50.042 CTF Challenge 2023

Team RaisinGang

Jiang Hongbei	(1005870)
Joel Sng Kiat Loong	(1005968)
John-David Tan Ming Sheng	(1005971)
Kwok Keith	(1006344)
Jon Koo Jia Jun	(1006388)

Stage 1: Steganography

Contact Keith (@akyholicx) or Jon (@agxhv) for assistance if you face any issues! (or require hints :P)

What is Steganography?

Steganography is the art of hiding secret data amongst everyday materials such as files, text, images, audio, etc.

For example, this phrase “Secret exists cause Ryan enabled text!”.
It can be read plainly as a joke or even it can be read with the first letters of each word to form the hidden message “Secret”.

Steganography today is significantly more sophisticated, however. They allow users to hide large amounts of information within image and audio files. These forms of steganography often are used in conjunction with cryptography. Finding the information is often a difficult task.

A little more about the history Steganography (Skip if you wish)

Steganography has its roots in ancient civilisations. The earliest documented ones dated back to 440 BC, when a Greek ruler, Histiaeus, shaved the head of his most trusted slave and tattooed a secret message on his scalp (ouch!). After his hair regrew, the slave was then sent as a messenger to deliver a concealed message.

In World War II, Steganography played a significant role in espionage. Agents would hide messages in seemingly innocent documents or images using invisible inks, and microdots.

Today, you can observe a wide use of Steganography. Digital watermarking, copyright protection and data authentication are some examples. It has also been applied to bypass internet censorship and surveillance in some cases.

TODO #1:

You are a time traveller and you have brought your laptop with you. The year is 1941 and you are trying to apply for a job at Bletchley Park to become Britain's greatest Code Breaker. During the Second World War, The Nazis have been known to send hidden messages through their complex machinery, known as the Enigma Machine. Fortunately or unfortunately, due to some Time Paradoxes, the British Codebreakers at Bletchley Park have managed to lay their hands on some shiny new technology from 2023. They have been streaming this surprisingly high quality video over British National Television as a recruitment challenge (https://raisins.sytes.net/sutd/term5/cybersecurity/ctf/video.mp4)[1] and there seems to be something weird happening every few minutes. You suspect that there might be secret coded messages hidden in the video, but you are confident that your futuristic mind and devices will make this task a piece of cake. **The famous mathematician Alan Turing is hiring new code breakers and he wants you to listen carefully. . .**

Hint: stage2 file is encrypted: AES-CBC
IV = b'\x12\xad\xf8\x8f\xb3\x10\x02\x92.\x98\t@\x02&\xd2T'

[1] If you are connected to SUTD_WIFI, use http://10.16.222.209/sutd/term5/cybersecurity/ctf/video.mp4 (IP address subject to change due to DHCP, please contact @agxhv if you have trouble accessing this resource)