Criptografia

Objetivo

Ilustrar a implementação da criptografia quântica pelo Arduino baseada em fótons.

Lista de Materiais

2	Placas de Arduinos
30	Jumpes
1	Display LCD
5	Módulo laser
5	Módulo receptor
1	Buzzer
	Pedaços de madeira

Montagem e execução do experimento

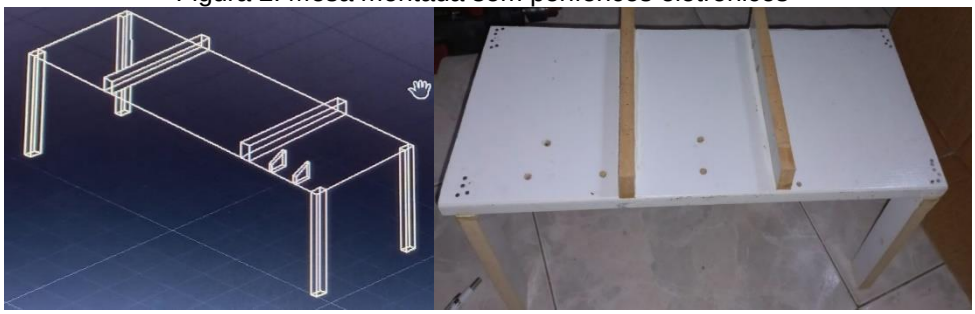
I. Pegue pedaços de madeira de 30 x 30 mm para fazer a mesa que comportará os componentes. (Figura 1).

Figura 1: Haste retangular de apoio dos componentes.

Fonte: Valmir Santos (2024).

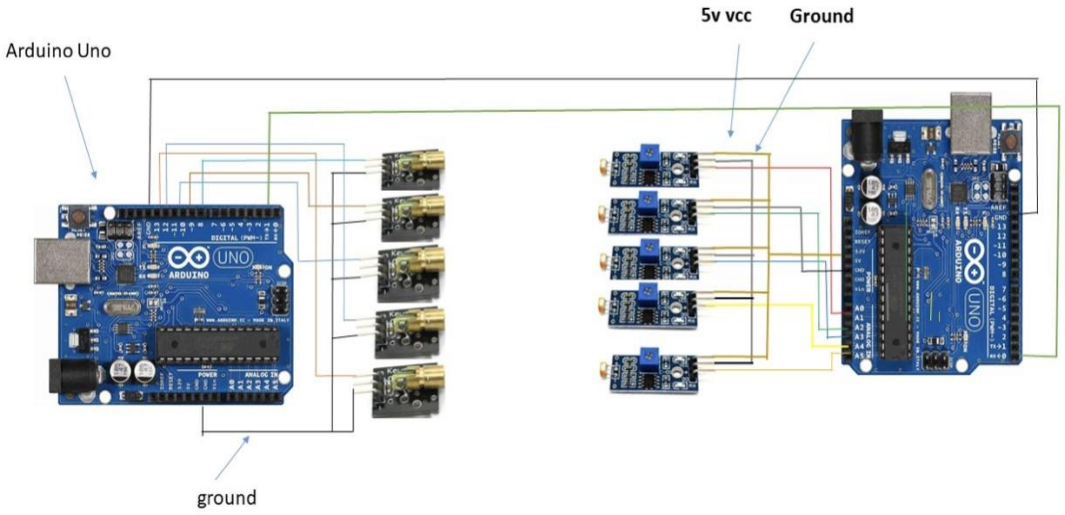
II. Pegue as 6 peças de madeiras para montar a mesa (Figura 2).

Figura 2: Mesa montada sem periféricos eletrônicos



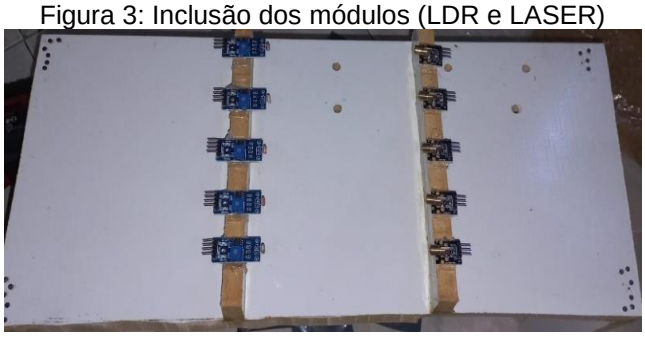
Fonte: Valmir Santos (2024).

III. O sistema sugerido inclui dois Arduinos, um no lado do transmissor e outro no lado do receptor, além dos diodos laser e fotorresistores. No lado do transmissor, uma configuração de cinco diodos laser operando aleatoriamente foi desenvolvida para emitir fótons. No lado do receptor, cinco resistores dependentes de luz (LDR), fotorresistores, são configurados como uma matriz desses fotorresisistores.



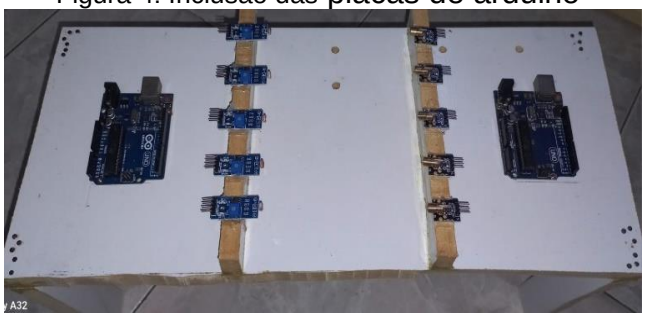
IV. Adote a sequência de montagem do experimento apresentada a seguir:

Figura 3: Inclusão dos módulos (LDR e LASER)



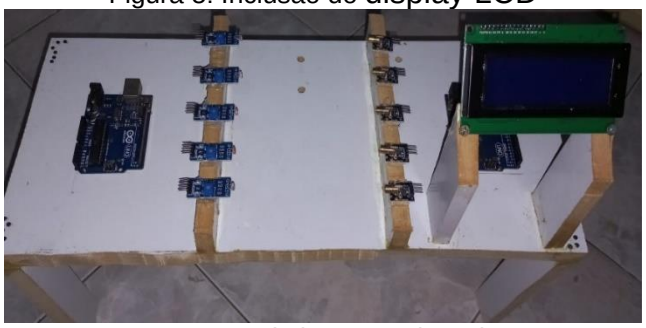
Fonte: Valmir Santos (2024)

Figura 4: Inclusão das placas de arduino



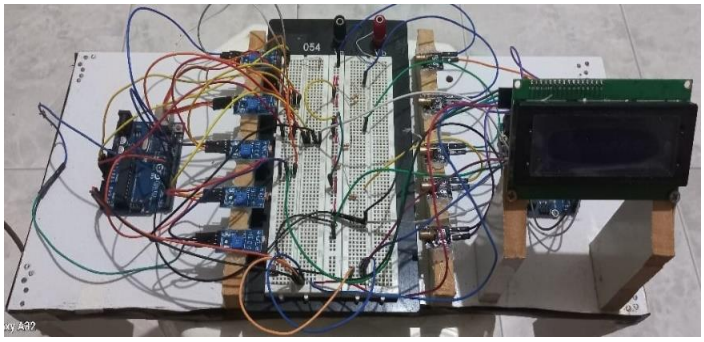
Fonte: Valmir Santos (2024)

Figura 5: Inclusão do display LCD



Fonte: Valmir Santos (2024)

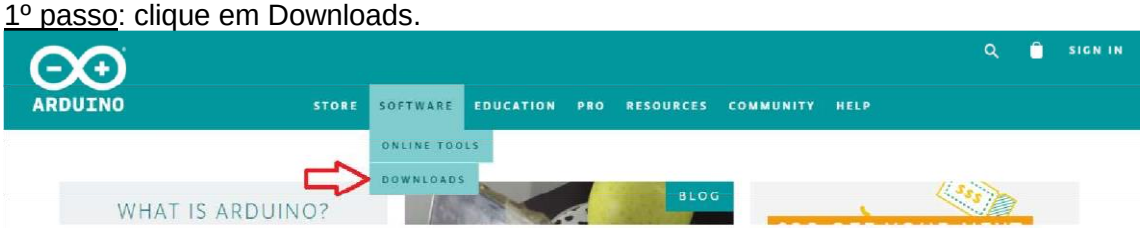
V. Experimento completo com módulos conectados por meio de jumpers e protoboard as duas controladoras e ao display LCD



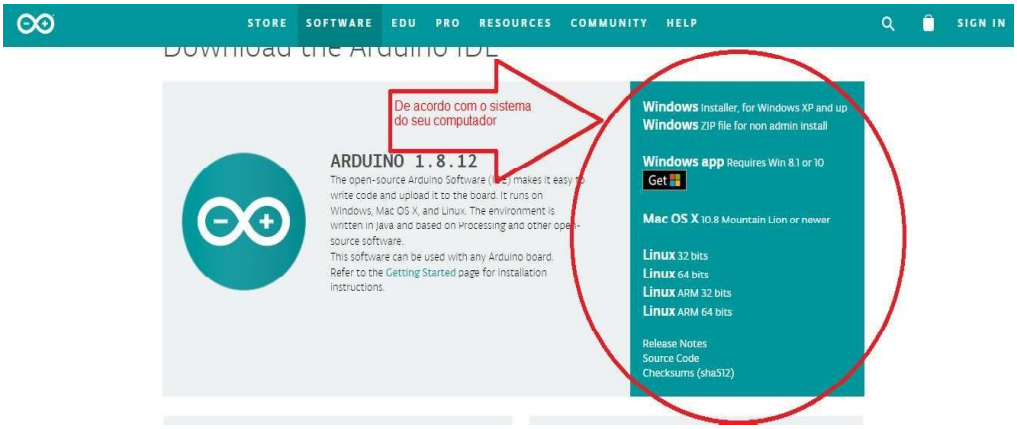
Fonte: Valmir Santos (2024).

VI. Para a conexão com o Arduino: Faça o download do aplicativo Arduino no endereço https://www.arduino.cc/. Depois siga os passos abaixo:

1º passo: clique em Downloads.



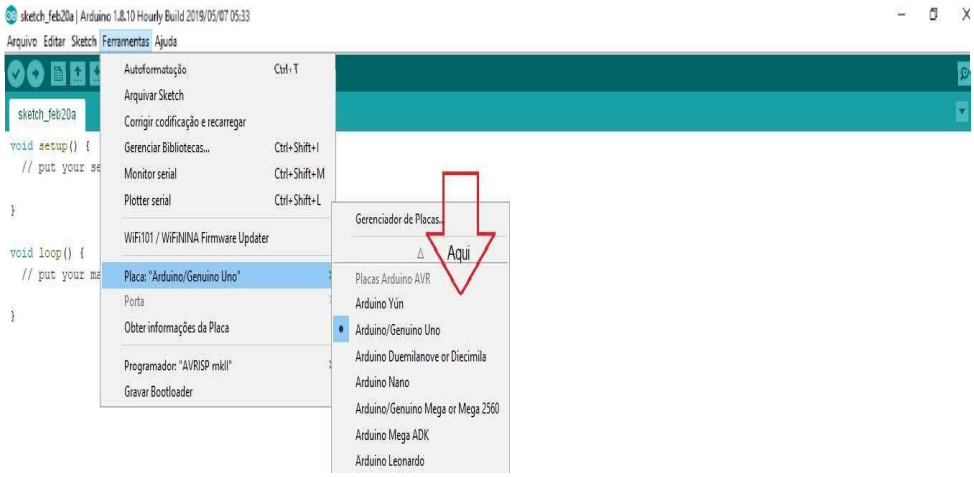
2º passo: escolha o sistema operacional.



3º passo: abra o programa na área de trabalho clicando duas vezes no ícone:

 .

4º passo: selecione a placa que será usada.



6º passo: cole o código na área de trabalho do programa, indicada a seguir.

VII. Insira o seguinte código:

```
#include <LiquidCrystal.h>
#include <SoftwareSerial.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
```

```
//////////////////////////

void printString(char *str);


//////////////////////////////////

LiquidCrystal_I2C lcd(0x27,20,4);

SoftwareSerial SerialCriada(2, 3); // RX, TX

SoftwareSerial SeriaCriada2(4, 5); // RX, TX
SoftwareSerial SerialCriada3(6, 7); // RX, TX
SoftwareSerial SerialCriada4(8, 9); // RX, TX
SoftwareSerial SerialCriada5(10, 11); // RX, TX
SoftwareSerial SerialCriada6(12, 13); // RX, TX


void setup()

 {
  // Abre a serial para receber dados
  Serial.begin(9600);// Velocidade de 960000 bits por segundo.
  Serial.println("Aguarde pelos dados.");
  SerialCriada.begin(9600);// Velocidade de 4800 bits por segundo.

Serial.flush();
  while(!Serial);
  lcd.begin();
  lcd.backlight();
  lcd.print("Valmir - Engenheiro");
  lcd.setCursor(6,2);
  lcd.print("Projeto");
  lcd.setCursor(6,1);
  lcd.print(" IFBA  ");
  lcd.setCursor(3,3);
  lcd.print(" Criptografia  ");


////////////////////////////////////

pinMode(4, INPUT);
pinMode(6, INPUT);
pinMode(8, INPUT);
pinMode(10, INPUT);
pinMode(12, INPUT);

}

void loop() {
  if (SerialCriada.available()) {// Se a serial tiver dados em seu buffer.
    Serial.write(SerialCriada.read());//Escreve na serial dados a SerialCriada

  if (Serial.available()) {
```

```
    // Wait a bit for the entire message to arrive
    delay(100);
    // Clear the screen
    lcd.clear();
while (Serial.available() > 0) {
      lcd.write(Serial.read());
    // Clear the screen

//////////////////////////////////////////
char str[66];

if(Serial.available())
  {

    short i=0;

    int num = Serial.available();

//////////////////////////////////////

}

}
  }

  }
}
```

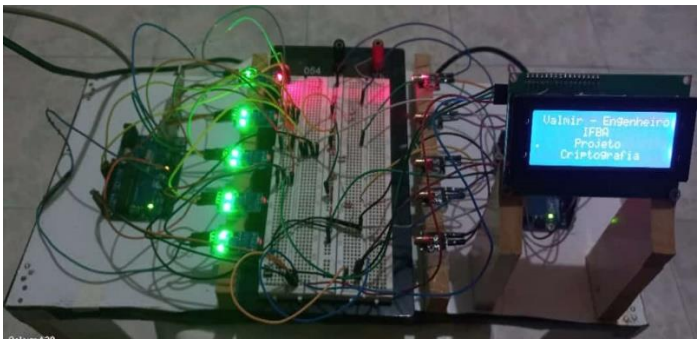
7º passo: clique em verificar para saber se há algum erro.

8º passo: transfira o código após conectar o cabo USB (Universal Serial Bus ou “Porta Universal”).

9º passo: verifique a informação que será mostrada no Monitor serial.

10º passo: ligue o Arduino com o computador com o código e o circuito montado na protoboard. Verifique o monitor Serial e o display LCD,

O experimento visa ilustrar como a informação pode ser cifrada (convertida em código binário), transmitida de forma segura e posteriormente decifrada, destacando o papel da criptografia na proteção da integridade e confidencialidade de mensagens.



Fonte: Valmir Santos (2024).

Fonte: Valmir Santos (2024).

Resultados e Discussão

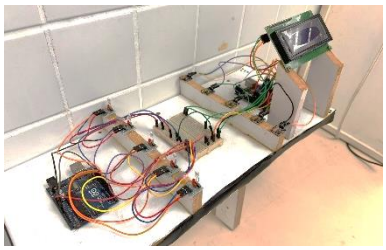
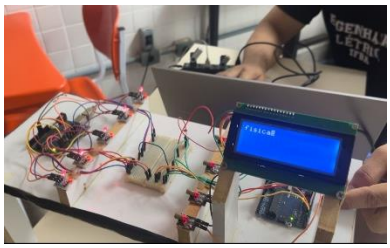
Cinco diodos laser conectados aos pinos 8, 9, 10, 11 e 12 dos chips Arduino. A criptografia de dados de informações que consistem em 0s e 1s é obtida usando lasers que produzem fótons aleatoriamente em bases diagonais e retilíneas. Esse processo é realizado por criptografia de ponta a ponta.

A principal vantagem da criptografia de ponta a ponta é proteger os dados de serem interceptados por qualquer pessoa que não seja o destinatário pretendido. A criptografia de ponta a ponta garante que o canal de comunicação permaneça privado.

Do lado receptor, cinco sensores fotorresistores no lado do receptor são usados para transmitir a presença ou ausência de luz ou para quantificar a intensidade da luz. No escuro, sua resistência era bastante alta, às vezes chegando a um milhão de ohms, mas quando exposta à luz, a resistência caía consideravelmente, às vezes para apenas alguns ohms, dependendo da força da luz. LDRs são dispositivos não lineares com uma sensibilidade que varia com o comprimento de onda da luz usada. Esses sensores estão ligados aos pinos (8, 9, 10, 11 e 12) do chip receptor Arduino.

A saída do LDR é conectada a um circuito conhecido como divisor de circuito de tensão, que é um circuito simples para diminuir a tensão. Ele dispersa a tensão de entrada entre os componentes do circuito. O melhor exemplo de um divisor de tensão eram dois resistores conectados em série, com a tensão de entrada aplicada no par de resistores e a tensão de saída medida em uma posição intermediária. Ele foi usado para gerar variantes de níveis de tensão a partir de uma única fonte de tensão, mantendo todos os componentes em um circuito em série com a mesma corrente. Este ponto poderia colocar uma questão, o "fotorresistor." já era um "resistor" e, portanto, limitaria a tensão do circuito. Por que não é possível conectá-lo com um pino e medi-lo? A resposta simples era que o Arduino podia medir facilmente a tensão, mas não a resistência. Resistores variáveis têm sido usados na maioria dos sensores, incluindo fotorresistores, sensores flexíveis e termistores. O Arduino e a "maioria dos circuitos integrados" apresentam um modesto sistema de conversor analógico-digital (ADC), o que dificulta o monitoramento das mudanças de resistência. Essa tecnologia transforma as mudanças de tensão analógica em sequências de 1 s e 0s que podem ser traduzidas em um número inteiro. Como o ADC foi projetado para ler mudanças de tensão, é necessário converter mudanças de resistência em mudanças de tensão para ler os valores do fotorresistor usando a leitura analógica do Arduino (que usa o ADC). A maneira mais fácil de conseguir isso era usando um divisor de tensão. Como o sensor era um resistor, a tensão nele deve variar. Não havia outros pontos de referência além de Vcc (5V) e terra, portanto, medir as mudanças de tensão seria complicado. O fotoresistores também tem uma classificação de corrente máxima; Um resistor em série ajudará a limitar o fluxo de corrente sob luz intensa.

A Figuras a seguir mostra como as frases podem ser enviadas e recebidas por meio do software, e o tempo é de cerca de 47 ms com uma taxa de bits de 9,6 kbps.

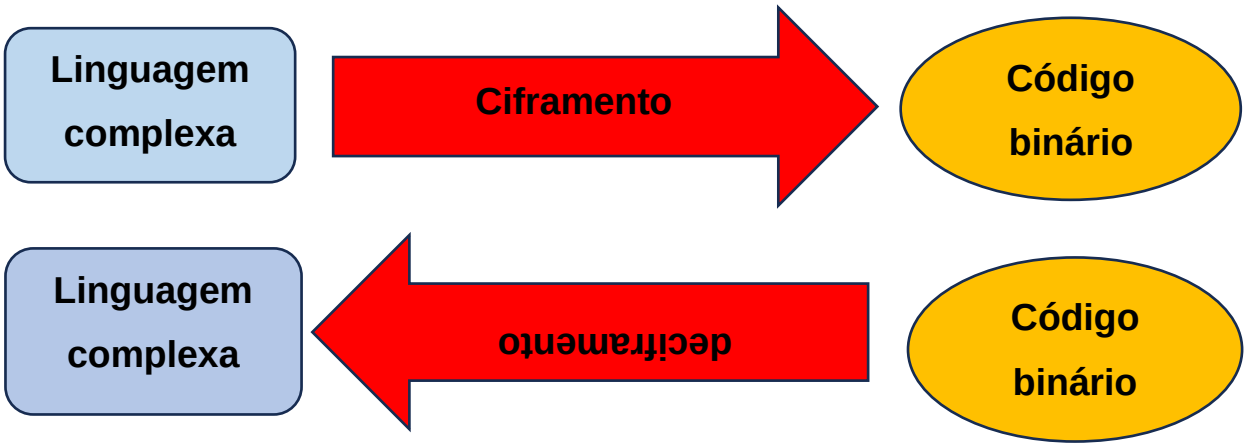




A criptografia é uma área que estuda técnicas para ocultar não apenas a mensagem real, mas o seu significado. Seu objetivo é garantir propriedades fundamentais de segurança, como a **confidencialidade, integridade e disponibilidade (CID)**, dependendo do mecanismo utilizado e da maneira como ele é empregado.

Ciframento
O processo de ciframento transforma um texto simples, composto por um alfabeto comum, em um texto cifrado. Nesse processo, as letras originais são substituídas por caracteres de um alfabeto cifrado, escondendo o conteúdo da mensagem. A função do ciframento é a responsável pela criptografia da mensagem original, convertendo-a em uma forma que só pode ser entendida por quem tiver a chave para decifrá-la.

Deciframento
O deciframento realiza o processo inverso, revertendo o texto cifrado ao seu formato original, de modo que o conteúdo da mensagem possa ser compreendido. A função de deciframento, portanto, é responsável pela descriptografia, devolvendo a mensagem ao seu formato legível.

Logo, tem-se que:



Aplicação na Criptografia Quântica

Em um cenário mais avançado, a criptografia quântica utiliza princípios da mecânica quântica, como o **entrelaçamento quântico** e o **princípio da incerteza**, para garantir uma segurança inquebrável na troca de informações. Diferentemente da criptografia

clássica, que depende de algoritmos matemáticos para proteger os dados, a criptografia quântica usa propriedades das partículas subatômicas para garantir que qualquer tentativa de interceptação seja detectada instantaneamente. Isso ocorre porque, no mundo quântico, observar uma partícula inevitavelmente altera seu estado, fazendo com que qualquer espionagem seja notada.

Exemplo de Ciframento e Deciframento em um Experimento

No experimento descrito, a criptografia é realizada através de um módulo transmissor de laser que transmite a informação. A mensagem original, representada em linguagem humana (complexa), é convertida em código de máquina (binário) pelo computador. Esse código binário é então transmitido via luz (através do módulo de laser), completando o processo de ciframento. No lado receptor, a informação binária é recebida e reconvertida para a linguagem complexa, completando o processo de deciframento. Este ciclo reflete os conceitos básicos de ciframento e deciframento, usados tanto na criptografia clássica quanto, em uma escala mais avançada, na criptografia quântica.

Conclusão

Este projeto, ao explorar o processo de criptografia e decifração, auxilia no desenvolvimento de competências fundamentais em Física Moderna e tecnologias avançadas como a criptografia quântica. A experimentação com esses conceitos oferece uma oportunidade de aprofundamento nas áreas de ciência e tecnologia, particularmente no ensino médio, permitindo que docentes apliquem a prática empírica em suas aulas de Física, promovendo uma compreensão mais sólida desses temas complexos.

Referências

QAISI, H. A.; AL-GAILANI, M. F. **Experimental Realization of Quantum Cryptography by Arduino**. (2024). Iraqi Journal of Information and Communication Technology, 6 (1), 1-8. https://doi.org/10.31987/ijict.6.1.204