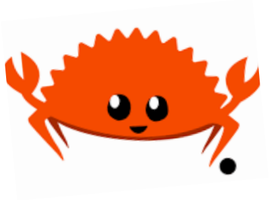
RANSOMWARE AND RUST



Topics Covered

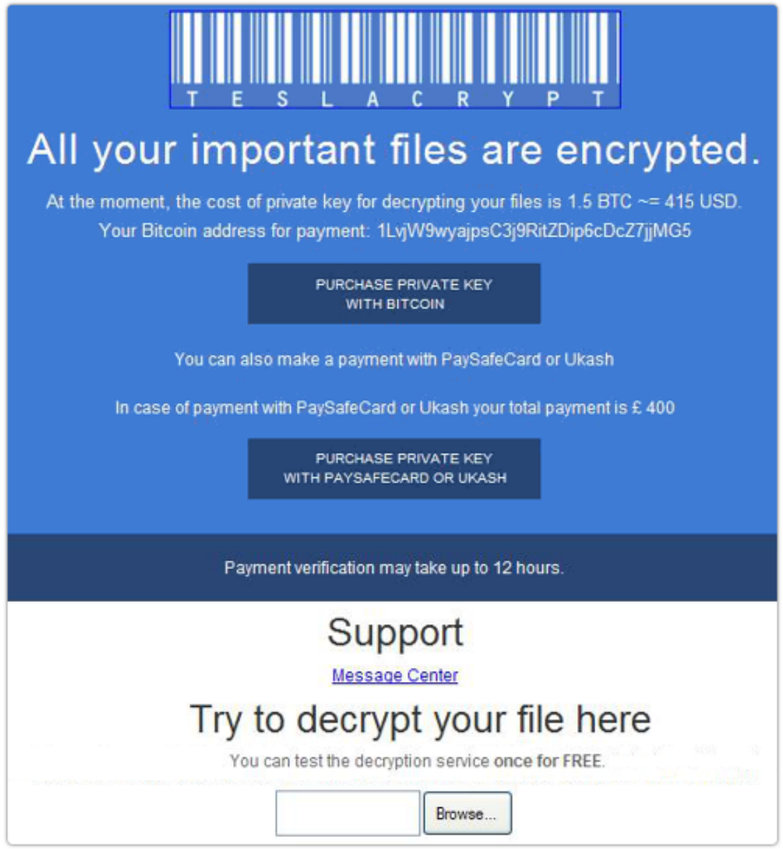
- Ransomware
- Working of Ransomware
- Cryptography
- Reverse Engineering
- Rust
- Why Rust?
- Rust Basics

Ransomware

- A malicious software designed to block access to the computer system or file.
- The attacker demands payment (ransom) in return to decrypt the files.
- Usually carried out using a Trojan.

Famous Ransomware Attacks

- WannaCry (Net loss: $4 billion)
- TeslaCrypt :- Targeted Gaming Files
- NotPetya (Net loss: $10 billion)
- Sodinokibi (Net loss: $200 million)
- Swissport:- Ransomware attack on Zurich Airport



Teslacrypt

Ransomware attack on Swissport causes delay at Zurich Airport

The security teams were quick to spot the attack and started restoring the firm's IT systems.

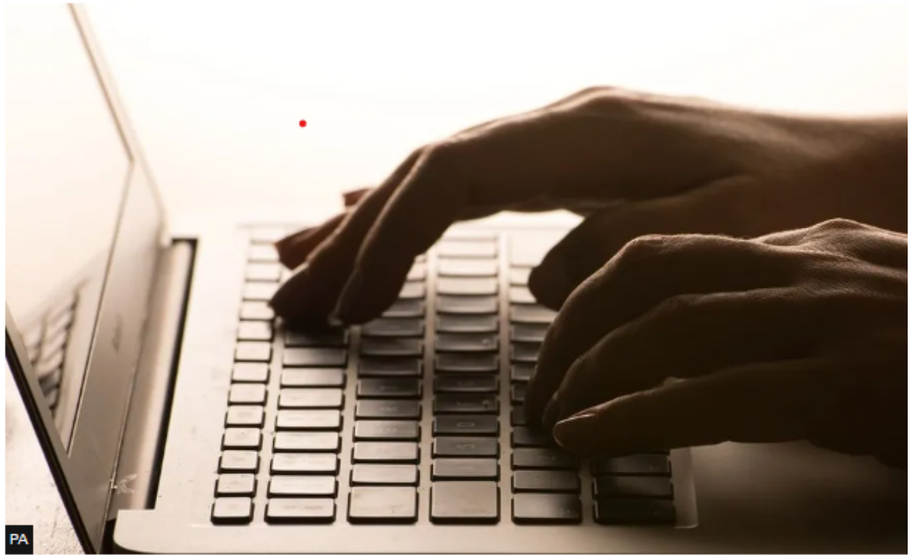
February 7, 2022

Share this article

Swissport is responsible for most of the operations at the airport, including check-in gates, airport security, baggage handling, aircraft fuelling, de-icing and lounge hospitality. Credit: Hansueli Krapf / Wikimedia.

UK and US blame Russia for 'malicious' NotPetya cyber-attack

15 February 2018



The Russian military was directly behind a "malicious" cyber-attack on Ukraine that spread globally last year, the US and Britain have said.

The White House said June's NotPetya ransomware attack caused billions of dollars in damage across Europe, Asia, and the Americas.

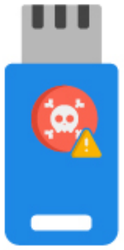
UK Defence Secretary Gavin Williamson said Russia was "ripping up the rule book" and the UK would respond.

Moscow denies being behind the attack, calling such claims "Russophobic".

How Ransomware works?

Malicious
Email Attachment

Infected Pen Drive



Malicious Website

01

User is infected
by ransomware

02

All data on the PC
and network is locked

03

Ransom demand to
unblock your data


Recycle Bin
@WanaDec...
Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/15/2017 19:18:09
Time Left
02:23:59:30
Your files will be lost on
5/19/2017 19:18:09
Time Left
06:23:59:30
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt
Search the web and Windows
Test Mode
Windows 10 Pro
Build 10240
7:18 PM
5/12/2017

Cryptography

There are two types of Encryption Methods

Symmetric Encryption

- Uses one key for encryption
- Fast Encryption
- Used on large amounts of data

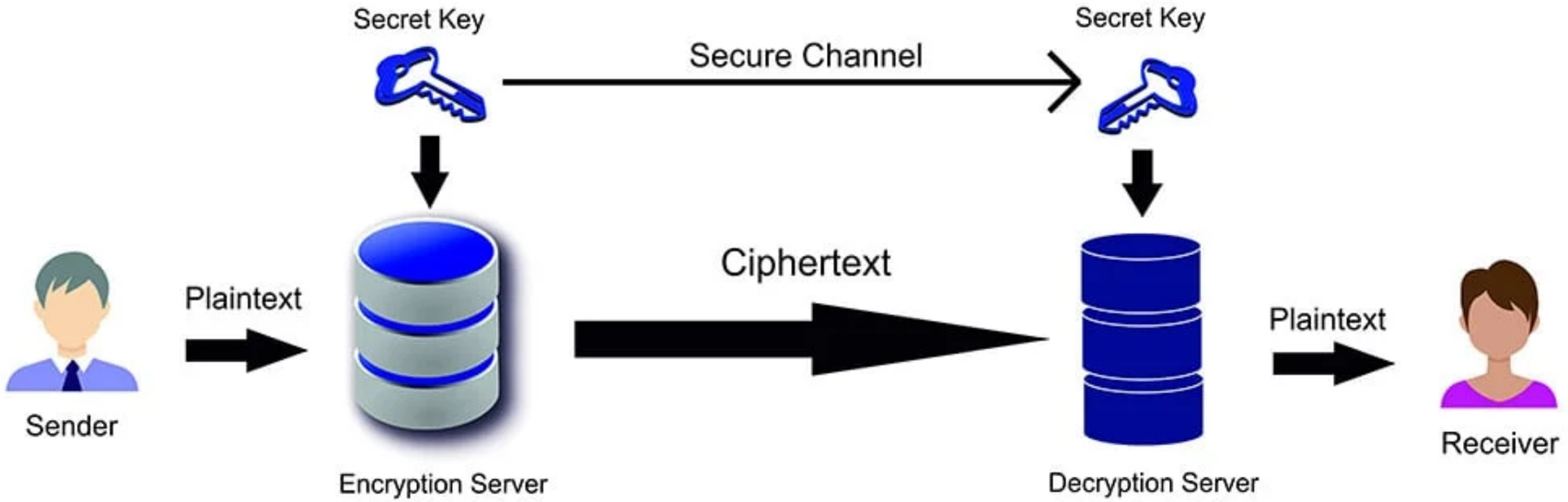
Asymmetric Encryption

- Uses two keys for encryption
- Slow Encryption
- Used on small amount of data

Cryptography

AES Encryption

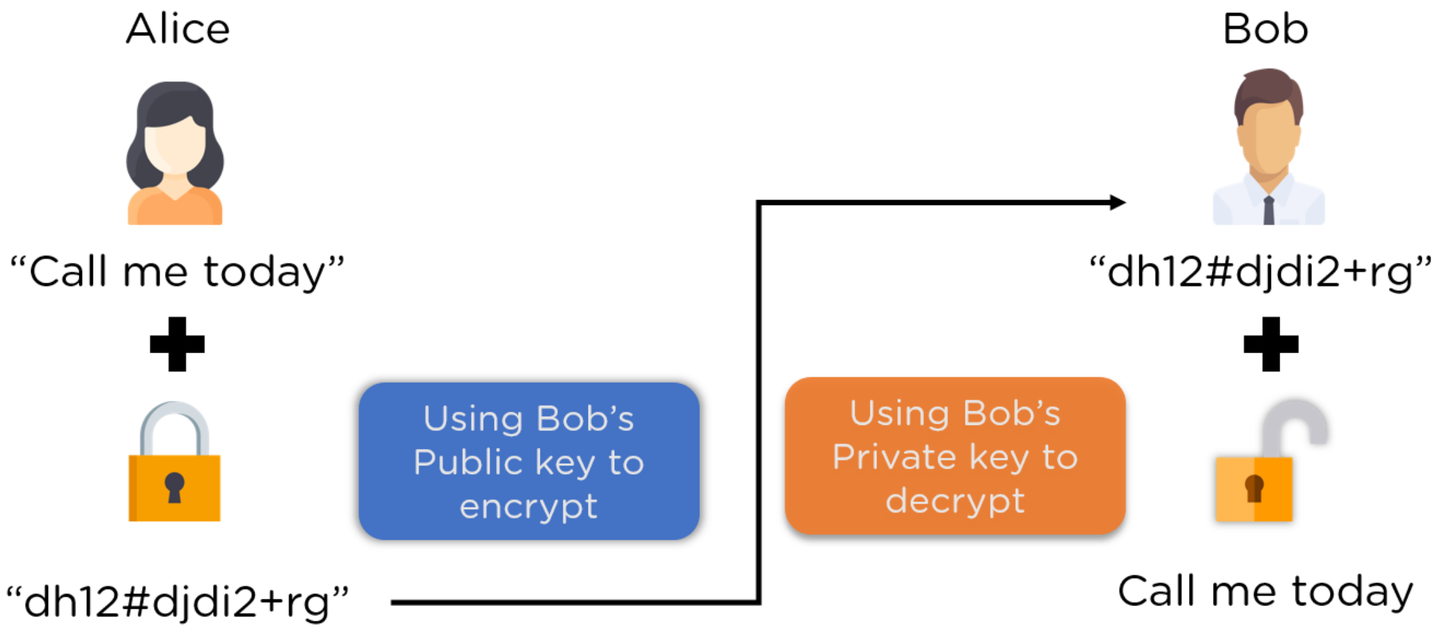
- Advanced Encryption Standard is a symmetric encryption algorithm.
- It uses one key for both encryption and decryption of data.

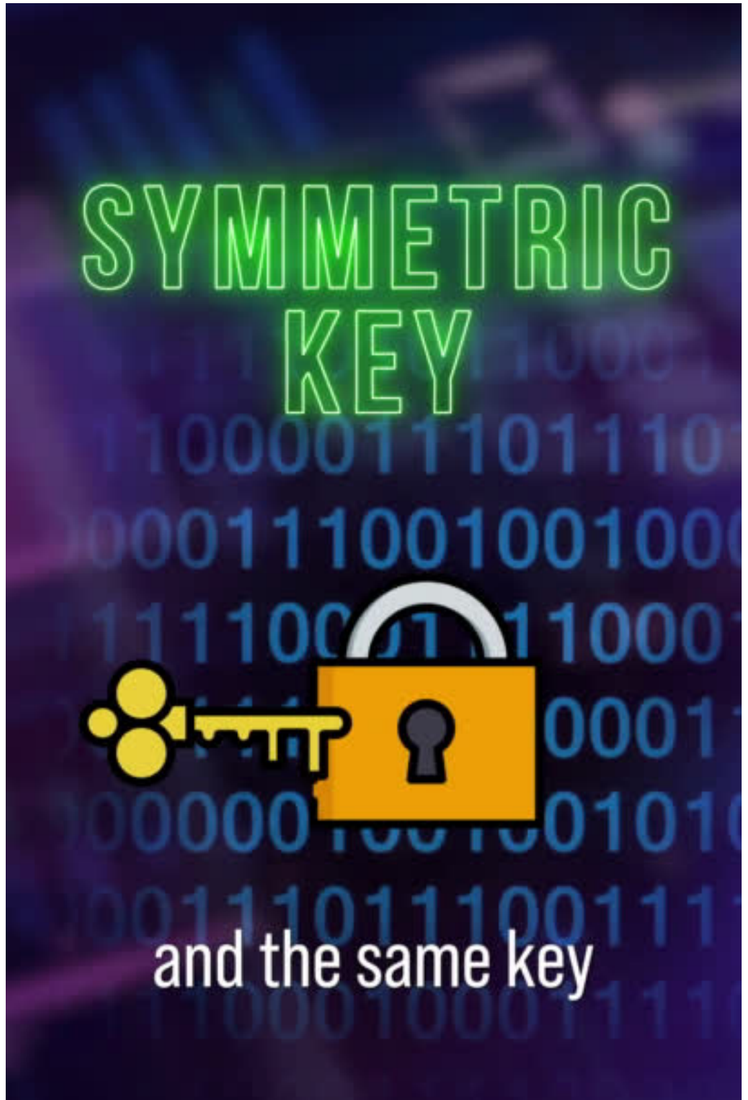


Cryptography

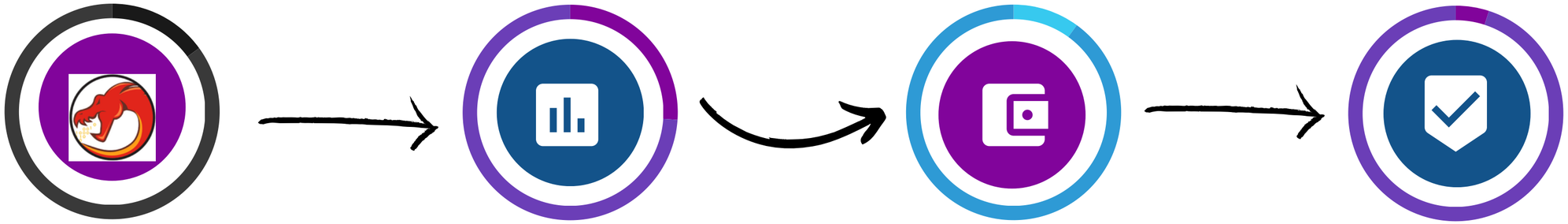
RSA Encryption

- RSA encryption is an asymmetric encryption algorithm.
- It uses two keys - **‘public and private’** to encrypt and decrypt data.




SYMMETRIC
KEY
and the same key

Reverse Engineering



Select a Decompiler

Analyze the code

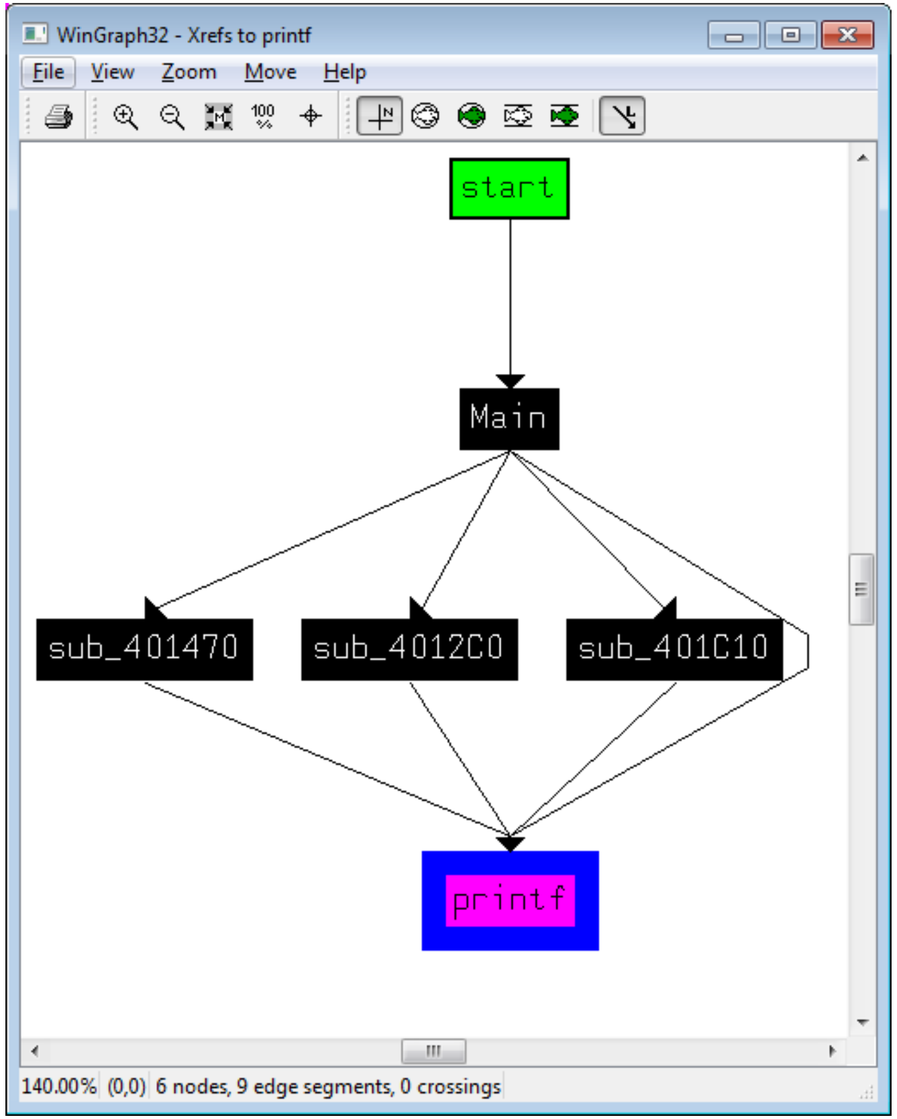
Observe its pattern in a virtual environment

Reverse Engineer the Program

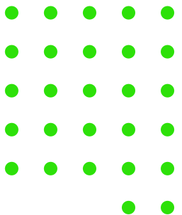
Decompile: FUN_08006d58 - (finder_plus.hex2)

```
1
2  void FUN_08006d58(void)
3
4  {
5    FUN_080031dc();
6    FUN_08002258();
7    do {
8    } while (*DAT_08006d84 == 0);
9    FUN_08008460(1);
10   do {
11     FUN_08008630();
12     FUN_0800852c();
13     FUN_080084a4();
14   } while( true );
15 }
16
```

Decompiled Code

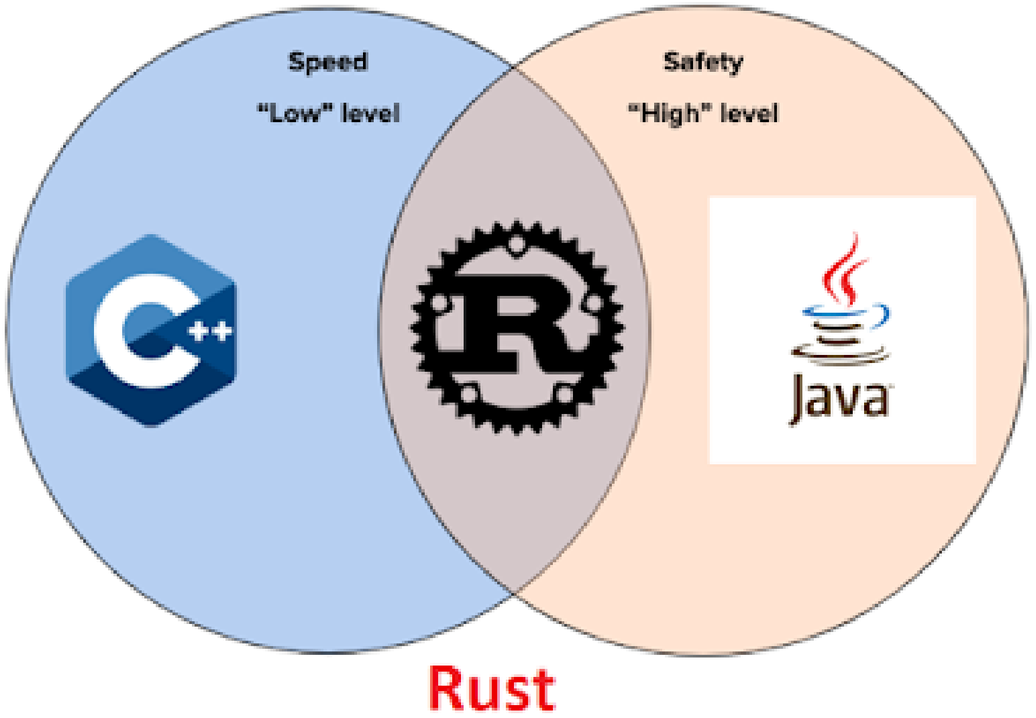


Function Call Graph



Rust

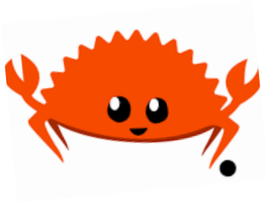
- Modern programming Language designed for **memory safety**.
- Gained popularity for addressing issues in **error handling** and **memory management**.
- Uses **Ownership and Borrowing Model** for Memory Management



Why Rust?

Reasons why Rust is difficult to decompile:

- Rust is a language designed to prevent errors
- Different versions of compilers generate different binary code
- Flexible library (crates) system.



Rust Basics

Variable Declaration and Data Types

```rust
fn main() {
    // Declare an immutable variable:
    let my_immutable_variable = 21;

    // Declare a mutable variable:
    let mut my_variable = 21;

    // Annotating a data type is optional:
    let my_var: u32 = 42;

    // Constants are different from variables:
    const MY_CONSTANT: u8 = 13;
}
```

Rust Basics

Function Declaration

- Like variable declaration, function declaration is also different in Rust.

```
fn func(x: u8, y: char, z: f32) -> bool {}
```

- `fn` — Used to declare a function
- `func` — Name of function
- `(x: u8, y: char, z: f32)` — Parameters of function
- `-> bool` — Return type of function

Rust Basics

File I/O

fs::File::open(path)- Opens a file

fs::read(path)- Reads the file at path ‘path’

io::Write::write- Writes into a file

drop(file)- Closes the opened file

Let's jump into the code!