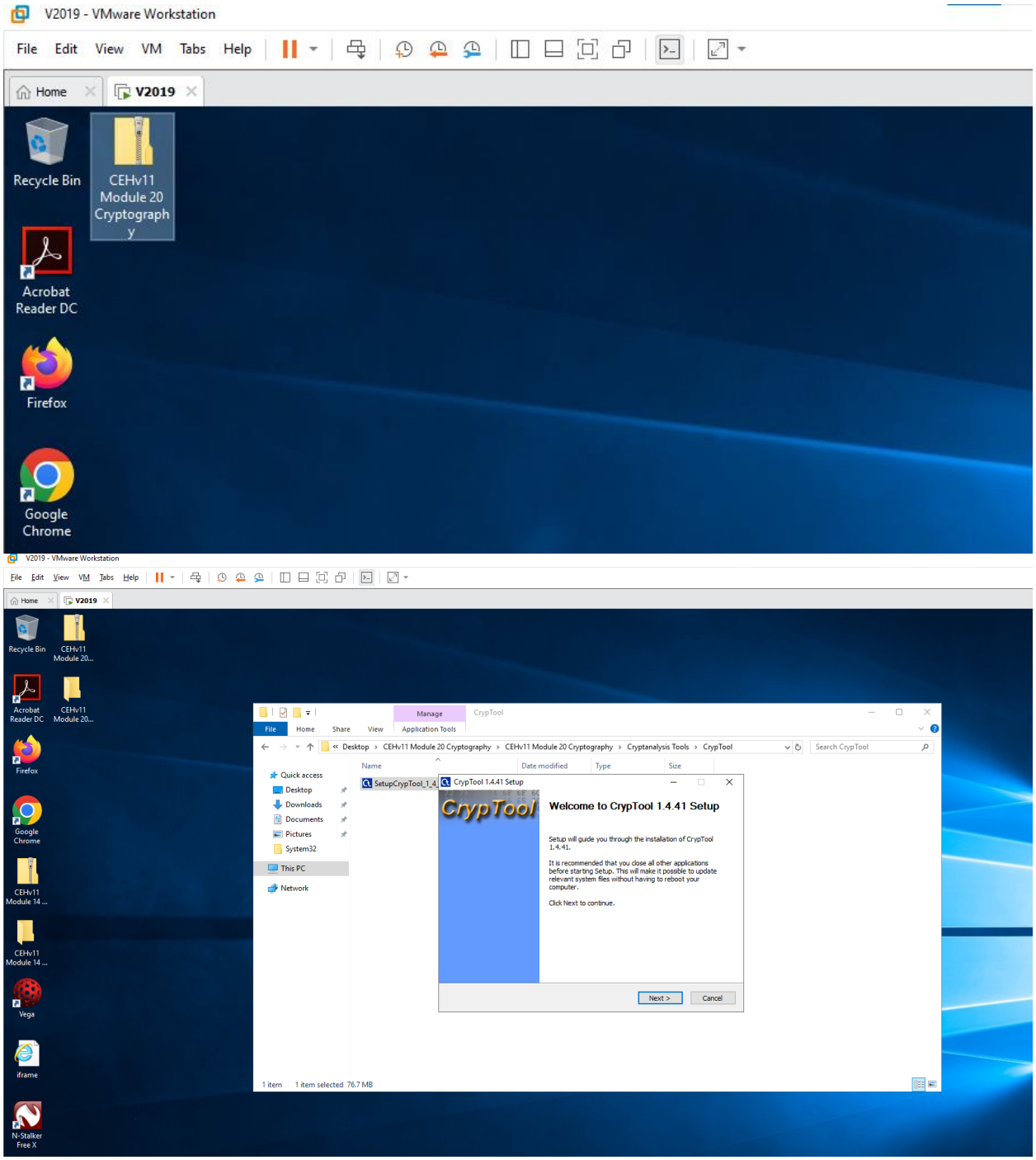
Lab 14: XOR Encryption in Python (10 pts.)

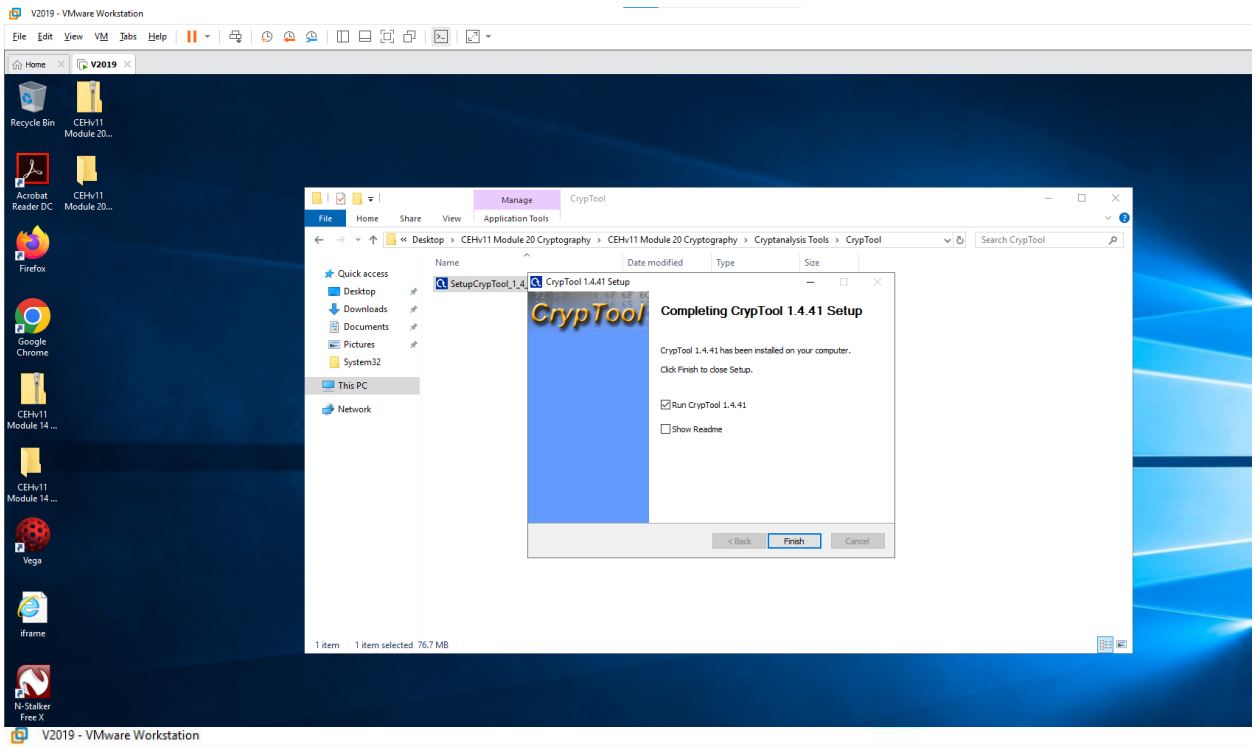
Course Name: Ethical Hacking and Offensive Security(HOD401)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 28/10/2023

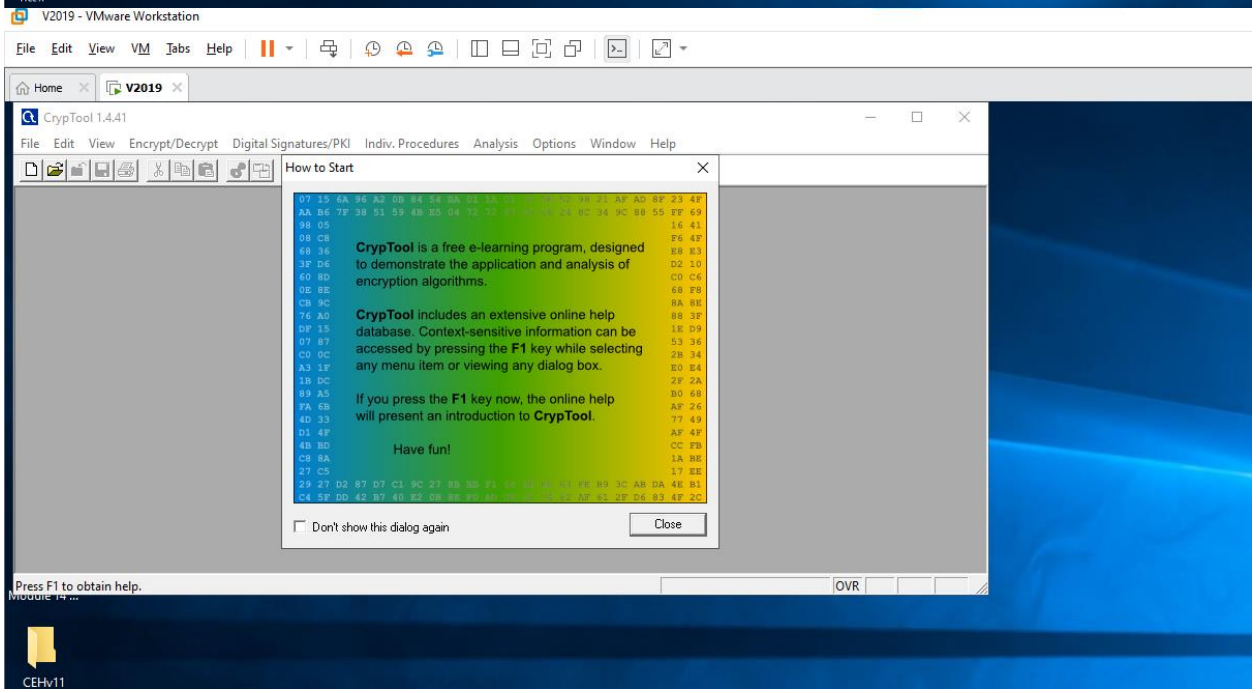
5. Perform Cryptanalysis using Various Cryptanalysis Tools

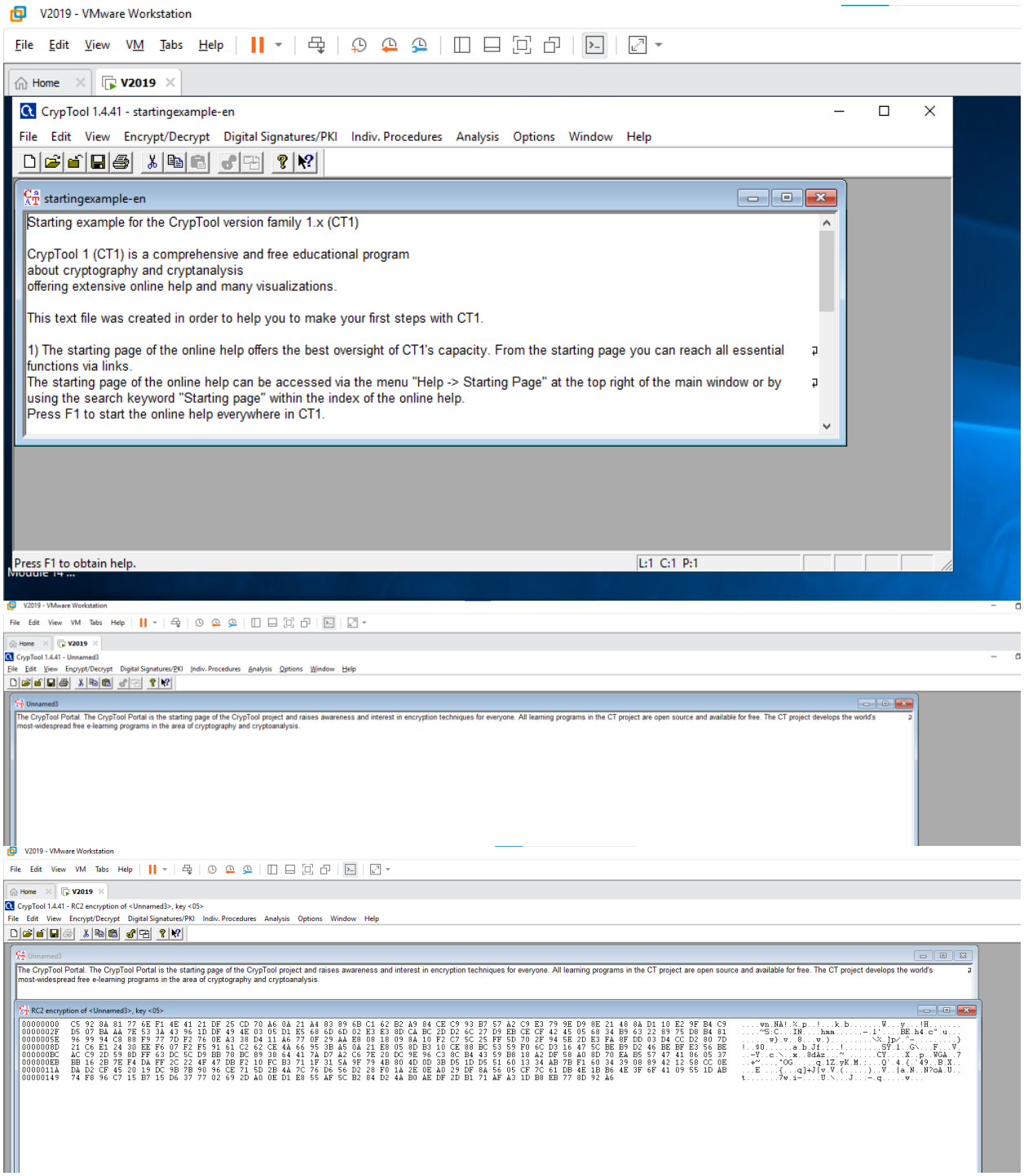
5.1 Perform Cryptanalysis using CrypTool

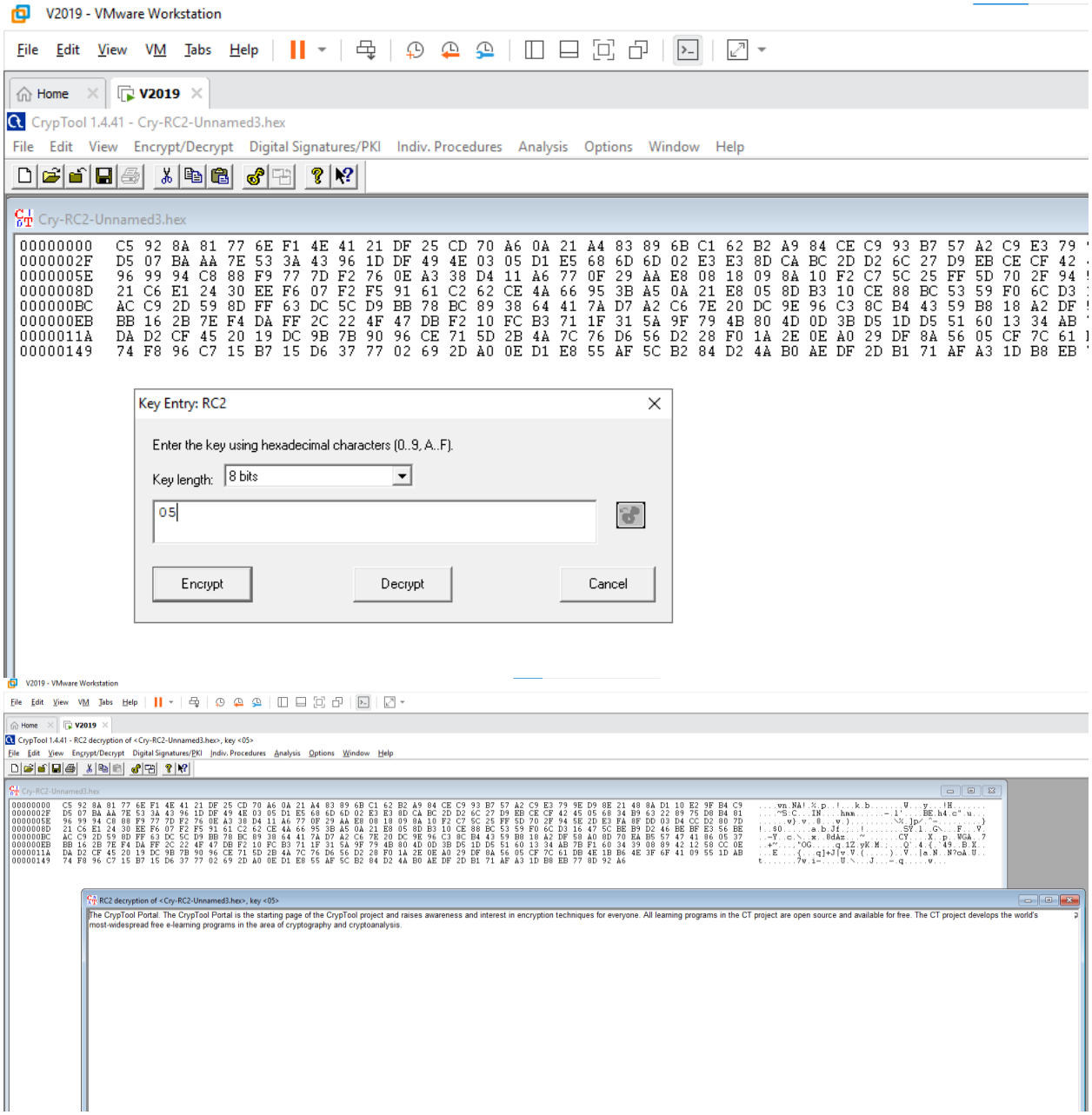
- Open Windows 10 and Windows Server 2019


V2019 - VMware Workstation
File Edit View VM Tabs Help
Home
V2019
Recycle Bin
CEHv11 Module 20 Cryptography
Acrobat Reader DC
Firefox
Google Chrome
Manage
CrypTool
File Home Share View Application Tools
Desktop › CEHv11 Module 20 Cryptography › CEHv11 Module 20 Cryptography › Cryptanalysis Tools › CrypTool
Search CrypTool
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name
Date modified
Type
Size
SetupCrypTool_1_4
CrypTool 1.4.41 Setup
CrypTool
Welcome to CrypTool 1.4.41 Setup
Setup will guide you through the installation of CrypTool 1.4.41.
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.
Click Next to continue.
Next >
Cancel
1 item
1 item selected 76.7 MB
CEHv11 Module 14 ...
Vega
iframe
N-Stalker Free X

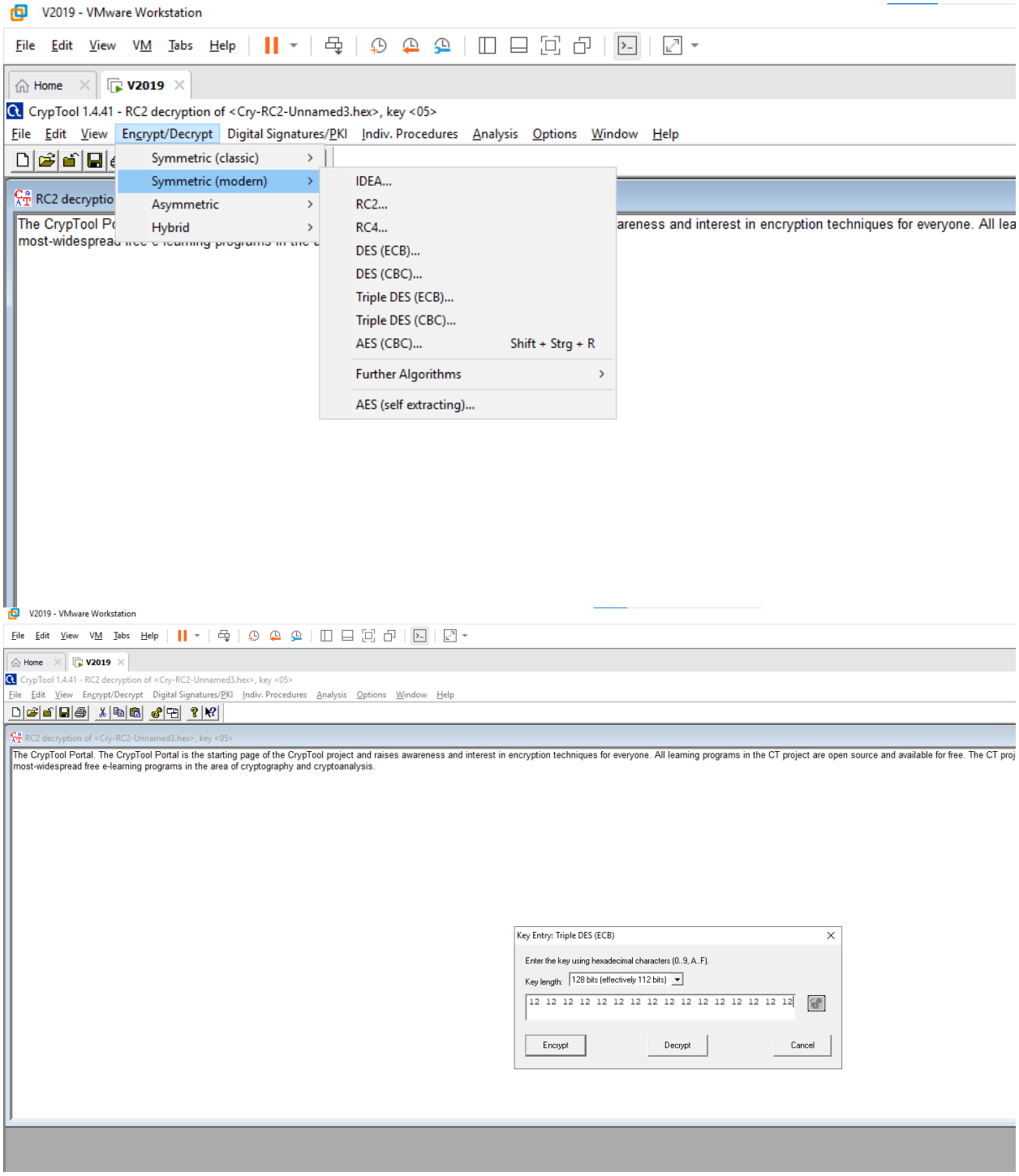

V2019 - VMware Workstation
File Edit View VM Tabs Help
Home
V2019
Recycle Bin
CEHv11 Module 20...
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module 14 ...
Vega
iframe
N-Stalker Free X
Manage
CrypTool
File Home Share View Application Tools
Desktop › CEHv11 Module 20 Cryptography › CEHv11 Module 20 Cryptography › Cryptanalysis Tools › CrypTool
Search CrypTool
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name
Date modified
Type
Size
SetupCrypTool_1_4
CrypTool 1.4.41 Setup
CrypTool
Completing CrypTool 1.4.41 Setup
CrypTool 1.4.41 has been installed on your computer.
Click Finish to close Setup.
Run CrypTool 1.4.41
Show Readme
< Back
Finish
Cancel
1 item
1 item selected 76.7 MB

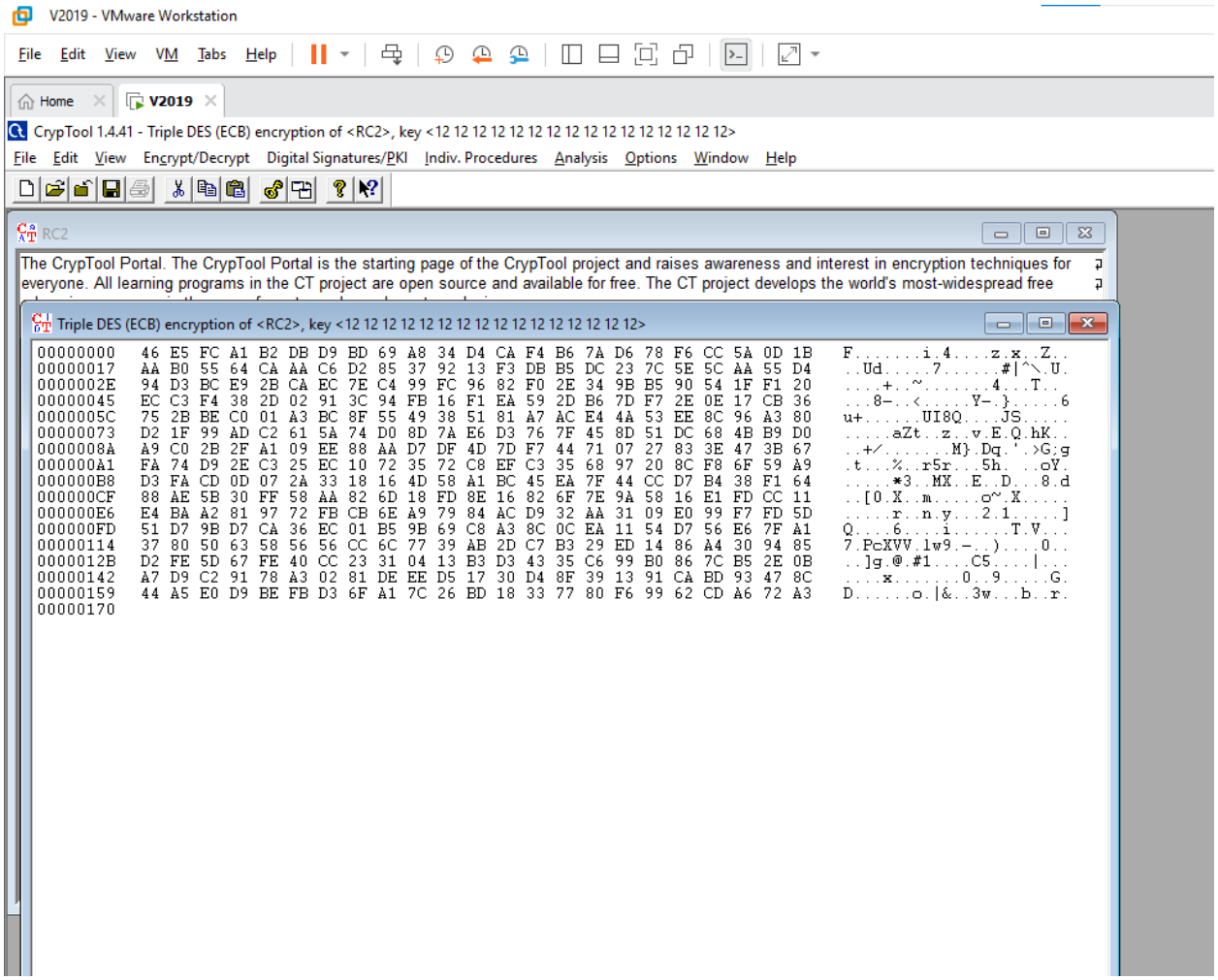

V2019 - VMware Workstation
File Edit View VM Tabs Help
Home
V2019
CrypTool 1.4.41
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
How to Start
CrypTool is a free e-learning program, designed to demonstrate the application and analysis of encryption algorithms.
CrypTool includes an extensive online help database. Context-sensitive information can be accessed by pressing the F1 key while selecting any menu item or viewing any dialog box.
If you press the F1 key now, the online help will present an introduction to CrypTool.
Have fun!
Don't show this dialog again
Close
Press F1 to obtain help.
OVR
CEHv11

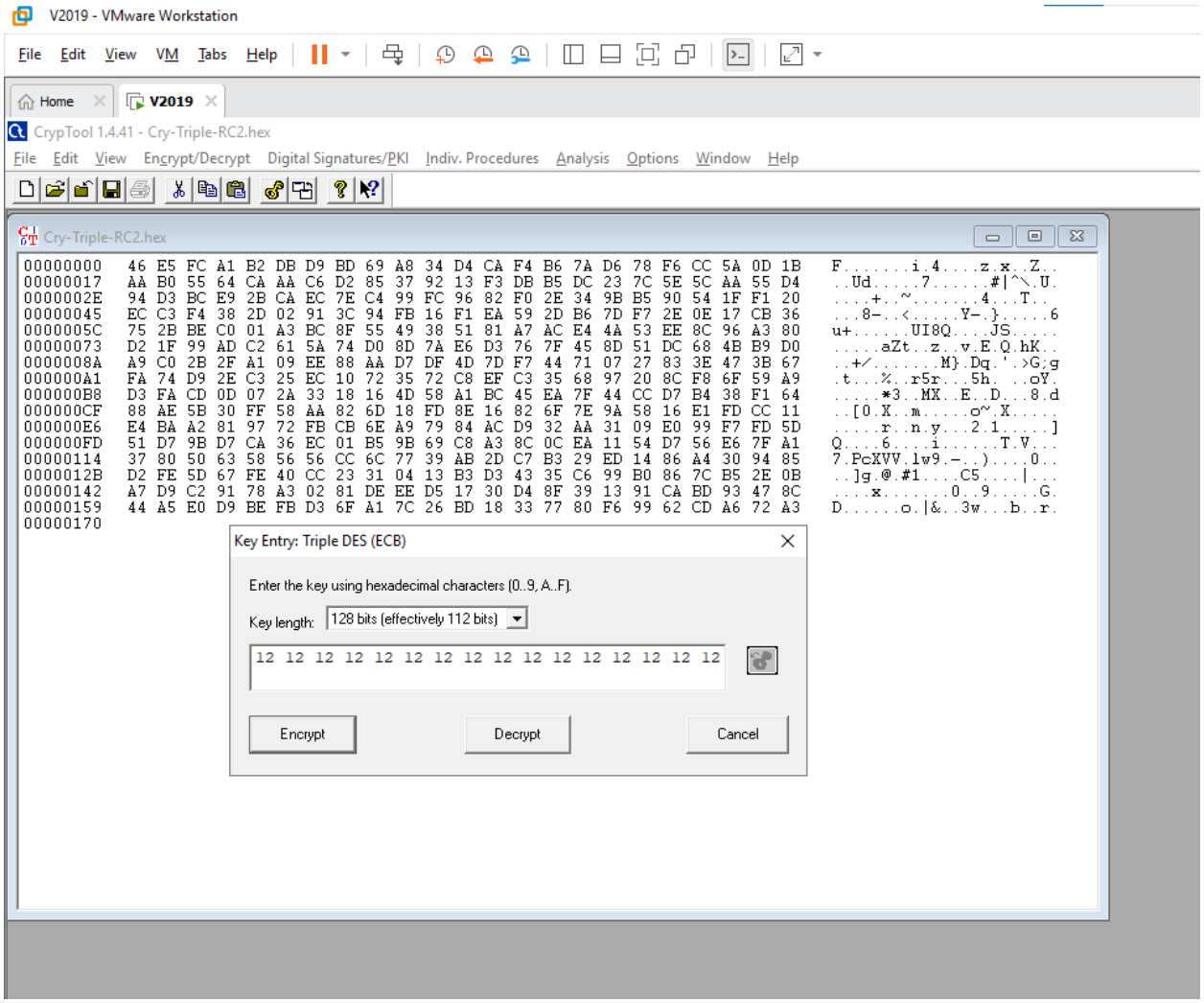

V2019 - VMware Workstation
File Edit View VM Tabs Help
Home
V2019
CrypTool 1.4.41 - startingexample-en
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en
Starting example for the CrypTool version family 1.x (CT1)
CrypTool 1 (CT1) is a comprehensive and free educational program
about cryptography and cryptanalysis
offering extensive online help and many visualizations.
This text file was created in order to help you to make your first steps with CT1.
1) The starting page of the online help offers the best oversight of CT1's capacity. From the starting page you can reach all essential functions via links.
The starting page of the online help can be accessed via the menu "Help -> Starting Page" at the top right of the main window or by using the search keyword "Starting page" within the index of the online help.
Press F1 to start the online help everywhere in CT1.
Press F1 to obtain help.
L:1 C:1 P:1
Unnamed3
The CrypTool Portal. The CrypTool Portal is the starting page of the CrypTool project and raises awareness and interest in encryption techniques for everyone. All learning programs in the CT project are open source and available for free. The CT project develops the world's most-widespread free e-learning programs in the area of cryptography and cryptoanalysis.
RC2 encryption of <Unnamed3>, key <05>

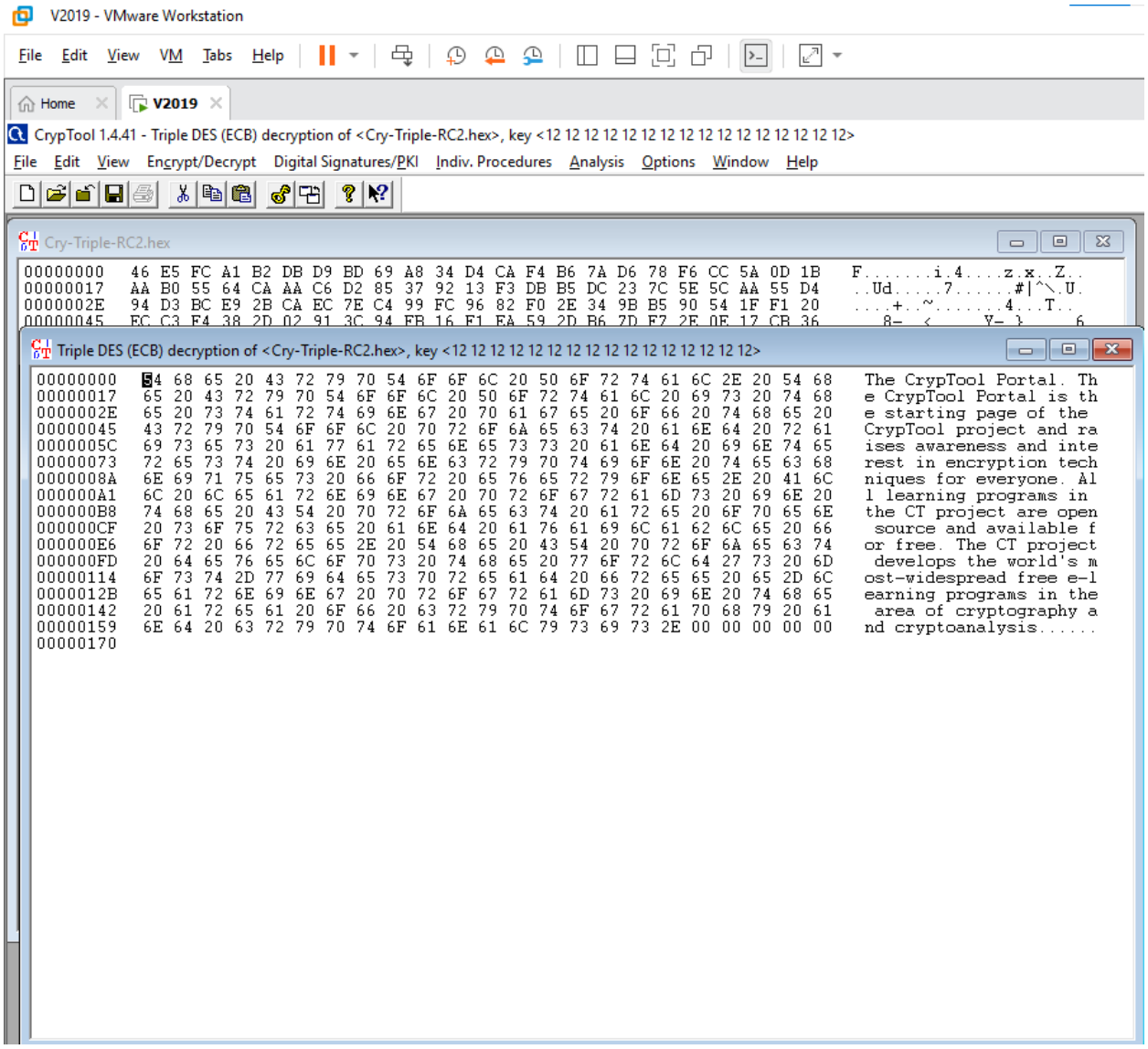

V2019 - VMware Workstation
File Edit View VM Tabs Help
Home
V2019
CrypTool 1.4.41 - Cry-RC2-Unnamed3.hex
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Cry-RC2-Unnamed3.hex
00000000 C5 92 8A 81 77 6E F1 4E 41 21 DF 25 CD 70 A6 0A 21 A4 83 89 6B C1 62 B2 A9 84 CE C9 93 B7 57 A2 C9 E3 79
0000002F D5 07 BA AA 7E 53 3A 43 96 1D DF 49 4E 03 05 D1 E5 68 6D 6D 02 E3 E3 8D CA BC 2D D2 6C 27 D9 EB CE CF 42
0000005E 96 99 94 C8 88 F9 77 7D F2 76 0E A3 38 D4 11 A6 77 0F 29 AA E8 08 18 09 8A 10 F2 C7 5C 25 FF 5D 70 2F 94
0000008D 21 C6 E1 24 30 EE F6 07 F2 F5 91 61 C2 62 CE 4A 66 95 3B A5 0A 21 E8 05 8D B3 10 CE 88 BC 53 59 F0 6C D3
000000BC AC C9 2D 59 8D FF 63 DC 5C D9 BB 78 BC 89 38 64 41 7A D7 A2 C6 7E 20 DC 9E 96 C3 8C B4 43 59 B8 18 A2 DF
000000EB BB 16 2B 7E F4 DA FF 2C 22 4F 47 DB F2 10 FC B3 71 1F 31 5A 9F 79 4B 80 4D 0D 3B D5 1D D5 51 60 13 34 AB
0000011A DA D2 CF 45 20 19 DC 9B 7B 90 96 CE 71 5D 2B 4A 7C 76 D6 56 D2 28 F0 1A 2E 0E A0 29 DF 8A 56 05 CF 7C 61
00000149 74 F8 96 C7 15 B7 15 D6 37 77 02 69 2D A0 0E D1 E8 55 AF 5C B2 84 D2 4A B0 AE DF 2D B1 71 AF A3 1D B8 EB
Key Entry: RC2
Enter the key using hexadecimal characters (0..9, A..F).
Key length: 8 bits
05
Encrypt
Decrypt
Cancel

V2019 - VMware Workstation
CrypTool 1.4.41 - RC2 decryption of <Cry-RC2-Unnamed3.hex>, key <05>
RC2 decryption of <Cry-RC2-Unnamed3.hex>, key <05>
The CrypTool Portal. The CrypTool Portal is the starting page of the CrypTool project and raises awareness and interest in encryption techniques for everyone. All learning programs in the CT project are open source and available for free. The CT project develops the world's most-widespread free e-learning programs in the area of cryptography and cryptoanalysis.

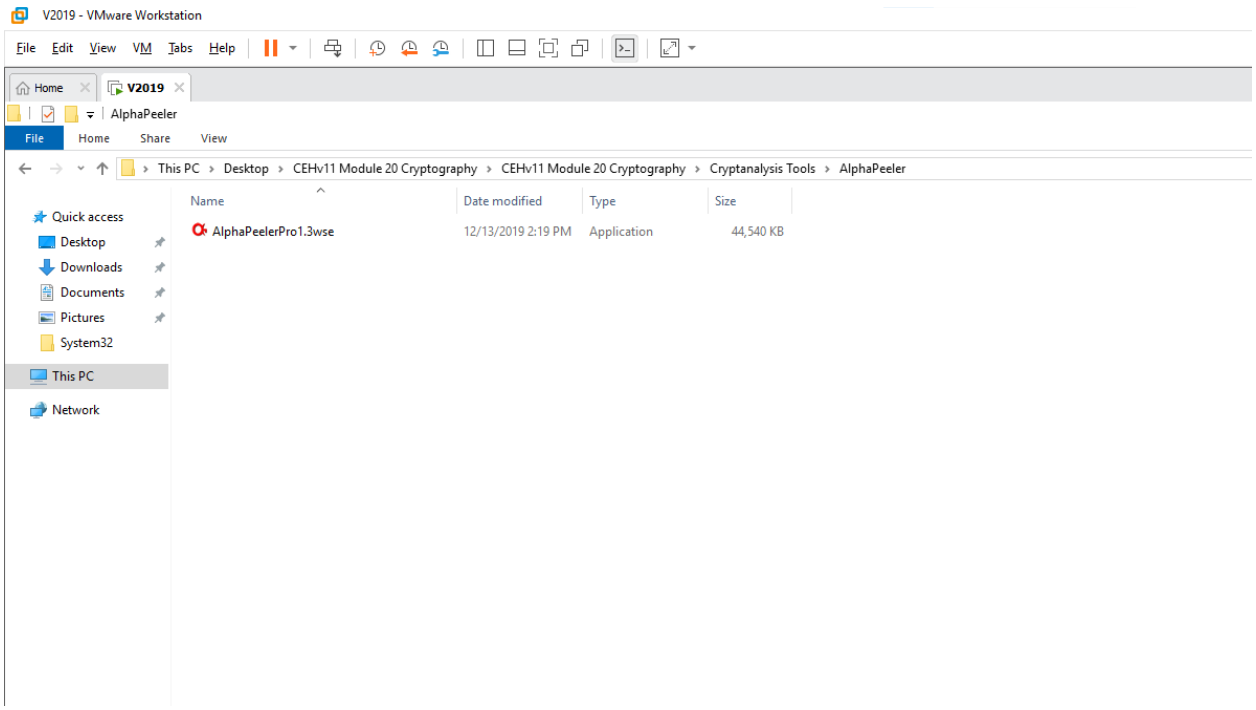

V2019 - VMware Workstation
File Edit View VM Tabs Help
Home
V2019
CrypTool 1.4.41 - RC2 decryption of <Cry-RC2-Unnamed3.hex>, key <05>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Symmetric (classic)
Symmetric (modern)
Asymmetric
Hybrid
IDEA...
RC2...
RC4...
DES (ECB)...
DES (CBC)...
Triple DES (ECB)...
Triple DES (CBC)...
AES (CBC)... Shift + Strg + R
Further Algorithms
AES (self extracting)...
RC2 decryptio
The CrypTool Po
areness and interest in encryption techniques for everyone. All lea
most-widespread
V2019 - VMware Workstation
File Edit View VM Tabs Help
Home
V2019
CrypTool 1.4.41 - RC2 decryption of <Cry-RC2-Unnamed3.hex>, key <05>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
RC2 decryption of <Cry-RC2-Unnamed3.hex>, key <05>
The CrypTool Portal. The CrypTool Portal is the starting page of the CrypTool project and raises awareness and interest in encryption techniques for everyone. All learning programs in the CT project are open source and available for free. The CT proj
most-widespread free e-learning programs in the area of cryptography and cryptoanalysis.
Key Entry: Triple DES (ECB)
Enter the key using hexadecimal characters (0..9, A..F).
Key length: 128 bits (effectively 112 bits)
12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12
Encrypt
Decrypt
Cancel

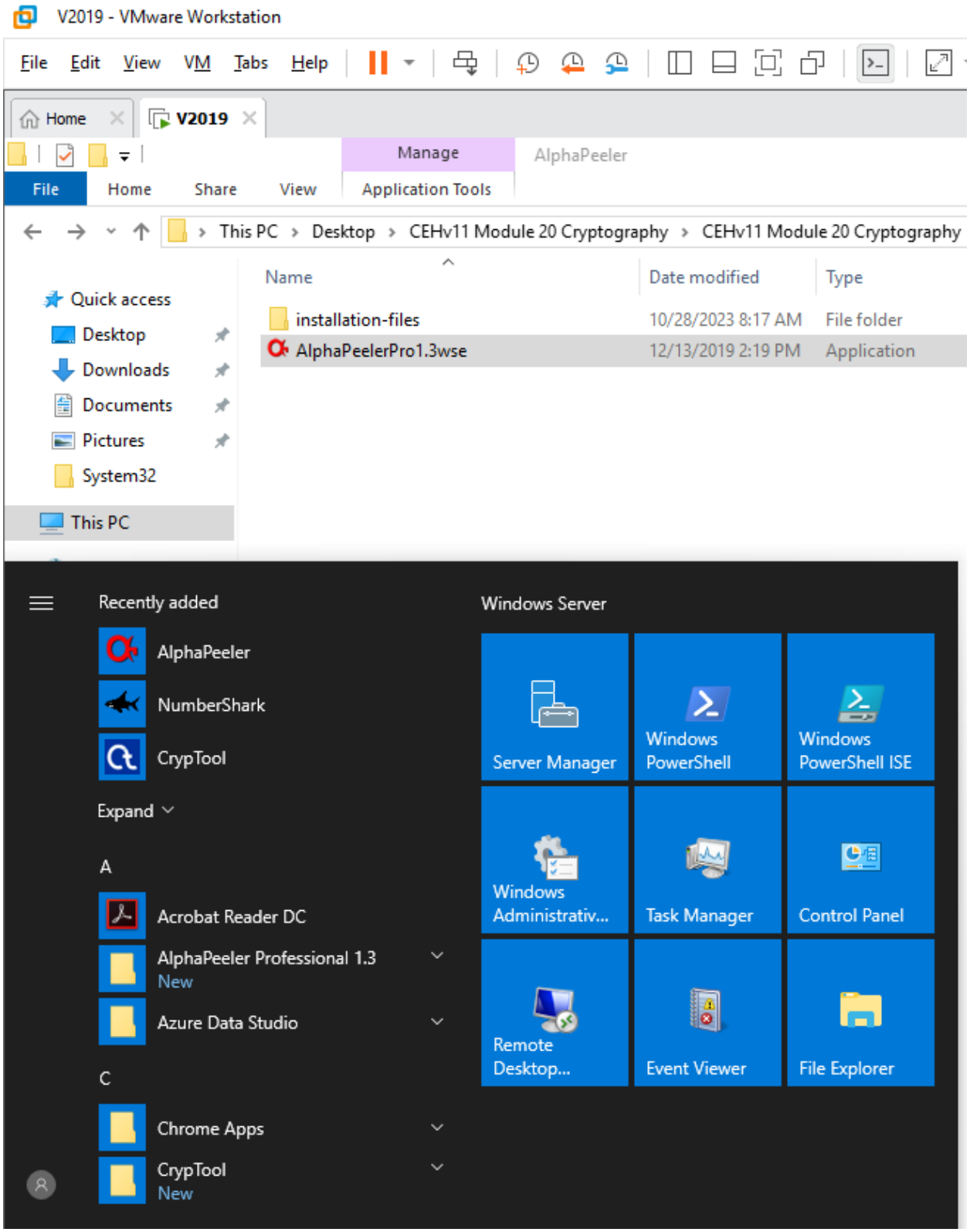

V2019 - VMware Workstation
File Edit View VM Tabs Help
Home
V2019
CrypTool 1.4.41 - Triple DES (ECB) encryption of <RC2>, key <12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
RC2
The CrypTool Portal. The CrypTool Portal is the starting page of the CrypTool project and raises awareness and interest in encryption techniques for everyone. All learning programs in the CT project are open source and available for free. The CT project develops the world's most-widespread free
Triple DES (ECB) encryption of <RC2>, key <12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12>
00000000 46 E5 FC A1 B2 DB D9 BD 69 A8 34 D4 CA F4 B6 7A D6 78 F6 CC 5A 0D 1B
00000017 AA B0 55 64 CA AA C6 D2 85 37 92 13 F3 DB B5 DC 23 7C 5E 5C AA 55 D4
0000002E 94 D3 BC E9 2B CA EC 7E C4 99 FC 96 82 F0 2E 34 9B B5 90 54 1F F1 20
00000045 EC C3 F4 38 2D 02 91 3C 94 FB 16 F1 EA 59 2D B6 7D F7 2E 0E 17 CB 36
0000005C 75 2B BE C0 01 A3 BC 8F 55 49 38 51 81 A7 AC E4 4A 53 EE 8C 96 A3 80
00000073 D2 1F 99 AD C2 61 5A 74 D0 8D 7A E6 D3 76 7F 45 8D 51 DC 68 4B B9 D0
0000008A A9 C0 2B 2F A1 09 EE 88 AA D7 DF 4D 7D F7 44 71 07 27 83 3E 47 3B 67
000000A1 FA 74 D9 2E C3 25 EC 10 72 35 72 C8 EF C3 35 68 97 20 8C F8 6F 59 A9
000000B8 D3 FA CD 0D 07 2A 33 18 16 4D 58 A1 BC 45 EA 7F 44 CC D7 B4 38 F1 64
000000CF 88 AE 5B 30 FF 58 AA 82 6D 18 FD 8E 16 82 6F 7E 9A 58 16 E1 FD CC 11
000000E6 E4 BA A2 81 97 72 FB CB 6E A9 79 84 AC D9 32 AA 31 09 E0 99 F7 FD 5D
000000FD 51 D7 9B D7 CA 36 EC 01 B5 9B 69 C8 A3 8C 0C EA 11 54 D7 56 E6 7F A1
00000114 37 80 50 63 58 56 56 CC 6C 77 39 AB 2D C7 B3 29 ED 14 86 A4 30 94 85
0000012B D2 FE 5D 67 FE 40 CC 23 31 04 13 B3 D3 43 35 C6 99 B0 86 7C B5 2E 0B
00000142 A7 D9 C2 91 78 A3 02 81 DE EE D5 17 30 D4 8F 39 13 91 CA BD 93 47 8C
00000159 44 A5 E0 D9 BE FB D3 6F A1 7C 26 BD 18 33 77 80 F6 99 62 CD A6 72 A3
00000170

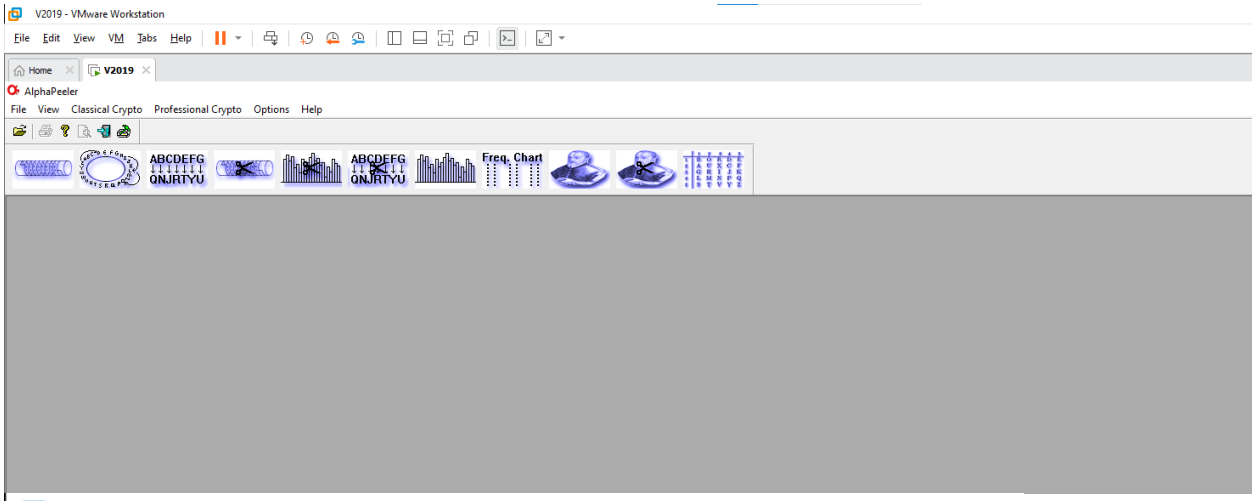

V2019 - VMware Workstation
File Edit View VM Tabs Help
Home
V2019
CrypTool 1.4.41 - Cry-Triple-RC2.hex
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Cry-Triple-RC2.hex
00000000 46 E5 FC A1 B2 DB D9 BD 69 A8 34 D4 CA F4 B6 7A D6 78 F6 CC 5A 0D 1B
00000017 AA B0 55 64 CA AA C6 D2 85 37 92 13 F3 DB B5 DC 23 7C 5E 5C AA 55 D4
0000002E 94 D3 BC E9 2B CA EC 7E C4 99 FC 96 82 F0 2E 34 9B B5 90 54 1F F1 20
00000045 EC C3 F4 38 2D 02 91 3C 94 FB 16 F1 EA 59 2D B6 7D F7 2E 0E 17 CB 36
0000005C 75 2B BE C0 01 A3 BC 8F 55 49 38 51 81 A7 AC E4 4A 53 EE 8C 96 A3 80
00000073 D2 1F 99 AD C2 61 5A 74 D0 8D 7A E6 D3 76 7F 45 8D 51 DC 68 4B B9 D0
0000008A A9 C0 2B 2F A1 09 EE 88 AA D7 DF 4D 7D F7 44 71 07 27 83 3E 47 3B 67
000000A1 FA 74 D9 2E C3 25 EC 10 72 35 72 C8 EF C3 35 68 97 20 8C F8 6F 59 A9
000000B8 D3 FA CD 0D 07 2A 33 18 16 4D 58 A1 BC 45 EA 7F 44 CC D7 B4 38 F1 64
000000CF 88 AE 5B 30 FF 58 AA 82 6D 18 FD 8E 16 82 6F 7E 9A 58 16 E1 FD CC 11
000000E6 E4 BA A2 81 97 72 FB CB 6E A9 79 84 AC D9 32 AA 31 09 E0 99 F7 FD 5D
000000FD 51 D7 9B D7 CA 36 EC 01 B5 9B 69 C8 A3 8C 0C EA 11 54 D7 56 E6 7F A1
00000114 37 80 50 63 58 56 56 CC 6C 77 39 AB 2D C7 B3 29 ED 14 86 A4 30 94 85
0000012B D2 FE 5D 67 FE 40 CC 23 31 04 13 B3 D3 43 35 C6 99 B0 86 7C B5 2E 0B
00000142 A7 D9 C2 91 78 A3 02 81 DE EE D5 17 30 D4 8F 39 13 91 CA BD 93 47 8C
00000159 44 A5 E0 D9 BE FB D3 6F A1 7C 26 BD 18 33 77 80 F6 99 62 CD A6 72 A3
00000170
Key Entry: Triple DES (ECB)
Enter the key using hexadecimal characters (0..9, A..F).
Key length: 128 bits (effectively 112 bits)
12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12
Encrypt
Decrypt
Cancel

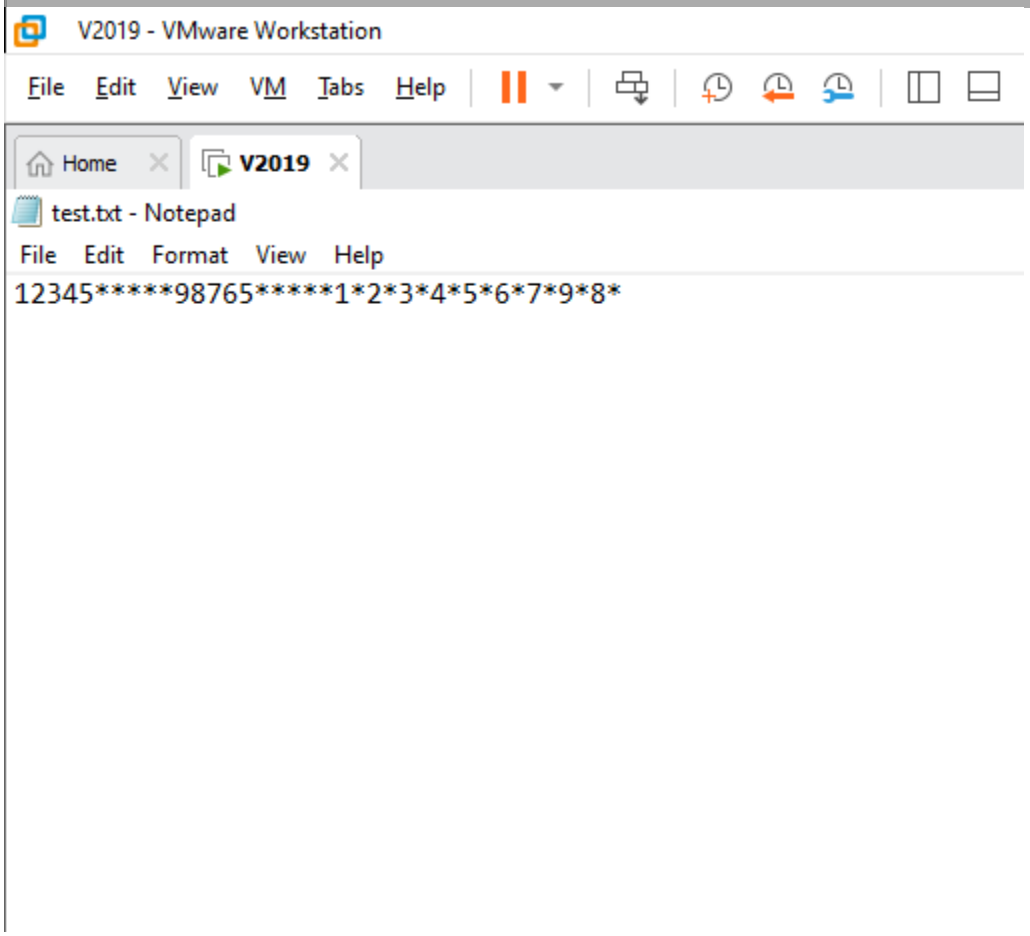


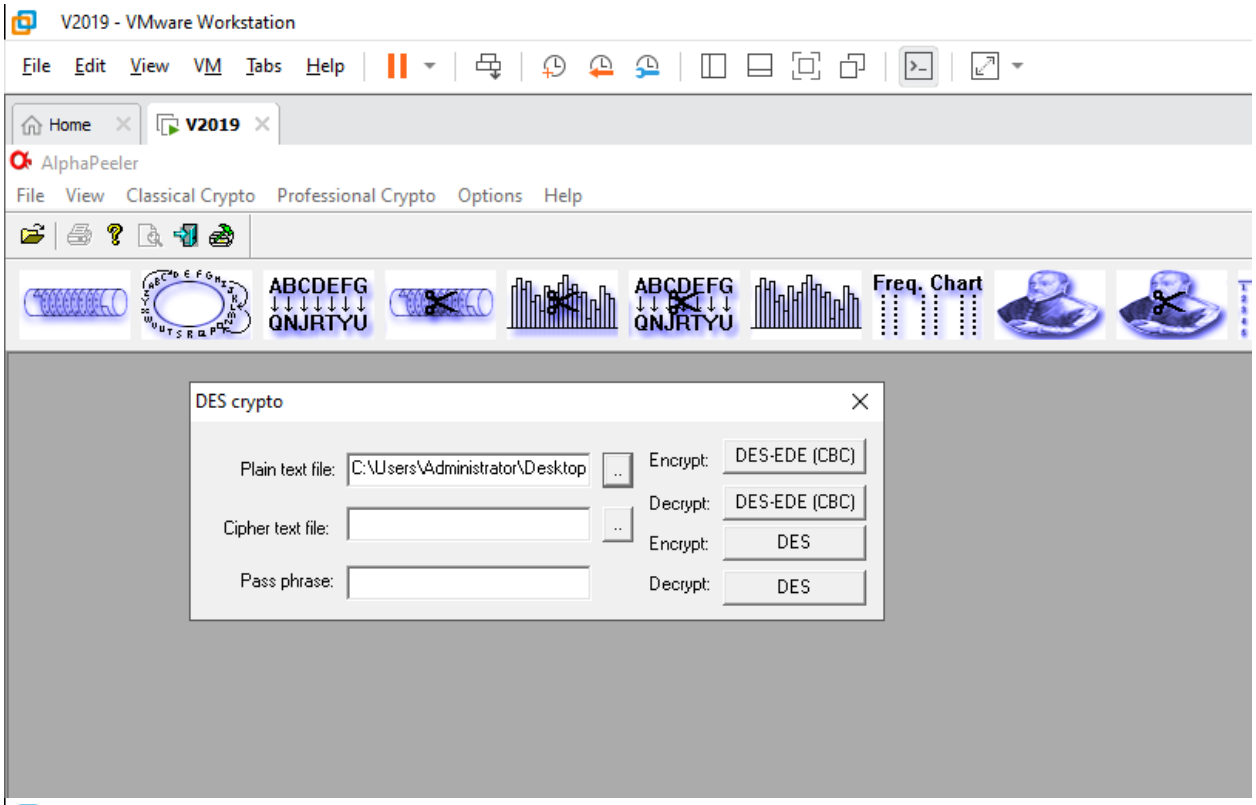
5.2 Perform Cryptanalysis using AlphaPeeler
- Open Windows 10

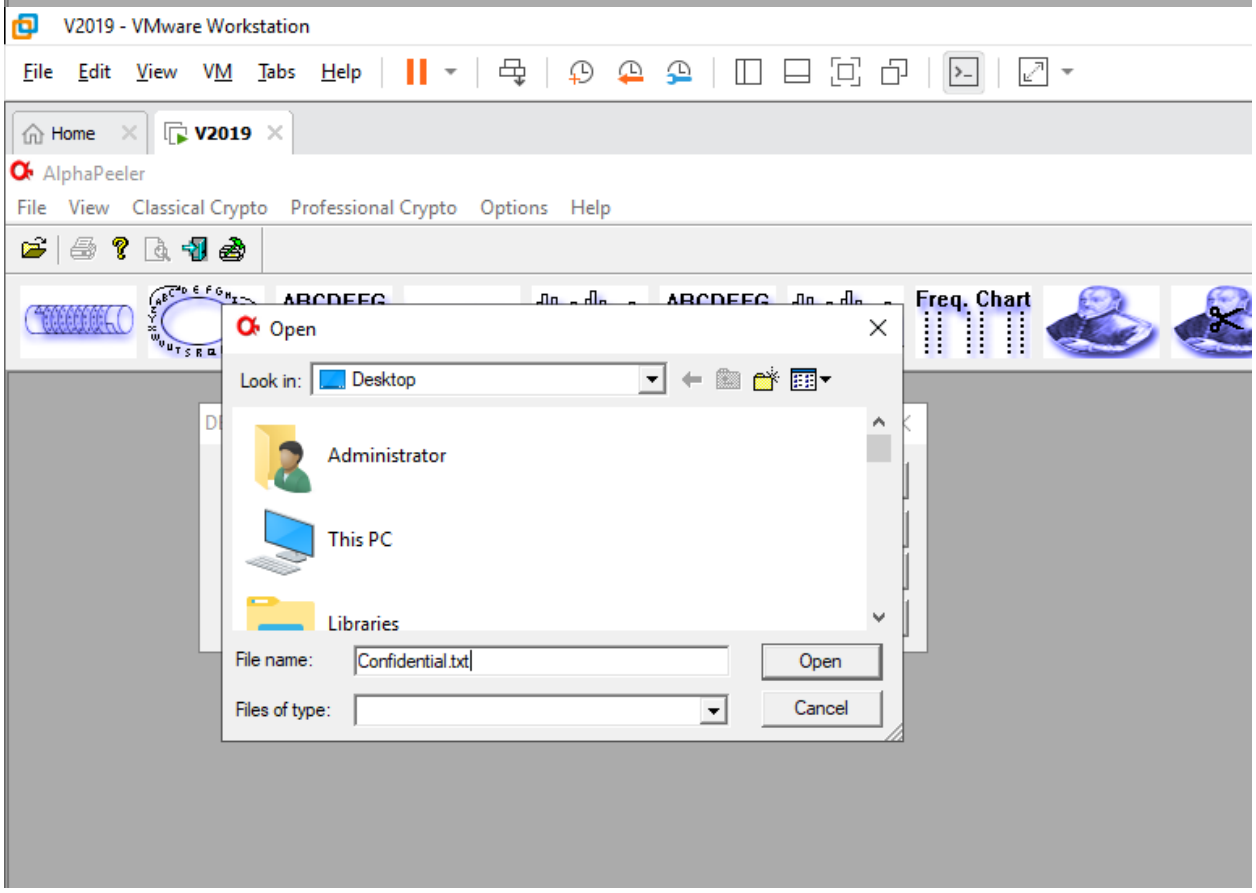

V2019 - VMware Workstation
File Edit View VM Tabs Help
Home
V2019
AlphaPeeler
File Home Share View
This PC › Desktop › CEHv11 Module 20 Cryptography › CEHv11 Module 20 Cryptography › Cryptanalysis Tools › AlphaPeeler
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name
Date modified
Type
Size
AlphaPeelerPro1.3wse
12/13/2019 2:19 PM
Application
44,540 KB

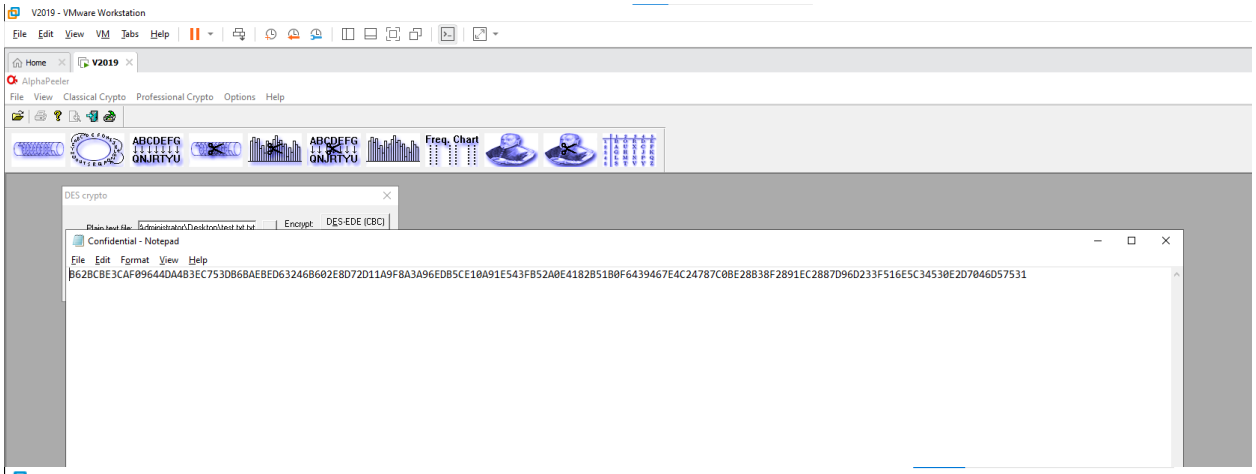

V2019 - VMware Workstation
File Edit View VM Tabs Help
Home
V2019
Manage
AlphaPeeler
File Home Share View Application Tools
This PC › Desktop › CEHv11 Module 20 Cryptography › CEHv11 Module 20 Cryptography
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Name
Date modified
Type
installation-files
10/28/2023 8:17 AM
File folder
AlphaPeelerPro1.3wse
12/13/2019 2:19 PM
Application
Recently added
AlphaPeeler
NumberShark
CrypTool
Expand
A
Acrobat Reader DC
AlphaPeeler Professional 1.3
New
Azure Data Studio
C
Chrome Apps
CrypTool
New
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer

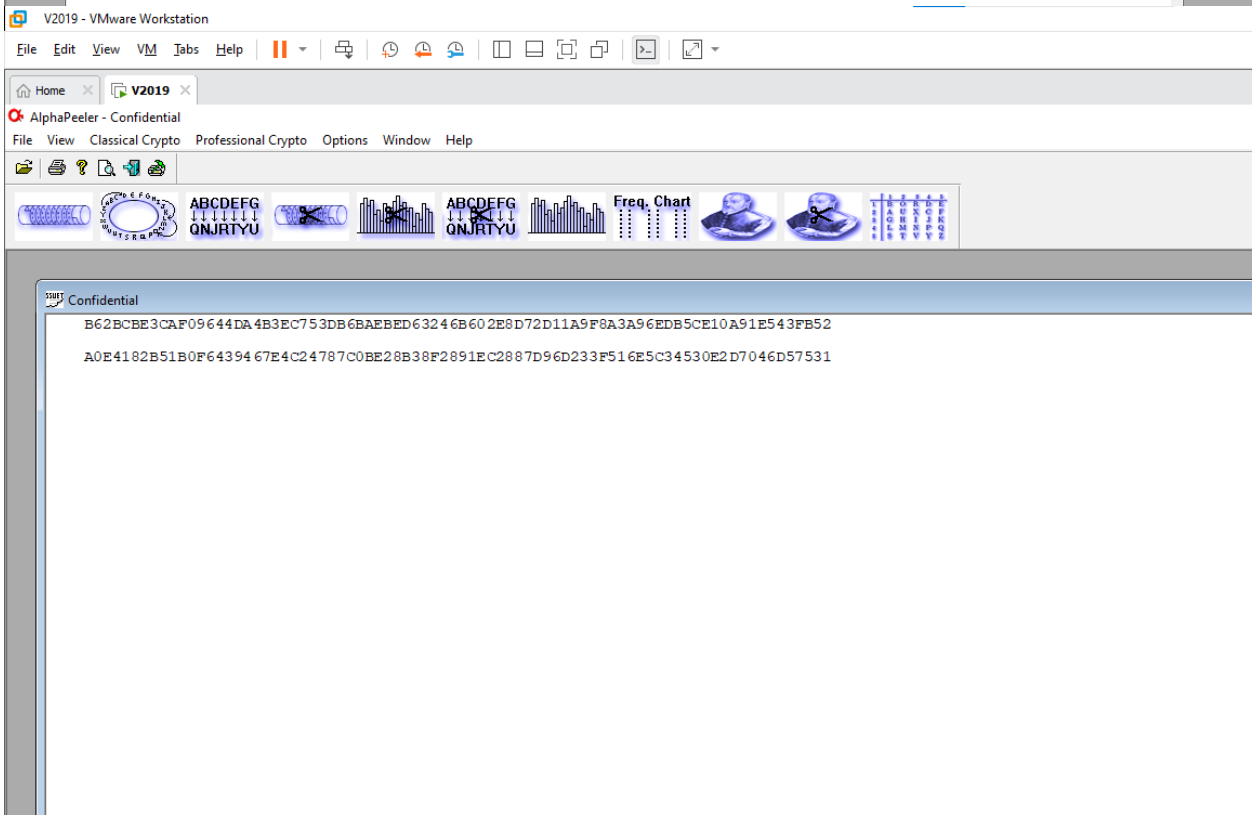

V2019 - VMware Workstation
File Edit View VM Tabs Help
Home
V2019
AlphaPeeler
File View Classical Crypto Professional Crypto Options Help
ABCDEFG
QNJRTYU
ABCDEFG
QNJRTYU
Freq. Chart

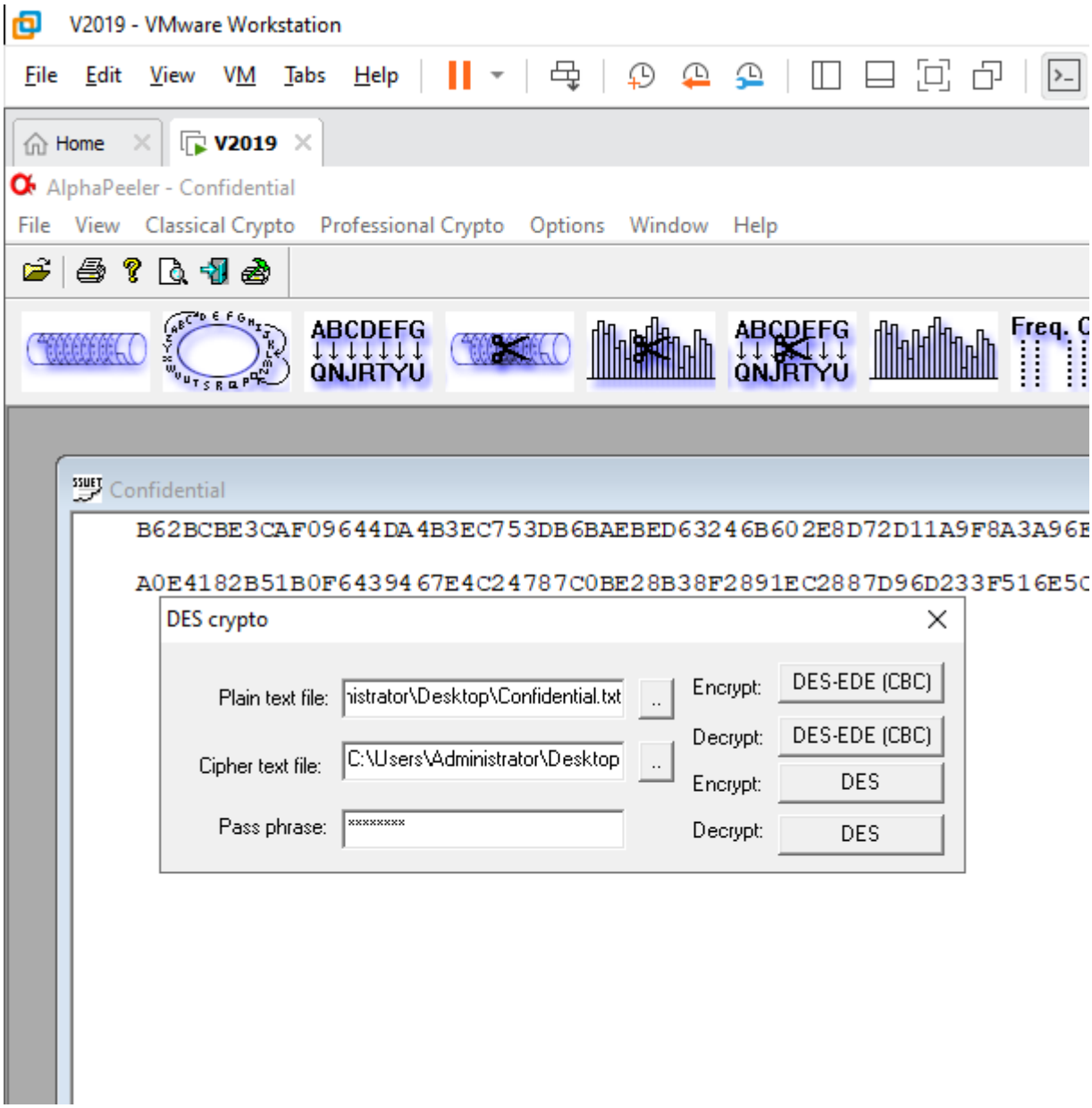

V2019 - VMware Workstation
File Edit View VM Tabs Help
Home
V2019
test.txt - Notepad
File Edit Format View Help
12345*****98765*****1*2*3*4*5*6*7*9*8*

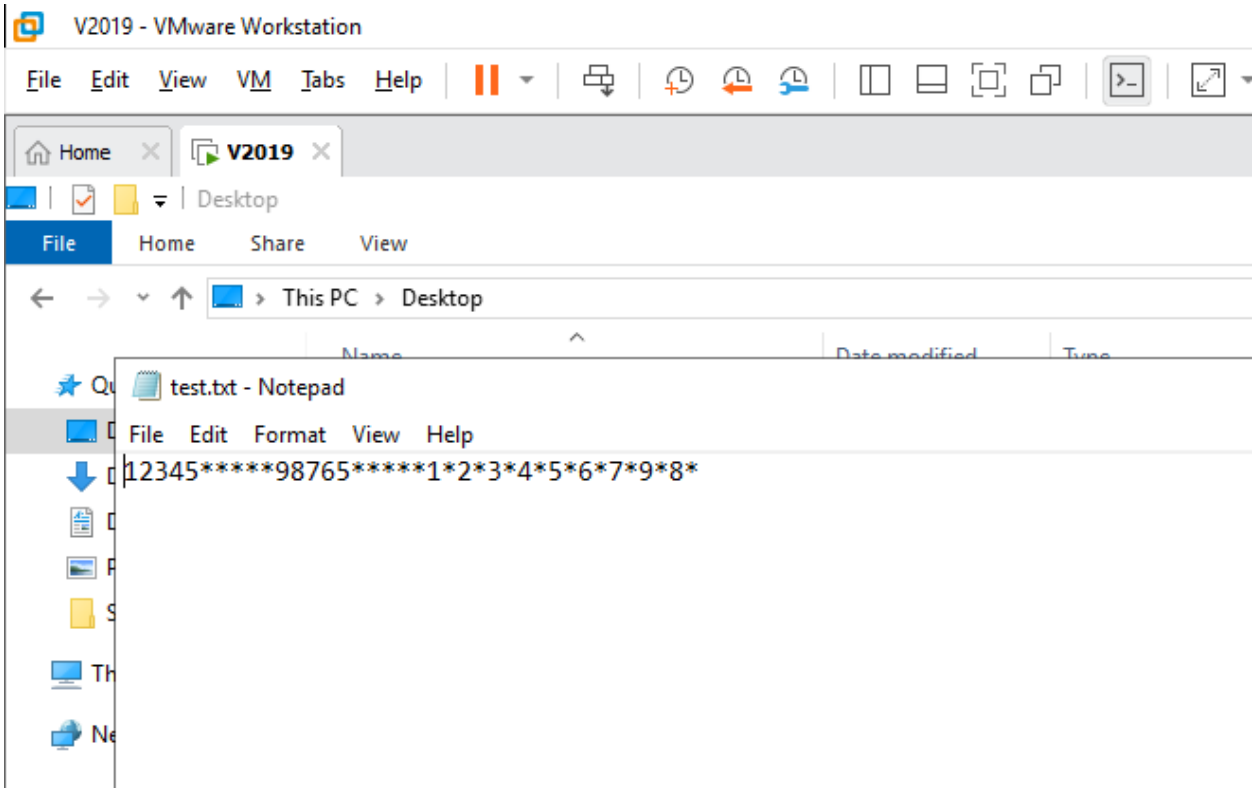

V2019 - VMware Workstation
File Edit View VM Tabs Help
Home
V2019
AlphaPeeler
File View Classical Crypto Professional Crypto Options Help
ABCDEFG
QNJRTYU
Freq. Chart
DES crypto
Plain text file:
C:\Users\Administrator\Desktop
Cipher text file:
Pass phrase:
Encrypt:
DES-EDE (CBC)
Decrypt:
DES-EDE (CBC)
Encrypt:
DES
Decrypt:
DES


V2019 - VMware Workstation
File Edit View VM Tabs Help
Home
V2019
AlphaPeeler
File View Classical Crypto Professional Crypto Options Help
Freq. Chart
Open
Look in:
Desktop
Administrator
This PC
Libraries
File name:
Confidential.txt
Open
Files of type:
Cancel


V2019 - VMware Workstation
File Edit View VM Tabs Help
Home
V2019
AlphaPeeler
File View Classical Crypto Professional Crypto Options Help
DES crypto
Encrypt
DES-EDE (CBC)
Confidential - Notepad
File Edit Format View Help
B62BCBE3CAF09644DA4B3EC753DB6BAEBED63246B602E8D72D11A9F8A3A96EDB5CE10A91E543FB52A0E4182B51B0F6439467E4C24787C0BE28B38F2891EC2887D96D233F516E5C34530E2D7046D57531


V2019 - VMware Workstation
File Edit View VM Tabs Help
Home
V2019
AlphaPeeler - Confidential
File View Classical Crypto Professional Crypto Options Window Help
Freq. Chart
Confidential
B62BCBE3CAF09644DA4B3EC753DB6BAEBED63246B602E8D72D11A9F8A3A96EDB5CE10A91E543FB52
A0E4182B51B0F6439467E4C24787C0BE28B38F2891EC2887D96D233F516E5C34530E2D7046D57531


V2019 - VMware Workstation
File Edit View VM Tabs Help
Home
V2019
AlphaPeeler - Confidential
File View Classical Crypto Professional Crypto Options Window Help
ABCDEFG
QNJRTYU
Confidential
B62BCBE3CAF09644DA4B3EC753DB6BAEBED63246B602E8D72D11A9F8A3A96E
A0E4182B51B0F64394 67E4C24787C0BE28B38F2891EC2887D96D233F516E5C
DES crypto
Plain text file:
istrator\Desktop\Confidential.txt
Cipher text file:
C:\Users\Administrator\Desktop
Pass phrase:
****
Encrypt:
DES-EDE (CBC)
Decrypt:
DES-EDE (CBC)
Encrypt:
DES
Decrypt:
DES


V2019 - VMware Workstation
File Edit View VM Tabs Help
Home
V2019
Desktop
File Home Share View
This PC › Desktop
test.txt - Notepad
File Edit Format View Help
12345*****98765*****1*2*3*4*5*6*7*9*8*