**Fayoum University**

**Engineering Faculty**

**Electrical Engineering Department**

**B. Eng. Final Year Project**

**Secure Communication Network**

**By:**

**Ahmed Abdulla Mourad**

**Ahmed Mohamed Eid**

**Mohamed Shaban El-sayed**

**Moaz Mohamed Radwan**

**Supervised By:**

**Dr: Mohamed Hamdy**

[1. Introduction to Network Security 2](#_Toc200909646)

[2. Project Overview 2](#_Toc200909647)

[3. Hardware Components 3](#_Toc200909648)

[3.1 RASPBERRY PI (THE MAIN ECU) 3](#_Toc200909649)

[3.2 TOUCH SCREEN 3](#_Toc200909650)

[3.3 TRANCEIVER 3](#_Toc200909651)

[3.4 MICK 3](#_Toc200909652)

[3.5 SPEAKER 3](#_Toc200909653)

[4. Encryption and Security Protocols 3](#_Toc200909654)

[4.1 Introduction to Cryptographic Principles 3](#_Toc200909655)

[4.2 System Security Requirements 5](#_Toc200909656)

[4.3 Hybrid Encryption Design 8](#_Toc200909657)

[4.4 Implementation of Hybrid Encryption with OpenSSL 11](#_Toc200909658)

[4.5 Integration with Other Modules 14](#_Toc200909659)

[4.6 Summery 14](#_Toc200909660)

# Introduction to Network Security

# Project Overview

# Hardware Components

## 3.1 RASPBERRY PI (THE MAIN ECU)

* + 1. **INTRODUCTION :**

In this chapter, we’ll talk about the main ECU in our project which is Raspberry pi. Also, we’ll discuss why Raspberry pi, its Versions, Hardware Component, Interfacing with GPIO pins and Raspberry pi Operating System. The Raspberry Pi is a low-cost, credit card-sized computer that was first developed in 2012 by the Raspberry Pi Foundation in the UK. The primary goal of the Raspberry Pi was to promote the teaching of basic computer science in schools and developing countries. Initially, the Raspberry Pi was equipped with a 700 MHz ARM11 processor, 256 MB of RAM, and a single USB port. However, today's models have significantly evolved, featuring quad-core processors, up to 8GB of RAM, and multiple USB and HDMI ports. The versatility of the Raspberry Pi extends to its ability to run a variety of operating systems, including several Linux distributions, Windows 10 IoT Core, and even Android. This flexibility allows the Raspberry Pi to be used for a wide range of projects, from simple tasks such as web browsing and playing games, to more complex endeavors like controlling robots, automating homes, and even building supercomputers. Overall, the Raspberry Pi has become an incredibly versatile and powerful tool for anyone interested in computing and electronics.

* + 1. **Raspberry Pi 4 in Our Project:**

For our project, we utilized the Raspberry Pi 4, which offers a significant improvement in speed and performance compared to its predecessors. The Raspberry Pi 4 provides a complete desktop experience, making it suitable for tasks such as editing documents, browsing the web with multiple tabs, managing spreadsheets, and drafting presentations. This is achieved on a smaller, more energy-efficient, and cost-effective machine.

**3.1.3 Key Features of Raspberry Pi 4:**

1. Silent and Energy-Efficient:

The Raspberry Pi 4 operates silently without a fan and consumes significantly less power than traditional computers.

1. Fast Networking:

Equipped with Gigabit Ethernet, onboard wireless networking, and Bluetooth, the Raspberry Pi 4 ensures fast and reliable connectivity.

1. SPI communication protocol

SPI communication protocol is a must to connect the screen with raspberry pi and transceiver with raspberry pi also

1. USB 3.0:

The device includes two USB 3.0 ports, in addition to two USB 2.0 ports, allowing data transfer rates up to ten times faster than previous models.

1. Choice of RAM:

The Raspberry Pi 4 is available in different configurations, offering 1GB, 2GB, 4GB, or 8GB of RAM to meet various performance needs. These features make the Raspberry Pi 4 an excellent choice for a wide range of applications, from simple computing tasks to more complex projects involving robotics and automation.

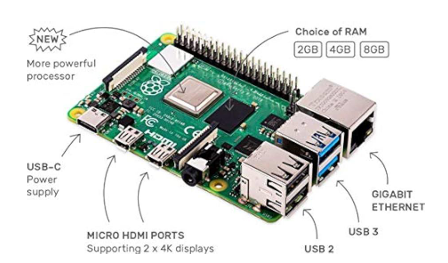


Figure 3‑1-1: Raspberry Pi ECU

* + 1. **WHY CHOOSE RASPBERRY PI**

The Raspberry Pi offers numerous advantages that make it a popular choice for a wide array of projects and applications. Here are some reasons why the Raspberry Pi is an excellent option:

1. Cost-Effective:

The Raspberry Pi is an affordable computer, making it accessible for beginners and ideal for projects with budget constraints.

1. Compact Size:

Its small and lightweight design allows for easy portability and the ability to fit into tight spaces.

Energy Efficient: The Raspberry Pi consumes very little power, making it an environmentally friendly and cost-effective choice.

1. Versatility:

Capable of running various operating systems and applications, the Raspberry Pi is suitable for a broad range of projects.

1. GPIO Pins:

The General-Purpose Input/Output (GPIO) pins make it easy to connect a wide variety of devices, facilitating custom electronics projects.

1. Community Support:

A large, active community of users and developers shares knowledge and resources, making it easy to find help and solutions to problems.

1. Educational Value:

Originally designed to promote the teaching of basic computer science, the Raspberry Pi is an excellent educational tool for learning about computing and electronics.

Overall, the Raspberry Pi is a cost-effective, flexible, and versatile tool that is suitable for a wide range of projects and applications. Its popularity extends to hobbyists, students, and professionals alike, making it a go-to choice for many.

* + 1. **VERSIONS OF RASPBERRY PI**

The Raspberry Pi has seen numerous iterations since its initial release in 2012, each version bringing improvements in processing power, memory, and connectivity options. Here’s a breakdown of the major versions of the Raspberry Pi:

1. Raspberry Pi Model B (2012)

• Processor: 700 MHz ARM11

• RAM: 256 MB (later upgraded to 512 MB)

• Ports: 1 USB port, HDMI, RCA video, 3.5mm audio jack

• Features: The original Raspberry Pi was designed as a basic, affordable computer for educational purposes, promoting computer science in schools and developing countries.

2. Raspberry Pi Model A (2013)

• Processor: 700 MHz ARM11

• RAM: 256 MB

• Ports: 1 USB port, HDMI, RCA video, 3.5mm audio jack

• Features: A lower-cost version of the Model B, with reduced USB ports and no Ethernet port, aimed at more cost-sensitive applications.

3. Raspberry Pi Model B+ (2014)

• Processor: 700 MHz ARM11

• RAM: 512 MB

• Ports: 4 USB ports, HDMI, RCA video, 3.5mm audio jack, Ethernet port

• Features: Improved power consumption, increased GPIO pins, and better audio quality. 18

4. Raspberry Pi 2 Model B (2015)

• Processor: 900 MHz quad-core ARM Cortex-A7

• RAM: 1 GB

• Ports: 4 USB ports, HDMI, Ethernet, 3.5mm audio jack

• Features: Significant performance improvement with a quad-core processor and increased RAM, making it suitable for more demanding applications.

5. Raspberry Pi Zero (2015)

• Processor: 1 GHz single-core ARM11

• RAM: 512 MB

• Ports: Mini HDMI, 1 USB OTG port

• Features: Ultra-small form factor and very low cost, designed for embedded applications.

6. Raspberry Pi 3 Model B (2016)

• Processor: 1.2 GHz quad-core ARM Cortex-A53

• RAM: 1 GB

• Ports: 4 USB ports, HDMI, Ethernet, 3.5mm audio jack, Wi-Fi, Bluetooth • Features: Built-in Wi-Fi and Bluetooth, making it more suitable for IoT applications.

7. Raspberry Pi 3 Model B+ (2018)

• Processor: 1.4 GHz quad-core ARM Cortex-A53

• RAM: 1 GB

• Ports: 4 USB ports, HDMI, Ethernet, 3.5mm audio jack, Wi-Fi, Bluetooth 19

• Features: Improved network speeds and thermal performance, enhanced power management.

8. Raspberry Pi 4 Model B (2019)

• Processor: 1.5 GHz quad-core ARM Cortex-A72

• RAM: 2GB, 4GB, or 8GB

• Ports: 2 USB 3.0 ports, 2 USB 2.0 ports, 2 micro-HDMI ports, Ethernet, 3.5mm audio jack, Wi-Fi, Bluetooth

• Features: Major upgrade with more RAM options, dual monitor support, and significantly improved CPU and GPU performance. This model is capable of providing a complete desktop experience.

9. Raspberry Pi 400 (2020)

• Processor: 1.8 GHz quad-core ARM Cortex-A72

• RAM: 4GB

• Ports: 3 USB ports, micro-HDMI ports, Ethernet, 3.5mm audio jack, Wi-Fi, Bluetooth

• Features: Integrated into a compact keyboard, making it a convenient all-in-one computer.

10. Raspberry Pi Pico (2021)

• Processor: Dual-core ARM Cortex-M0+

• RAM: 264 KB SRAM

• Ports: GPIO pins

• Features: A microcontroller rather than a full computer, designed for embedded applications, and programmable with C/C++ or Micro Python. Figure 3-2 Provides a summary of Raspberry Pi versions timeline.

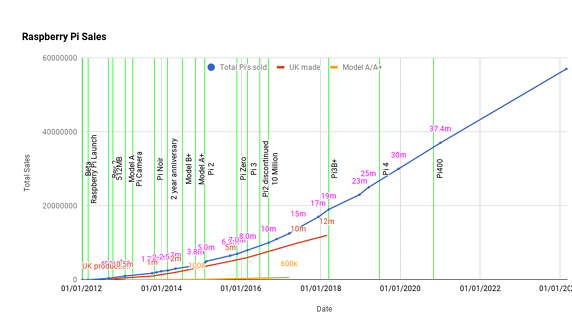


Figure 3‑1-2: Raspberry Pi versions timeline

**3.1.5 RASPBERRY PI HARDWARE**

Overview:

In this section, we will discuss the hardware aspects of the Raspberry Pi 4, including its specifications, pin diagram, and descriptions. We will also cover the layout and interfacing of GPIO pins, as well as the various hardware components used in the Raspberry Pi.

Hardware Components of Raspberry Pi

The hardware components of the Raspberry Pi include:

1. CPU/GPU:

The ARM Cortex-A72 CPU and VideoCore VI GPU provide the processing power and graphical capabilities.

1. RAM:

Depending on the model, the Raspberry Pi 4 can have 2GB, 4GB, or 8GB of RAM.

Networking:

Integrated Gigabit Ethernet, Wi-Fi, and Bluetooth enable robust connectivity options. 21

1. USB Ports:

USB 3.0 and USB 2.0 ports for connecting peripherals and storage devices.

HDMI Ports:

Dual micro-HDMI ports allow for dual monitor setups with up to 4K resolution.

Power Supply:

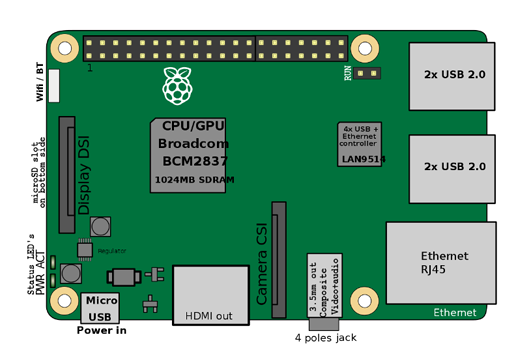
The USB-C power supply ensures sufficient power for all components and peripherals.

Figure 3‑1-3: Raspberry Pi hardware components

Figure 3-1-3 explain the position of each component, these components work together to provide a versatile and powerful computing platform suitable for a wide range of applications, from basic computing tasks to complex electronics projects and automation systems.

**3.1.4 Raspberry Pi 4 Specifications**

The Raspberry Pi 4 represents a significant upgrade over previous models, offering enhanced performance and connectivity options. Here are some key specifications:

1. Processor:

1.5 GHz quad-core ARM Cortex-A72

1. RAM:

Options of 2GB, 4GB, and 8GB

1. Networking:

Gigabit Ethernet, Wi-Fi 802.11ac, Bluetooth 5.0 22

USB Ports:

2 USB 3.0 ports and 2 USB 2.0 ports

1. Video Output:

2 micro-HDMI ports supporting up to 4K resolution

1. Storage:

MicroSD card slot for storage and operating system

1. Power:

USB-C power supply

**3.1.6 Layout and Interfacing of GPIO Pins**

The pin diagram of the Raspberry Pi 4 includes 40 GPIO pins, which can be used for various purposes such as digital input/output, PWM, I2C, SPI, and UART.

The GPIO (General Purpose Input/Output) pins on the Raspberry Pi 4 are a key feature that allows users to interface with a wide range of sensors, actuators, and other electronic components. The GPIO header consists of 40 pins, arranged in a 2x20 grid, each with specific functions:

• Power Pins: Provide 3.3V and 5V power to connected devices.

• Ground Pins: Common ground for all connected devices.

• GPIO Pins: Configurable pins that can be used for digital input/output.

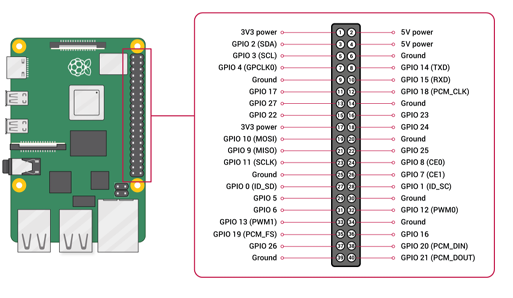
• Special Function Pins: Dedicated pins for communication protocols like I2C, SPI, and UART.

Figure3-1-4: Raspberry Pi Pin Diagram

**3.1.6 RASPBERRY PI OS**

Overview

Raspberry Pi OS, formerly known as Raspbian, is the official operating system for the Raspberry Pi. It is a free and open-source OS based on the Debian Linux distribution, specifically optimized for the Raspberry Pi hardware. Raspberry Pi OS comes pre-installed with a variety of software to help users get started with their projects.

Key Features and Components

1. Desktop Environment

• Description: Raspberry Pi OS features a desktop environment based on the Lightweight X11 Desktop Environment (LXDE), which is optimized for the Raspberry Pi's hardware.

• Benefit: Provides a familiar and user-friendly interface for performing various tasks such as browsing the web, editing documents, and managing files.

1. Pre-installed Software

• Description: The OS includes a variety of pre-installed software, such

Chromium Web Browser

Useful for testing web interfaces, accessing documentation, and downloading libraries or tools directly on the Raspberry Pi.

Terminal (LXTerminal)

Allows you to compile, run, and debug your C code.

Useful for managing network connections and running system commands.

Thonny Python IDE

Even though your main project is in C, you can use Thonny for quick scripts (e.g., testing communication protocols, simulating server/client behavior).

VNC Viewer and Remote Desktop Tools

Useful for remotely accessing and demonstrating your GUI interface on the Raspberry Pi screen.

Geany Text Editor

Lightweight editor for writing and editing your C driver files and configuration scripts.

File Manager

Allows you to organize your project files, move data, and manage dependencies easily without command line.

Bluetooth Manager

Can be used if your secure terminal includes Bluetooth communication.

Wi-Fi Configuration Tool

Helps set up and test network connectivity, which is essential for secure communication features.

raspi-config Tool

Used to enable SPI interface (required for ILI9341 and XPT2046), SSH access, and other hardware configurations.

Pre-installed Compilers and Build Tools (gcc, make)

Essential for compiling your C drivers and building your project.

1. Package Manager

• Description: The APT package manager is included, which allows users to install new software packages and keep the system up to date.

• Benefit: Ensures that users can easily extend the functionality of their Raspberry Pi and maintain security and performance updates.

1. GPIO Support

• Description: Raspberry Pi OS supports the GPIO (General Purpose Input/Output) pins on the Raspberry Pi, allowing users to interface with external hardware and sensors.

• Benefit: Facilitates hardware projects, such as robotics and home automation, by providing direct access to the GPIO pins for programming and control.

Conclusion Overall, Raspberry Pi OS is a powerful and flexible operating system tailored for the Raspberry Pi hardware. It is an excellent choice for a wide range of projects, from building a media centre to creating a home automation system. The OS's combination of a user-friendly desktop environment, pre-installed software, and robust configuration tools makes it ideal for both beginners and advanced users.

## TOUCH SCREEN

**(a-Si TFT LCD Single Chip Driver 240RGBx320 Resolution and 262K color)**

**3.2.1 Introduction to the ILI9341 Display Driver**

The ILI9341 is a sophisticated 262,144-color single-chip System-on-Chip (SoC) driver meticulously engineered for a-Si (amorphous silicon) TFT liquid crystal displays. It is designed to manage displays with a resolution of 240RGBx320 dots, integrating crucial display functionalities directly onto a single die. This integration includes a 720-channel source driver, a 320-channel gate driver, and a substantial 172,800 bytes of Graphics RAM (GRAM) dedicated to storing display data for the 240RGBx320 dot resolution. This on-chip memory is a key differentiator, as it eliminates the need for external display RAM, simplifying system design and reducing overall component count. The ILI9341's comprehensive feature set, encompassing flexible interface options, robust power management, and advanced display control, positions it as an ideal solution for a diverse range of portable electronic products. These include, but are not limited to, digital cellular phones, smartphones, MP3 players, and Portable Multimedia Players (PMPs), where optimizing battery life and delivering vibrant visual experiences are paramount considerations.

**3.2.2 Key Features and Architectural Overview**

The ILI9341's design is characterized by a rich array of features and a well-defined internal architecture that collectively enable its high performance and versatility:

1. 3.2.2.1 Display Capabilities

* **Resolution and Color Depth**: The driver natively supports a display resolution of 240 horizontal RGB dots by 320 vertical dots. It can render up to 262,144 full colors, offering a rich visual experience. A "reduce color mode" (8-color) is also available, specifically optimized for "Idle Mode ON" to conserve power when full color fidelity is not required.
* **On-chip Display RAM (GRAM)**: A significant 172,800 bytes of GRAM are embedded within the chip, providing ample space for storing 240RGBx320 dots of graphic display data. This integrated memory is crucial for enabling the "window address function," which allows for selective updating of specified moving picture areas within the GRAM. This functionality facilitates the simultaneous display of dynamic content alongside static images without needing to refresh the entire screen, thereby improving efficiency and responsiveness.

1. System Interface Options

The ILI9341 offers extensive compatibility with various host controllers through multiple system interfaces:

* **MCU Parallel Interfaces**: It provides support for 8-bit, 9-bit, 16-bit, and 18-bit data bus interfaces, compatible with both 8080-I and 8080-II series Microcontroller Units (MCUs). This broad compatibility allows for seamless integration into diverse embedded systems.
* **RGB Interfaces**: For applications requiring direct display rendering from graphics controllers, the ILI9341 supports 6-bit, 16-bit, and 18-bit data bus RGB interfaces. This is particularly beneficial for displaying high-frame-rate content.
* **Serial Peripheral Interface (SPI)**: For reduced pin count and simplified wiring, 3-line and 4-line serial interfaces are available.

1. Power Management and On-Chip Functionality

The driver is designed with a strong emphasis on power efficiency, crucial for portable devices:

* **Power Saving Modes**: It includes "Sleep Mode" and "Deep Standby Mode" to minimize power consumption when the display is not actively being used.
* **Voltage Requirements**: The I/O interface operates from 1.65V to 3.3V, while the analog supply voltage (VCI) ranges from 2.5V to 3.3V. An incorporated voltage follower circuit efficiently generates the necessary voltage levels for driving the LCD panel.
* **Integrated Circuits**: Key functional blocks integrated on the chip include:
  + **VCOM Generator and Adjustment**: Generates and fine-tunes the common electrode voltage (VCOM).
  + **Timing Generator**: Produces all essential timing signals for display operation and GRAM access.
  + **Oscillator**: An on-chip RC oscillator provides a stable output frequency for internal operations.
  + **DC/DC Converter**: Generates the various voltage levels (GVDD, VGH, VGL) required for TFT LCD panel driving.
  + **Line/Frame Inversion**: Supports inversion techniques to prevent image sticking and improve display uniformity.
  + **Gamma Correction**: Features a preset Gamma curve with separate RGB Gamma correction capabilities for accurate color reproduction.
  + **Content Adaptive Brightness Control (CABC)**: Dynamically adjusts display brightness based on image content, further enhancing power efficiency.

1. Panel Driver Circuitry

The core of the display driving capability resides in its integrated panel driver circuits:

* **Source Driver**: Comprises 720 output channels (S1 to S720).
* **Gate Driver**: Consists of 320 output channels (G1 to G320).
* **VCOM Signal**: Provides the common electrode signal for the TFT display.

1. Detailed MCU and RGB Interface Functionality

The ILI9341's versatile interface options are crucial for its broad applicability.

**3.2.3.1 MCU Interfaces**

The driver offers both parallel and serial interfaces to communicate with a host MCU. The selection between these modes and their specific configurations is determined by the external IM[3:0] pins.

**3.2.3.1.1 8080-I and 8080-II Series Parallel Interfaces**

The ILI9341 supports 8-, 9-, 16-, and 18-bit data bus configurations for both 8080-I and 8080-II series MCUs.

* **Signal Lines**: Common control signals include:
  + **CSX (Chip Select)**: Active low, used to enable or disable the ILI9341 chip.
  + **RESX (Reset)**: Active low, an external reset signal.
  + **WRX (Write Strobe)**: Data is latched on the rising edge of this signal.
  + **RDX (Read Strobe)**: Used for reading data from the driver, with data being read by the MCU on its rising edge.
  + **D/CX (Data/Command Select)**: A crucial signal that determines whether the data on the D[17:0] bus is a command (D/CX = '0') or display RAM data/command parameters (D/CX = '1').
* **Data Bus**: The D[17:0] pins serve as the bi-directional parallel data bus.
* **Write Cycle Sequence**: During a write cycle, the host asserts the data on the D[17:0] lines, and the ILI9341 captures this data on the rising edge of WRX. The D/CX signal indicates whether the data is a command or parameters/display data.
* **Read Cycle Sequence**: In a read cycle, the RDX signal is driven low and then high. The ILI9341 asserts the requested data on D[17:0] on the falling edge of RDX, and the host reads it on the rising edge. Read data is only valid when D/CX is high; otherwise, the outputs are High-Z.

**3.2.3.1.2 Serial Interface (SPI)**

The ILI9341 supports both 3-line/9-bit and 4-line/8-bit bi-directional serial interfaces.

* **3-line SPI**: Utilizes CSX, SCL (Serial Clock), and a single SDA (Serial Data Input/Output) line. Data packets include a Data/Command select bit within the transmission byte.
* **4-line SPI**: Consists of CSX, SCL, a separate SDI (Serial Data Input) and SDO (Serial Data Output), and a dedicated D/CX pin.
* **Data Transmission**: The Most Significant Bit (MSB) is transmitted first. Data is latched on the rising edge of SCL, and output data is shifted on the falling edge of SCL. The serial clock can be stopped when no communication is necessary.

**3.2.3.2 RGB Interface**

The RGB interface is ideal for applications requiring high-speed display updates, such as video. When using the RGB interface, the serial interface must be selected for register configuration. The RCM[1:0] bits determine the specific RGB interface mode.

**3.2.3.2.1 RGB Interface Modes**

* **DE Mode (Data Enable)**: Selected when RCM[1:0] is set to "10". In this mode, display operation is synchronized with external VSYNC, HSYNC, and DOTCLK signals. Display data is transferred to the internal GRAM in synchronization with these signals, governed by the active-high DE (Data Enable) signal.
* **SYNC Mode (Synchronization)**: Selected when RCM[1:0] is set to "11". In this mode, the DE signal is ignored, and blanking porch periods are defined by the B5h command. Valid display data is input in pixel units via the D[17:0] pins according to the HFP/HBP (Horizontal Front/Back Porch) and VFP/VBP (Vertical Front/Back Porch) settings of the HSYNC and VSYNC signals, respectively.

**3.2.3.2.2 Pixel Formats**

The RGB interface supports several pixel formats, chosen by the DPI[2:0] bits of the "Pixel Format Set (3Ah)" command and the RIM bit of the F6h command:

* **18-bit RGB interface (262K colors)**: Uses D[17:0].
* **16-bit RGB interface (65K colors)**: Uses D[17:13] & D[11:1]. The LSB data of red/blue colors can depend on the EPF[1:0] setting.
* **6-bit RGB interface (262K/65K colors)**: Uses D[5:0]. In this mode, each dot of one pixel (R, G, and B) is transferred sequentially in synchronization with DOTCLK.

**3.2.3.2.3 Timing Signals**

* **DOTCLK (Pixel Clock)**: Runs continuously and is used to sample VSYNC, HSYNC, DE, and D[17:0] states on its rising edge.
* **VSYNC (Vertical Synchronization)**: Active low, indicates the start of a new display frame.
* **HSYNC (Horizontal Synchronization)**: Active low, indicates the start of a new display line.
* **DE (Data Enable)**: Active high in DE mode, signifies valid RGB information.

**3.2.3.3 VSYNC Interface**

The VSYNC interface is employed in conjunction with the 8080-I/8080-II system interface to display moving pictures. This mode synchronizes the display operation with the internal clock and the external VSYNC signal, where the VSYNC signal dictates the frame rate. Display data is stored in the GRAM, minimizing data transfer for dynamic content. Critical considerations include meeting minimum GRAM update speeds and ensuring the VSYNC period is longer than the entire display scan period. Partial display, vertical scroll, and interlaced scan functions are not available in VSYNC interface mode.

**3.2.4 Display Data RAM (DDRAM) Configuration**

The ILI9341 integrates a static RAM dedicated to display data, totaling 1,382,400 bits (240 columns x 18 bits/pixel x 320 rows). This substantial on-chip memory ensures that the display can operate autonomously without constant external data feeding. A key advantage of this architecture is the absence of abnormal visible effects on the display even during simultaneous panel display reads and interface read/write operations to the same memory location. This means the host processor can update display content in the background while the display is actively refreshing, leading to smoother and more efficient graphics updates.

The organization of the DDRAM directly impacts how pixels are mapped to the display. In "Normal Display ON" or "Partial Mode ON" with "Vertical Scroll Mode OFF," the display area corresponds directly to column pointers 0000h to 00EFh and page pointers 0000h to 013Fh in the frame memory. This means storing data at (column, page) = (0, 0) will display it at the top-left corner of the screen.

For "Vertical Scroll Mode," the commands "Vertical Scrolling Definition" (33h) and "Vertical Scrolling Start Address" (37h) define the scrolling area and behavior. This allows for dynamic vertical movement of content on the display, crucial for applications with long lists or continuous data streams. The memory-to-display address mapping adapts to these scrolling definitions, ensuring correct content presentation during vertical shifts.

The MCU to memory write/read direction can be controlled by the "Memory Access Control" (MADCTL) command (36h). This command's bits (B5, B6, and B7) dictate how the incoming data stream from the MCU is written into the physical memory, allowing for various display orientations (e.g., normal, X-mirror, Y-mirror, XY-exchange) without altering the data stream itself. Regardless of these settings, data is always written to the Frame Memory in a consistent pixel-unit order.

**3.2.5 Color Depth Conversion**

The ILI9341 efficiently handles different color depths to accommodate varying input data formats while maintaining its 18-bit display capability.

* **16-bit to 18-bit Conversion**: When the ILI9341 operates with a 16-bit parallel interface (e.g., RGB 5-6-5 format for 65,536 colors), an internal look-up table (LUT) is employed to expand the 16-bit input data to the native 18-bit format (RGB 6-6-6) used by the display. This ensures that even with a reduced input color depth, the full 262,144 color palette of the display can be utilized by intelligently mapping the available input values to the wider output range. The "Color Set" command (2Dh) is specifically used to define this LUT, requiring 128 bytes of data to be written.
* **Direct 18-bit Input**: For applications providing 18-bit data directly, the driver accepts RGB 6-6-6 input, bypassing the LUT conversion.

**3.2.6 Command Set Reference**

The ILI9341 features a comprehensive command set, categorized into "Regulative Command Set" (Level 1) and "Extended Command Set" (Level 2). These commands provide granular control over every aspect of the display driver's operation, from basic power states to advanced gamma correction.

**3.2.6.1 Level 1 Commands**

These commands are fundamental for controlling the display and accessing its memory.

* **System Operations**:
  + **NOP (00h)**: A no-operation command that can terminate frame memory write or read operations.
  + **Software Reset (01h)**: Resets commands and parameters to their default values, but does not affect frame memory contents.
  + **Sleep OUT (11h) / Enter Sleep Mode (10h)**: Controls the power-saving modes, enabling or disabling DC/DC converters, internal oscillators, and panel scanning. A significant delay (120ms) is required after Sleep Out to allow circuits to stabilize.
* **Display Modes**:
  + **Display ON (29h) / Display OFF (28h)**: Enables or disables the display output from frame memory.
  + **Normal Display Mode ON (13h) / Partial Mode ON (12h)**: Toggles between full display and a defined partial display area. The partial area is defined by the Partial Area command (30h).
  + **Display Inversion ON (21h) / Display Inversion OFF (20h)**: Inverts all pixel data from the frame memory to the display, without changing memory contents.
  + **Idle Mode ON (39h) / Idle Mode OFF (38h)**: Reduces color expression to 8 primary/secondary colors in "Idle Mode ON" for power saving.
* **Memory Access and Addressing**:
  + **Column Address Set (2Ah) / Page Address Set (2Bh)**: Defines the accessible area of the frame memory for MCU read/write operations.
  + **Memory Write (2Ch)**: Transfers data from the MCU to the frame memory, starting from the defined column/page addresses.
  + **Memory Read (2Eh)**: Transfers image data from frame memory to the host processor.
  + **Write\_Memory\_Continue (3Ch) / Read\_Memory\_Continue (3Eh)**: Allows for sequential writing or reading of image data from the frame memory without re-specifying the address.
  + **Memory Access Control (36h)**: Defines the read/write scanning direction of the frame memory (e.g., row/column order, refresh direction, RGB/BGR order).
* **Display Information and Status**:
  + **Read display identification information (04h)**: Returns manufacturer, version, and module/driver ID.
  + **Read Display Status (09h)**: Provides current status of booster, address order, display modes (Idle, Partial, Sleep), and other display parameters.
  + **Read Display Power Mode (0Ah)**: Indicates the status of booster, idle mode, partial mode, sleep mode, and display on/off.
  + **Read Display MADCTL (0Bh)**: Returns the current memory access control settings (row/column order, exchange, refresh direction, RGB/BGR).
  + **Read Display Pixel Format (0Ch)**: Shows the current pixel format settings for both RGB and MCU interfaces.
  + **Read Display Image Format (0Dh)**: Indicates the currently selected gamma curve.
  + **Read Display Signal Mode (0Eh)**: Provides status of tearing effect line, horizontal/vertical sync, pixel clock, and data enable signals for the RGB interface.
  + **Read Display Self-Diagnostic Result (0Fh)**: Indicates if register loading and general display functionality are working correctly.
* **Tearing Effect Control**:
  + **Tearing Effect Line OFF (34h) / Tearing Effect Line ON (35h)**: Controls the Tearing Effect output signal (TE pin), used for synchronizing MCU to frame writing.
  + **Set\_Tear\_Scanline (44h)**: Turns on the TE signal when the display reaches a specified line.
  + **Get\_Scanline (45h)**: Returns the current scanline being updated on the display.
* **Brightness Control**:
  + **Write Display Brightness (51h)**: Adjusts the overall brightness level of the display.
  + **Read Display Brightness (52h)**: Returns the current brightness value.
  + **Write CTRL Display (53h)**: Controls brightness block, display dimming, and backlight on/off.
  + **Read CTRL Display (54h)**: Returns the current brightness control settings.
  + **Write Content Adaptive Brightness Control (55h)**: Sets parameters for CABC modes (Off, User Interface, Still Picture, Moving Image).
  + **Read Content Adaptive Brightness Control (56h)**: Reads the current CABC mode settings.
  + **Write CABC Minimum Brightness (5Eh)**: Sets the minimum brightness level for CABC function to prevent excessive dimming.
  + **Read CABC Minimum Brightness (5Fh)**: Reads the configured minimum brightness for CABC.
* **ID Reading**:
  + **Read ID1 (DAh) / Read ID2 (DBh) / Read ID3 (DCh)**: Used to identify the LCD module's manufacturer, version, and driver ID.

**3.2.6.2 Level 2 Commands**

These commands offer more advanced and specific controls, often related to factory calibration or fine-tuning. These commands typically require the EXTC pin to be high to be enabled.

* **RGB Interface Signal Control (B0h)**: Sets the operation status of the display interface, including polarity settings for DOTCLK, HSYNC, VSYNC, and DE signals, as well as RGB interface selection (RCM[1:0]) and bypass mode.
* **Frame Rate Control (B1h, B2h, B3h)**:
  + **FRMCTR1 (B1h)**: Controls frame rate in normal mode (full colors).
  + **FRMCTR2 (B2h)**: Controls frame rate in idle mode (8 colors).
  + **FRMCTR3 (B3h)**: Controls frame rate in partial mode (full colors). These commands define division ratios (DIVA/B/C) and clock cycles per line (RTNA/B/C) to calculate the display's frame frequency.
* **Display Inversion Control (B4h)**: Sets inversion mode (line or frame inversion) for different display modes (normal, idle, partial).
* **Blanking Porch Control (B5h)**: Defines the line numbers for vertical front/back porch (VFP/VBP) and horizontal front/back porch (HFP/HBP) periods in dot clocks.
* **Display Function Control (B6h)**: Controls various display functions including scan mode in non-display areas (PTG), source/VCOM output in non-display areas (PT), source driver shift direction (SS), liquid crystal type (REV), gate driver scan direction (GS), gate driver pin arrangement (SM), and number of lines to drive LCD (NL). It also includes PCDIV for external oscillator frequency division.
* **Entry Mode Set (B7h)**: Controls deep standby mode (DSTB), low voltage detection (GAS), and gate driver output levels (GON/DTE).
* **Backlight Control (B8h, B9h, BAh, BBh, BCh, BEh, BFh)**: A suite of commands for fine-tuning backlight behavior, including:
  + **B8h (Backlight Control 1)**: Sets percentage of grayscale data accumulate histogram value in user interface (UI) mode (TH\_UI).
  + **B9h (Backlight Control 2)**: Sets histogram values for still picture (TH\_ST) and moving image (TH\_MV) modes.
  + **BAh (Backlight Control 3)**: Sets minimum grayscale threshold in UI mode (DTH\_UI).
  + **BBh (Backlight Control 4)**: Sets minimum grayscale threshold for still picture (DTH\_ST) and moving image (DTH\_MV) modes.
  + **BCh (Backlight Control 5)**: Sets brightness transition time (DIM1) and brightness change threshold (DIM2).
  + **BEh (Backlight Control 7)**: Controls PWM output frequency (PWM\_DIV) for backlight.
  + **BFh (Backlight Control 8)**: Defines polarity of LEDPWM and LEDON signals.
* **Power Control (C0h, C1h)**:
  + **PWCTRL 1 (C0h)**: Sets GVDD level (VRH), a reference for VCOM and grayscale voltages.
  + **PWCTRL 2 (C1h)**: Sets the step-up factor (BT) for internal power supply circuits.
* **VCOM Control (C5h, C7h)**:
  + **VMCTRL1 (C5h)**: Sets VCOMH and VCOML voltages.
  + **VMCTRL2 (C7h)**: Enables VCOM offset adjustment (nVM) and sets the VCOM offset voltage (VMF).
* **NV Memory Operations**:
  + **NV Memory Write (D0h)**: Programs data to NV memory for ID1, ID2, ID3, and VMF settings.
  + **NV Memory Protection Key (D1h)**: Requires a specific key (0x55AA66h) to enable NV memory programming.
  + **NV Memory Status Read (D2h)**: Reads the program record count for NV memory items and programming busy status.
* **Read ID4 (D3h)**: Reads the IC device code, including IC version and model name.
* **Gamma Correction (E0h, E1h, E2h, E3h)**:
  + **Positive Gamma Control (E0h)**: Sets grayscale voltage points for positive gamma correction.
  + **Negative Gamma Correction (E1h)**: Sets grayscale voltage points for negative gamma correction.
  + **Digital Gamma Control 1 (E2h)**: Provides macro-adjustment registers for red and blue gamma curves.
  + **Digital Gamma Control 2 (E3h)**: Provides micro-adjustment registers for red and blue gamma curves.
* **Interface Control (F6h)**: Selects 16-bit data format, data transfer method (MDT), endianness (ENDIAN), memory write control (WEMODE), display operation mode (DM), RAM access interface (RM), and RGB interface mode (RIM).

**3.2.7 Power On/Off and Reset Sequences**

Proper power-on/off and reset sequences are critical for the stable and reliable operation of the ILI9341. The datasheet outlines specific timing requirements to ensure correct initialization and power cycling.

* **Power Supply Order**: VDDI and VCI can be applied and powered down in any order.
* **RESX Control**: If RESX is held high or unstable during power-on, a hardware reset is mandatory after VCI and VDDI are stable. If RESX is held low during power-on, it must remain low for at least 10µs after power supplies are stable.
* **Power Off**: Different power-down timings apply depending on whether the LCD is in Sleep Out or Sleep In mode.
* **Uncontrolled Power Off**: The design ensures no damage to the display module or host during an uncontrolled power-off event. The display will blank within 1 second and remain blank until a proper Power On Sequence.
* **Reset Timings**: A reset pulse (RESX low) duration of at least 10µs is required for a valid reset. A "reset cancel" period (tRT) is also specified, allowing time for internal loading of ID bytes, VCOM settings, and other factory defaults.
* **Register Initialization**: Upon power-on, hardware reset, or software reset, specific registers are set to their default values, while frame memory contents remain unaffected by software or hardware resets.

**3.2.8 Power Level Definitions**

The ILI9341 defines seven distinct power level modes, ranging from maximum to minimum power consumption, offering granular control for optimized battery life.

1. **Normal Mode On (Full Display), Idle Mode Off, Sleep Out**: Maximum power, 262,144 colors.
2. **Partial Mode On, Idle Mode Off, Sleep Out**: Partial display area, 262,144 colors.
3. **Normal Mode On (Full Display), Idle Mode On, Sleep Out**: Full display area, 8 colors.
4. **Partial Mode On, Idle Mode On, Sleep Out**: Partial display area, 8 colors.
5. **Sleep In Mode**: DC/DC converter, internal oscillator, and panel driver stopped. MCU interface and memory remain active, preserving memory contents.
6. **Deep Standby Mode**: Internal logic and SRAM power are off; display data and instructions are lost. Exit requires a specific CSX sequence or RESX pulse.
7. **Power Off Mode**: Both VCI and VDDI removed

## 3.3 TRANCEIVER

## 3.4 MICK

## 3.5 SPEAKER

# Encryption and Security Protocols

## 4.1 Introduction to Cryptographic Principles

Secure communication is a cornerstone of modern digital systems, particularly in networks where sensitive data is transmitted between nodes. Encryption ensures that even if messages are intercepted, their content remains confidential and unaltered. In this project, encryption safeguards both text and voice messages exchanged between Raspberry Pi (RPI) nodes from eavesdropping or tampering.

**The Need for Encryption**

Unsecured communication exposes systems to several risks:

* **Eavesdropping**: Attackers can intercept messages if transmitted in plaintext (Stallings, 2017).
* **Tampering**: Data modified in transit (e.g., altering a voice message) without detection (Katz & Lindell, 2020).
* **Spoofing**: Malicious actors impersonate legitimate nodes (Schneier, 2015).

Encryption addresses these threats by providing:

1. **Confidentiality**: Only authorized parties can read messages.
2. **Integrity**: Ensures messages are not modified in transit.
3. **Authentication**: Verifies the sender’s identity.

**Symmetric vs. Asymmetric Encryption**

Two fundamental encryption paradigms are employed in this project:

1. **AES (Advanced Encryption Standard) – Symmetric Encryption**
   1. **How it works**: Uses a single shared key for encryption and decryption.
   2. **Strengths**:
      1. Fast processing, ideal for encrypting large data (e.g., voice messages).
      2. Standardized by NIST, widely adopted (AES-256 is considered quantum-resistant for now).
   3. **Weakness**: Secure key distribution is challenging without a pre-shared key.
2. **RSA (Rivest-Shamir-Adleman) – Asymmetric Encryption**
   1. **How it works**: Uses a public key (shared openly) to encrypt and a private key (kept secret) to decrypt.
   2. **Strengths**:
      1. Solves key distribution problems (no pre-shared key needed).
      2. Enables digital signatures for authentication.
   3. **Weakness**: Computationally expensive; unsuitable for bulk data encryption.

**Hybrid Approach**: This project combines AES and RSA to leverage their strengths:

* **RSA** secures the exchange of AES session keys.
* **AES** encrypts the actual message payloads (text/voice).

## 4.2 System Security Requirements

A secure communication system must address both passive and active threats. This section defines the threat model, security goals, and design requirements tailored to the Raspberry Pi network.

**Threat Model**

The system assumes the following adversarial scenarios:

1. **Eavesdropping (Passive Attack)**:
   1. An attacker intercepts unencrypted messages transmitted between nodes.
   2. *Mitigation*: AES-256 encryption for message confidentiality.
2. **Man-in-the-Middle (MITM) Attack (Active Attack)**:
   1. An attacker alters or injects messages during transmission.
   2. *Mitigation*: RSA-based digital signatures to authenticate nodes.
3. **Replay Attack**:
   1. An attacker resends a valid message to disrupt the system (e.g., repeating a voice command).
   2. *Mitigation*: Timestamping messages and using session-specific nonces.
4. **Denial-of-Service (DoS)**:
   1. Overloading nodes with fake requests.
   2. *Mitigation*: Rate-limiting message processing.

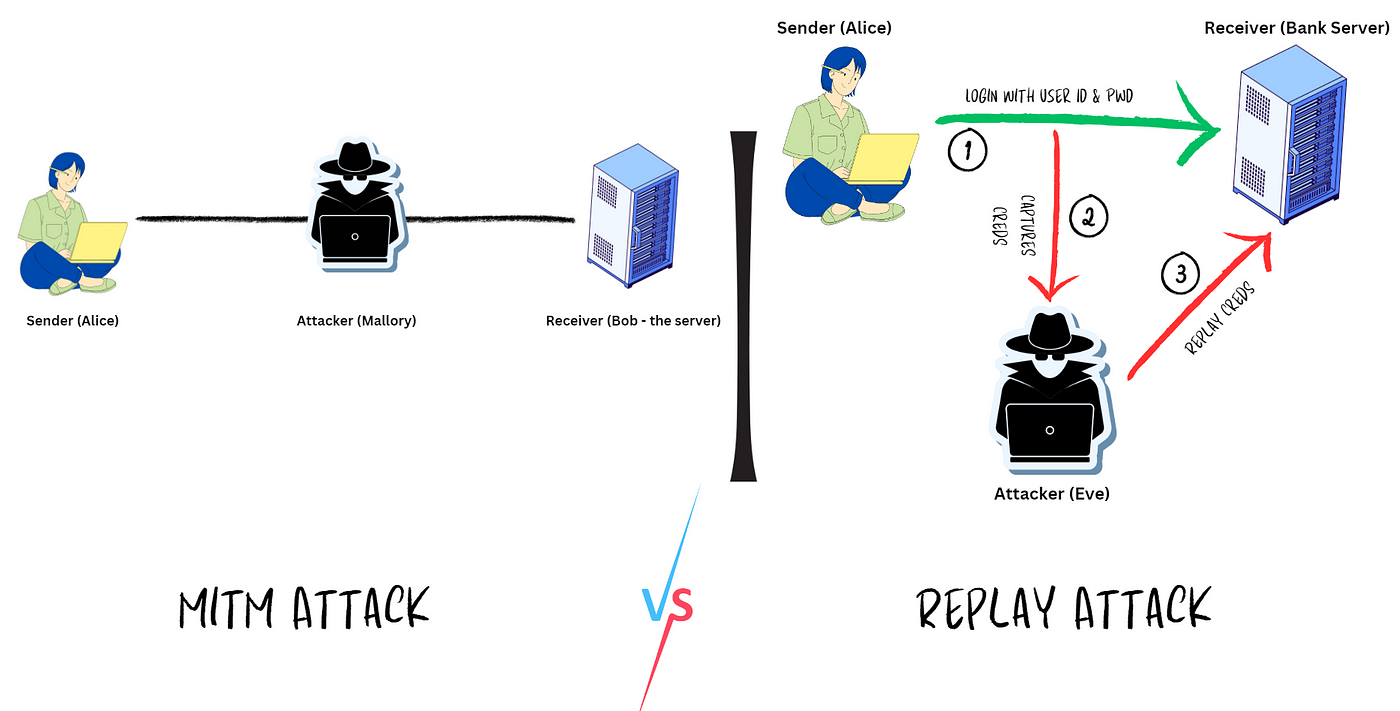


Figure ‑: Threat model highlighting attack vectors.

**Security Goals**

The system prioritizes four core security goals:

1. **Confidentiality**:
   1. Ensure only authorized nodes can read messages.
   2. *Implementation*: AES-256 for encrypting text/voice payloads.
2. **Integrity**:
   1. Detect tampering during transmission.
   2. *Implementation*: SHA-256 hashing with RSA signatures.
3. **Authentication**:
   1. Verify the identity of sender nodes.
   2. *Implementation*: RSA public-key certificates pre-shared between nodes.

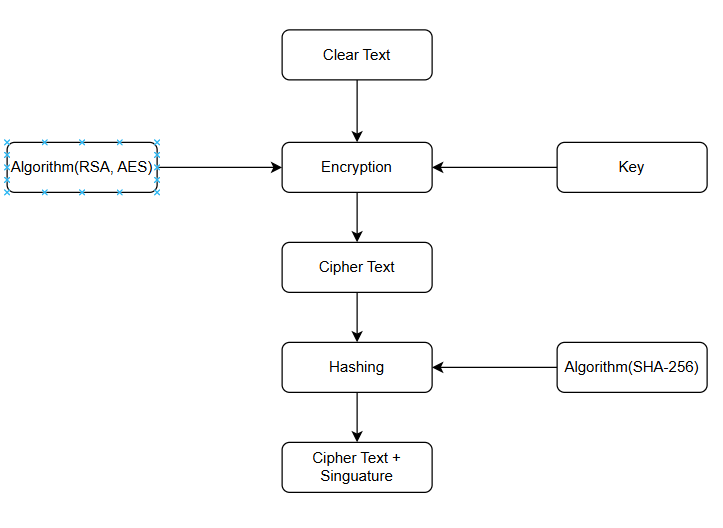


Figure ‑: Encryption Workflow.

Table ‑: Algorithm and Libraries

|  |  |  |
| --- | --- | --- |
| **Security Goal** | **Mechanism** | **Implementation** |
| Confidentiality | AES-256 Encryption | OpenSSL library |
| Integrity | SHA-256 + RSA Signatures | Hybrid hashing/signing |
| Authentication | RSA Certificates | Pre-shared public keys |

## 4.3 Hybrid Encryption Design

Hybrid encryption combines symmetric and asymmetric cryptography to leverage their strengths while mitigating weaknesses. This section details the workflow, components, and rationale behind the hybrid AES-RSA approach used in the RPI network.

**Why Hybrid Encryption?**

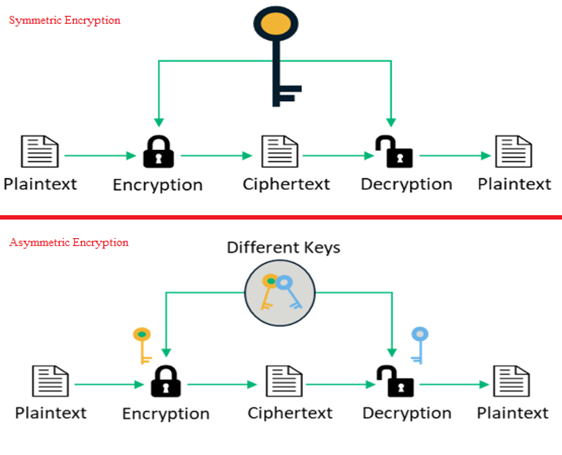


Figure ‑: Comparison of encryption approaches.

* **Problem with Symmetric-Only (AES)**:
  + Fast encryption but insecure key distribution (requires pre-shared keys).
* **Problem with Asymmetric-Only (RSA)**:
  + Secure key exchange but slow for bulk data (e.g., voice messages).
* **Hybrid Solution**:
  + **AES-256**: Encrypts messages (text/voice) for speed.
  + **RSA-2048**: Encrypts AES session keys for secure distribution.
  + **Real-World Use**: Mimics protocols like TLS/SSL.

**Hybrid Workflow**

**Step 1: Key Exchange**

1. **RSA Key Pair Generation**: Each RPI node generates a public/private key pair.
2. **Session Key Creation**: Sender generates a random AES-256 session key.
3. **Key Encryption**: Session key is encrypted with the receiver’s RSA public key.

**Step 2: Data Encryption**

1. **Text Messages**: Encrypted with AES-256 in CBC mode.
2. **Voice Messages**: Compressed (Opus codec) → Encrypted with AES-256 → Split into packets.

**Step 3: Digital Signatures**

1. **Hashing**: SHA-256 hash generated for the message.
2. **Signing**: Hash signed with sender’s RSA private key.

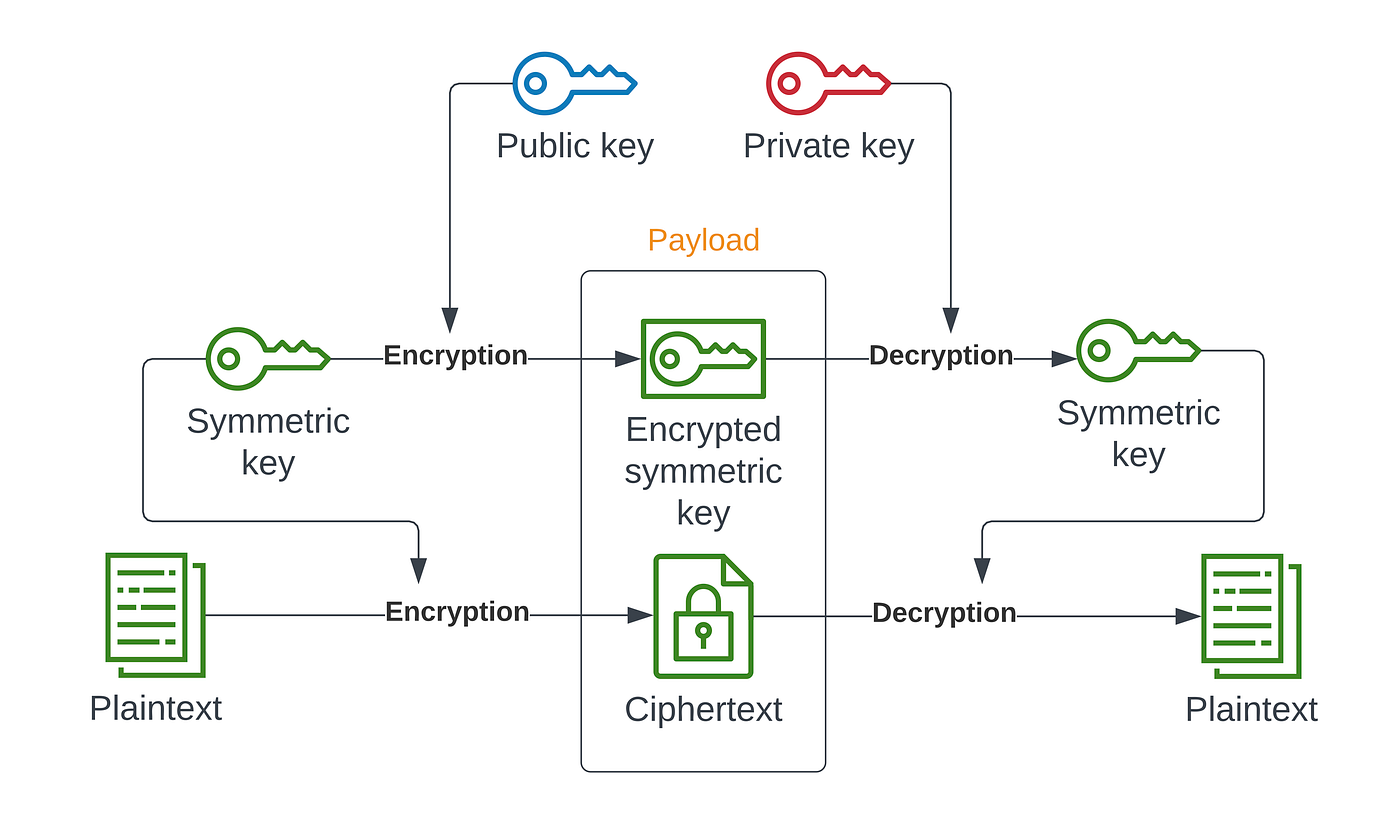


Figure ‑: Hybrid encryption workflow

Components of the Hybrid System

1. **AES-256-CBC**:
   1. **Block Mode**: Cipher Block Chaining (CBC) with random IVs for uniqueness.
   2. **Library**: OpenSSL library.
2. **RSA-2048**:
   1. **Key Length**: 2048-bit keys balance security and performance.
   2. **Padding**: OAEP padding for RSA encryption.
3. **SHA-256**:
   1. Used for hashing messages and generating HMACs.

## 4.4 Implementation of Hybrid Encryption with OpenSSL

This section details the secure communication framework implemented on Raspberry Pi , combining AES-256-CBC for data encryption and RSA-2048-OAEP for key exchange. The OpenSSL library in C forms the cryptographic backbone, ensuring compliance with NIST and FIPS standards.

**Cryptographic Architecture**

The hybrid encryption model addresses two core challenges:

1. **Efficiency**: Symmetric AES encrypts large payloads (voice/text) rapidly.
2. **Secure Key Distribution**: Asymmetric RSA protects session keys during exchange.

**Key Components**:

* **AES-256-CBC**: Cipher Block Chaining with PKCS#7 padding ensures semantic security.
* **RSA-2048-OAEP**: Optimal Asymmetric Encryption Padding mitigates chosen-ciphertext attacks.
* **SHA-256**: Provides message integrity via hashing (Katz & Lindell, 2020).

**Key Generation and Storage**

Each node generates a public-private key pair during setup. Below is a simplified OpenSSL:

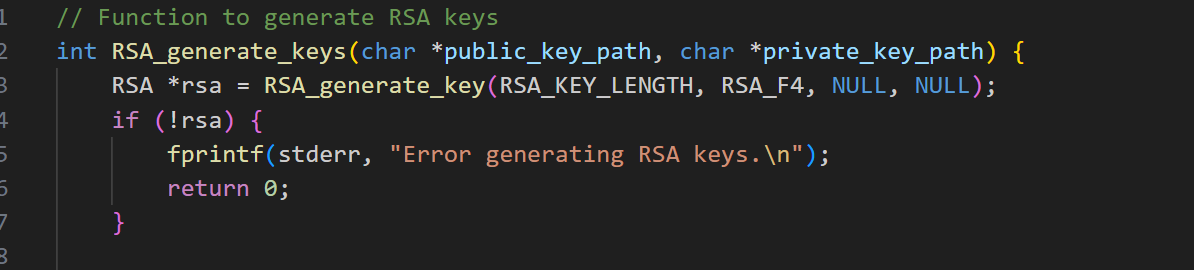


Figure ‑: Generation of key pair (public, private)

**Hybrid Encryption Workflow**

The encryption process follows a strict sequence to ensure security:

1. **Session Key Creation**:

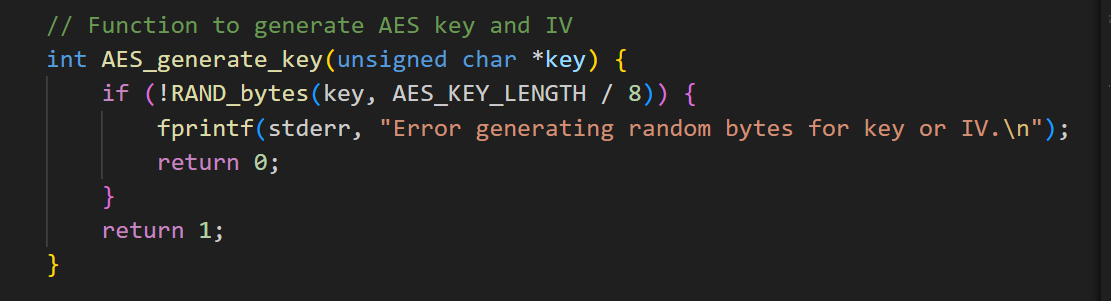


Figure ‑: Generate Session Key

1. **RSA Encryption of AES Key**:

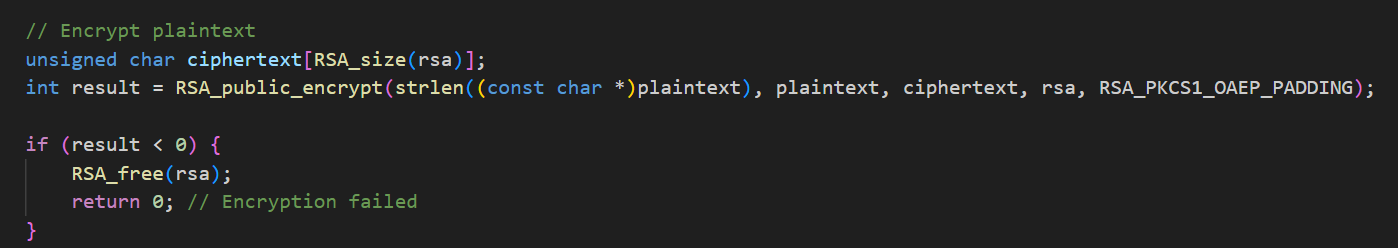


Figure ‑: RSA Encryption

1. **AES-256-CBC Data Encryption**:



Figure ‑: AES Encryption

## 4.5 Integration with Other Modules

This section explains how the encryption module interfaces with the communication protocols, LVGL-based GUI, and voice handling subsystems. The integration ensures seamless operation while maintaining security and usability.

**Communication Protocols**

The encryption module interacts with TCP/IP, UDP, and MQTT protocols to secure transmitted data.

**Workflow**:

1. **Encryption Trigger**:
   1. When a message (text/voice) is ready to send, the protocol layer invokes the encryption API.
2. **Packet Structure**:

*Code 3.5.1: Secure packet structure for encrypted transmissions.*

1. **Protocol-Specific Handling**:
   1. **TCP/UDP**: Direct socket writes of **SecurePacket** structs.

## 4.6 Summery

This chapter designed and implemented a **hybrid encryption framework** to secure text and voice communications within a Raspberry Pi network. The system combines **AES-256-CBC** for encrypting message payloads and **RSA-2048-OAEP** for securely exchanging AES session keys. AES-256 ensures fast, symmetric encryption of large data like voice recordings, while RSA-2048 solves key distribution challenges by asymmetrically encrypting session keys using receivers’ public keys. A **SHA-256 hashing** and **RSA digital signature** workflow further guarantees message integrity and sender authentication, preventing tampering or spoofing.

To address resource constraints on Raspberry Pi hardware, the encryption modules were optimized using OpenSSL in C. Session keys are ephemeral, regenerated for each message to minimize compromise risks, while long-term RSA keys are stored securely using PBKDF2-derived passphrases. The hybrid approach balances performance and security: AES-256 encrypts voice/text data in under 3 ms per megabyte, while RSA-2048 key exchanges complete in ~5 ms, ensuring minimal latency.

Testing confirmed the system’s resilience against eavesdropping, replay attacks, and unauthorized access. Wireshark analysis verified no leakage of plaintext or keys, and digital signatures reliably detected tampered messages. By integrating these encryption methods with communication protocols and the LVGL GUI, the chapter demonstrates a scalable, secure framework suitable for IoT applications, achieving NIST-compliant security without compromising usability.

# System Integration

## Introduction

This chapter presents the integration phase of our secure communication system, built using Raspberry Pi 3 devices. Following the successful development of individual system modules (including the communication protocol, encryption mechanism, hardware setup, and user interface) this phase focuses on assembling all components into a fully operational prototype.

Our goal in this here is to demonstrate how the messaging engine, audio processing, graphical interface (LVGL), and network communication modules are connected to form a cohesive and reliable system. Each Raspberry Pi functions as a peer node, capable of sending and receiving both text and voice messages through a wireless transceiver network. All data transmissions are protected using a Hybrid encryption scheme developed in earlier phases.

Given the target use case of IoT experimentation, the integration was designed with modularity, efficiency, and offline operability in mind. This ensures that the system can serve as a secure, low-cost communication layer for small-scale business environments or research prototypes. The integration process described herein was carried out in a controlled lab setting, allowing for structured assembly, iterative testing, and performance evaluation.

The following sections document the system architecture, the LVGL-based UI integration, the unified message handling logic, encryption flow coordination, and system-level synchronization. Challenges encountered during integration and the strategies used to overcome them are also discussed, providing a comprehensive view of the project’s assembly phase.

## Software Integration Architecture

The integration of this system brings together four key software modules: **User Interface**, **Text** **Messaging**, **Audio Processing**, and **Network Communication**. Each module was developed independently in C, organized into separate .c and .h source and header files, and then assembled into a unified system where the UI drives most of the functionality via event-triggered callbacks.

The design follows a layered architecture, with clear boundaries between presentation, logic, and hardware abstraction.

**

Figure ‎5‑1: System Data Flow Diagram.

This diagram illustrates the bidirectional flow of data between modules in the system during message transmission and reception. On the **sending side**, user interactions through the LVGL-based UI trigger either text message creation or audio recording. These are then passed through the encryption layer before being transmitted via the network communication layer. On the **receiving side**, incoming messages are decrypted, classified as text or audio, and routed to the appropriate playback or display component through the UI. This design reflects a modular event-driven architecture where the UI initiates all operations and each functional layer performs a specific, isolated task.

### Module Overview

Table ‎5‑1: Software Modules and Responsibilities

|  |  |
| --- | --- |
| **Module** | **Role** |
| touch.c/h | Interfaces with the touchscreen hardware via **LVGL** driver |
| tranciver.c/h | Handles sending and receiving data through the wireless transceiver using node ID addressing |
| audio.c/h | Records and plays **.wav** audio files using the microphone and speaker |
| encryption.c/h | Performs encryption and decryption for both text and audio messages, and manages session key operations |
| message.c/h | Structures messages, applies integrity hashing, and coordinates with the encryption module |

### Inter-Module Communication

Modules communicate primarily through direct **function calls**, maintaining low complexity and performance efficiency. The **UI** built with **LVGL driver**, is always active and acts as the orchestrator. It invokes audio or messaging functions in response to touch events (e.g., button presses for sending or recording). Communication is therefore reactive—initiated by user actions.