Enkripsi Transmisi Data pada Mikrokontroler Arduino Menggunakan XOR Cipher Sederhana

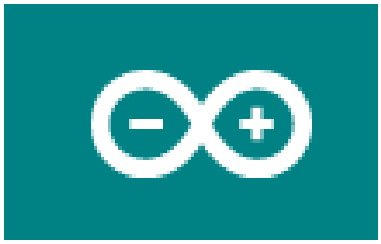
Jeremya Dharmawan Raharjo - 13521131
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13521131@std.stei.itb.ac.id

***Abstrak*—Mikrokontroler telah menjadi bagian yang terintegrasi dengan piranti IoT(Internet of Things) untuk berbagai aplikasi pada bidang teknologi. Arduino, salah satu mikrokontroler, menggunakan protokol komunikasi seperti USART untuk berkomunikasi dengan piranti lainnya. Transmisi data antar piranti dapat menggunakan metode enkripsi demi menjamin keamanan isi data yang ditransmisikan, salah satunya enkripsi dengan XOR Cipher. XOR Cipher sendiri merupakan penerapan dari aljabar Boolean pada bidang kriptografi.**

***Kata kunci*—Mikrokontroler, Arduino, Transmisi Data, USART, Kriptografi, Operasi XOR.**

I. PENDAHULUAN

Kebergantungan manusia terhadap teknologi membuat integrasi antara IoT(*Internet of Things)* dan mikrokontroler kian menjadi kebutuhan primer untuk memudahkan kehidupan manusia. Salah satu merk mikrokontroler yang terkenal di pasaran yaitu Arduino, sebuah perusahaan mikrokontroler asal Italia. Arduino sendiri merupakan sebuah perangkat elektronik yang bersifat *open source* dan sering digunakan untuk merancang dan membuat perangkat elektronik serta perangkat lunak yang mudah untuk digunakan.



Gambar 1: Logo Arduino,
diakses dari https://www.arduino.cc/

Perangkat lunak dari Arduino sendiri diprogram menggunakan bahasa C++ yang implementasinya menyesuaikan dengan lingkungan pengembangan perangkat lunak Arduino. Pemrograman ini mencakup dengan fitur-fitur yang ditawarkan oleh Arduino, seperti integrasi dengan sensor, servo, pengendali peralatan pintar, dan masih banyak lagi.

Transmisi data pada Arduino dapat dilakukan dari sensor, antar-perangkat berbasiskan mikrokontroler, maupun komputer personal. Transmisi data ke/dari komputer personal biasanya menggunakan USB yang berbasiskan protokol komunikasi USART.

Keamanan dari sistem transmisi data ini merupakan aspek yang perlu dikaji. Sudah banyak algoritma kriptografi yang dikembangkan untuk mengamankan sistem transmisi data. Pada makalah ini akan dibahas pengamanan dari data yang ditransmisikan menggunakan XOR Cipher.

II. LANDASAN TEORI

A. Aljabar Boolean

Salah satu bidang studi pada Matematika Diskrit membahas mengenai Aljabar Boolean. Aljabar Boolean sendiri ditemukan oleh George Boole, pada tahun 1854. Penemuan ini didasarkan atas keserupaan antara hukum-hukum aljabar logika dan hukum-hukum aljabar himpunan. Aljabar Boolean di dunia modern sangat aplikatif terhadap pendesainan IC(*integrated circuit*), rangkaian pensaklaran, beserta rangkaian digital.

DEFINISI[1]

Misalkan B adalah himpunan yang didefinisikan pada dua operator biner, + dan ·, dan sebuah operator uner, ’. Misalkan 0 dan 1 adalah dua elemen yang berbeda dari B. Maka, tupel

$< B, +, \cdot, ', 0, 1 >$

disebut aljabar Boolean jika untuk setiap a, b, cB berlaku aksioma berikut:

1. Identitas

$(i)\ a + 0 = a$
$(ii)\ a \cdot 1 = a$

2. Komutatif

$(i)\ a + b = b + a$
$(ii)\ a \cdot b = b \cdot a$

3. Distributif

$(i)\ a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
$(ii)\ a + (b \cdot c) = (a + b) \cdot (a + c)$

4. Komplemen

Untuk setiap $a \in B$ terdapat elemen unik $a' \in B$ sehingga

$(i)\ a + a' = 1$
$(ii)\ a \cdot a' = 0$

Aljabar Boolean 2-Nilai merupakan aljabar Boolean dengan pengaplikasian paling luas. Pada Aljabar Boolean 2 nilai, terdapat kaidah dan properti sebagai berikut:

i. B = {0,1}

ii. operator biner: + dan ·, operator uner: ’ . Adapun operator + ekivalen dengan OR, operator · ekivalen dengan AND, dan operator ’ ekivalen dengan NOT.

iii. Berikut ini merupakan kaidah untuk operator biner dan operator uner:

a) Operator biner AND

a	b	$a \cdot b$
0	0	0
0	1	0
1	0	0
1	1	1

Gambar 2: Tabel Kebenaran Operasi AND, (Sumber: [1])

b) Operator biner OR

a	b	$a + b$
0	0	0
0	1	1
1	0	1
1	1	1

Gambar 3: Tabel Kebenaran Operasi OR, (Sumber: [1])

c) operator uner NOT

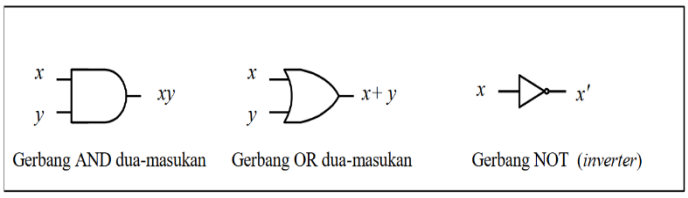
a	$a’$
0	1
1	0

Gambar 4: Tabel Kebenaran Operasi NOT, (Sumber: [1])

iv. Keempat aksioma di atas terpenuhi

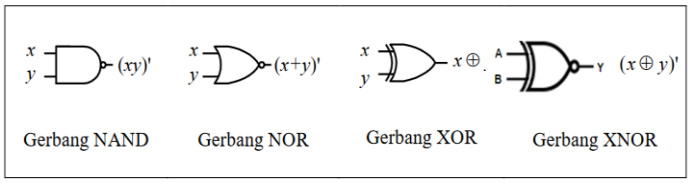
B. Gerbang Logika

Adapun untuk mewakili operator dasar Boolean, terdapat 3 buah gerbang logika dasar: gerbang AND dengan 2 masukan, gerband OR dengan 2 masukan, dan gerbang NOT(inverter) dengan satu buah masukan.



Gambar 5: 3 Gerbang Logika Dasar (Sumber: [1])

Selain ketiga jenis gerbang logika tersebut, terdapat gerbang logika turunan: NAND, NOR, XOR, dan XNOR.



Gambar 6: Gerbang-gerbang Logika Turunan (Sumber: [1])

Untuk gerbang XOR sendiri(exclusive OR), berikut merupakan tabel kebenaran berdasarkan input dan outputnya:

Input		Output
A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

Gambar 7: Tabel Kebenaran Operasi XOR, (Sumber: https://en.wikipedia.org/wiki/XOR_gate, diakses pada 11 Desember 2022)

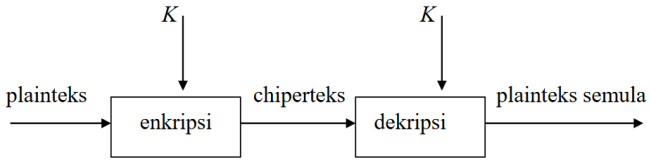
C. Kriptografi

Kriptografi[3] merupakan ilmu dan seni untuk menjaga keamanan pesan dengan cara menyandikannya menjadi bentuk lain yang tidak bermakna. Kriptografi sendiri berasal dari Bahasa Yunani, yang artinya “*secret writing*”. Berikut merupakan beberapa terminologi dalam Kriptografi:

- **Pesan**: data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain: **plainteks** (plaintext)
- **Cipherteks** (ciphertext): pesan yang telah disandikan sehingga tidak memiliki makna lagi.

Contoh:
Plainteks: `culik anak itu jam 11 siang`
Cipherteks: `t^$gfUi9rewoFpfdWqL:[uTcxZy`

- **Enkripsi** (encryption): proses menyandikan plainteks menjadi cipherteks.
- **Dekripsi** (decryption): Proses mengembalikan cipherteks menjadi plainteksnya.



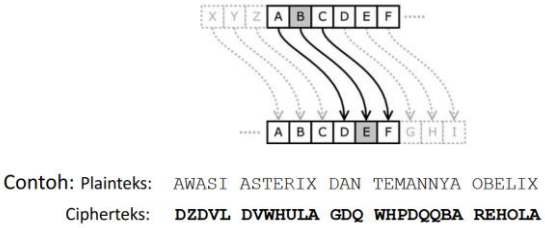
Gambar 8: Ilustrasi proses enkripsi-dekripsi (Sumber: [2])

Adapun beberapa aplikasi dari Enkripsi-Dekripsi adalah sebagai berikut:

1. Pengiriman data melalui saluran komunikasi (*data encryption on motion).*

→ pesan dikirim dalam bentuk cipherteks
2. Penyimpanan dokumen di dalam disk storage (*data encryption at rest*)
→ data disimpan di dalam disk dalam bentuk cipherteks

Algoritma kriptografi sederhana yang paling terkenal ialah Caesar cipher. Algoritma ini digunakan pada masa pemerintahan Julius Caesar. Tiap huruf alfabet digeser 3 huruf ke kanan secara *wrapping*



Gambar 9: Ilustrasi Algoritma Caesar Cipher(Sumber: [2])

Pada masa kini, terdapat algoritma kriptografi yang lebih modern. Salah satunya algoritma RSA(Ronald Rivest, Adi Shamir, dan Leonard Adleman), algoritma kriptografi yang memanfaatkan subjek teori bilangan dengan menghitung kekongruenan lanjar untuk proses enkripsi dan dekripsi.

D. XOR Cipher

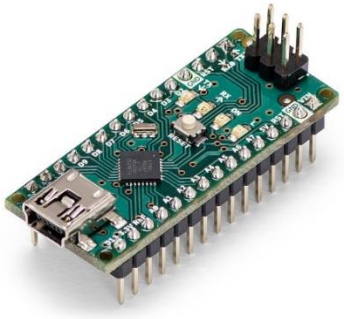
XOR cipher[3] merupakan salah satu jenis metode kriptografi yang digunakan untuk melakukan enkripsi dan dekripsi data. Enkripsi ini menggunakan kunci yang disebut XOR key, yang merupakan sebuah string binary. XOR cipher menggunakan prinsip XOR (Exclusive OR) yang berbasiskan pada aljabar boolean untuk melakukan enkripsi dan dekripsi data.

XOR cipher sendiri membutuhkan sebuah kunci XOR untuk melakukan enkripsi data dengan cara melakukan operasi XOR antara data yang akan dienkripsi dan kunci XOR. Setelah data dienkripsi, ia hanya dapat didekripsi kembali dengan menggunakan kunci XOR yang sama. Berikut merupakan prinsip enkripsi-dekripsi dari informasi oleh algoritma ini.

$$\text{Ciphertext: } C_i = P_i \oplus K_i$$
$$\text{Plaintext: } P_i = C_i \oplus K_i$$

Aplikasi XOR cipher cukup sederhana, namun keamanannya tidak sebaik enkripsi kriptografi lainnya seperti algoritma AES atau RSA.

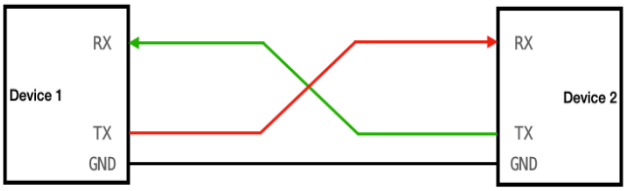
E. Arduino Nano



Gambar 10: Arduino Nano, diakses dari https://store.arduino.cc/products/arduino-nano

Arduino Nano[4] adalah salah satu jenis papan mikrokontroler yang dikembangkan oleh Arduino. Board ini memiliki ukuran yang lebih kecil dibandingkan dengan board Arduino lainnya seperti Arduino Uno, sehingga sering disebut sebagai versi mini dari Arduino Uno. Arduino Nano juga memiliki fitur yang hampir sama dengan Arduino Uno, seperti memiliki 14 pin digital I/O dan 8 pin input analog, serta dapat digunakan untuk memprogram berbagai jenis proyek elektronik. Namun, ada beberapa perbedaan, seperti Arduino Nano menggunakan prosesor ATmega328 sedangkan Arduino Uno menggunakan prosesor ATmega2560. Arduino Nano memiliki bentuk yang kecil sehingga cocok untuk mengembangkan perangkat elektronik berbasis mikrokontroler dengan skala yang kecil.

F. USART



Gambar 11: Ilustrasi Komunikasi via USART, diakses dari https://vanhunteradams.com/Protocols/UART/UART.html

USART[5] adalah singkatan dari *Universal Synchronous Asynchronous Receiver Transmitter*, yaitu sebuah perangkat yang digunakan untuk mentransmisikan dan menerima data secara sinkron maupun asinkron. USART biasanya digunakan dalam sistem komunikasi serial, seperti komunikasi antara mikrokontroler-komputer atau antar dua mikrokontroler. USART bisa digunakan untuk mentransmisikan data secara sinkron, di mana data ditransmisikan berdasarkan *clock* yang dibangkitkan oleh salah satu perangkat, atau asinkron, di mana data ditransmisikan tanpa menggunakan *clock* eksternal.

Pada Arduino, USART dapat digunakan melalui USB dengan menggunakan fungsi serial. Fungsi ini akan memicu USART yang terintegrasi pada Arduino, sehingga dapat digunakan untuk menerima dan mengirimkan data melalui USB. Dengan menggunakan fungsi `serial`, data dapat dikirimkan dari komputer ke Arduino atau sebaliknya, sehingga dapat digunakan untuk mengontrol perangkat yang terhubung ke Arduino atau menampilkan informasi dari Arduino ke komputer.

Untuk menggunakan USART via USB pada Arduino, mengoneksikan USB antara Arduino dan komputer. Kemudian, akses USART melalui fungsi `serial` yang disediakan oleh Arduino. Fungsi serial memiliki beberapa parameter yang dapat Anda gunakan untuk mengatur kecepatan transmisi data, jenis data yang dikirimkan, dan lain-lain. Untuk melakukan inisiasi, gunakan perintah `Serial.begin()` untuk mengaktifkan USART dan mengatur kecepatan transmisi data. Misalnya, jika ingin mengatur kecepatan transmisi data ke 9600 baud dapat menggunakan perintah `Serial.begin(9600)`. USART yang telah diaktifkan dapat digunakan untuk mengirimkan dan

menerima data via USB.

III. Pembahasan

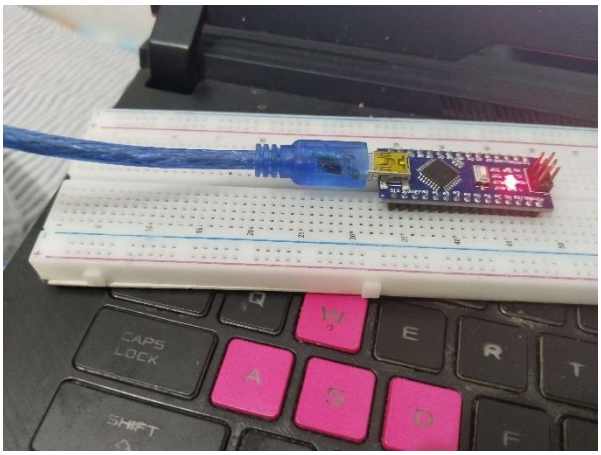
A. Perancangan Kode pada Arduino

Pada makalah ini penulis menggunakan Arduino Nano yang diprogram menggunakan Arduino IDE. Perancangan perangkat lunak untuk proses enkripsi-dekripsi dilakukan dengan Arduino IDE yang berbasiskan bahasa c++. Berikut adalah implementasi dari kode algoritma enkripsi ini:

```
String plaintext = "";
String ciphertext = "";
String decoded_ciphertext = "";
char x = '\0';
boolean state = false;

#define KEY '@'

void setup() {
  Serial.begin(9600);
  Serial.println("Selamat datang di Arduino Nano!");

}

void loop() {

  while(Serial.available()){
    x = Serial.read();
    plaintext += (char) x;

    if(x == '\n'){
      state = true;
      ciphertext += '\n';
      decoded_ciphertext += '\n';
    }
    else{
      ciphertext += (char) (x^KEY);
      decoded_ciphertext += (char) (((char) (x^KEY)) ^ KEY);
    }
  }

  if(state){
    Serial.println("plaintext string:");
    Serial.print(plaintext);
    Serial.println("ciphertext string:");
    Serial.print(ciphertext);
    Serial.println("decoded string:");
    Serial.print(decoded_ciphertext);

    plaintext = "";
    ciphertext = "";
    decoded_ciphertext = "";
    state = false;
  }
}
```

Pada kode di atas, penulis memanfaatkan operator Boolean XOR '^' sebagai operator utama dalam melakukan enkripsi pada plainteks yang penulis akan kirim melalui komputer. Selain itu, penulis menggunakan karakter '@' sebagai kunci enkripsi pada saat melakukan transmisi data. Tak hanya sebagai kunci enkripsi, dengan kunci yang sama dapat dilakukan dekripsi pada penggunaan XOR cipher.

B. Setup Piranti Keras



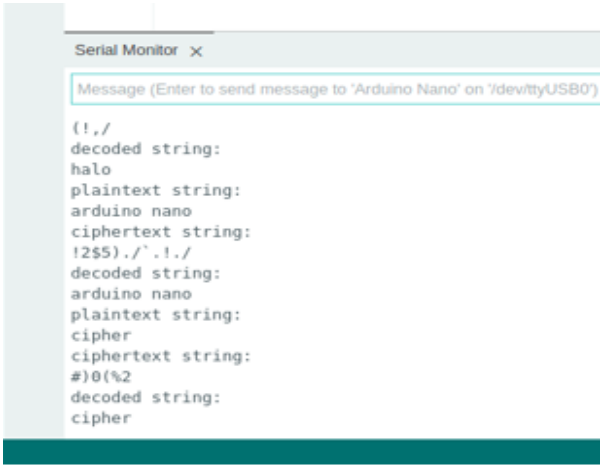
Gambar 12: Setup Arduino(sumber: dokumentasi pribadi)

Penulis memanfaatkan fitur USART yang dimiliki oleh Arduino Nano untuk melakukan komunikasi antara Arduino dan komputer. Dengan menggunakan kabel USB, komunikasi terjadi dua arah antara komputer dan Arduino Nano milik penulis.

C. Pengujian Enkripsi Data

Gambar 13: Hasil pengujian pertama(sumber: dokumentasi pribadi)

Pada pengujian pertama, penulis telah berhasil dalam melakukan enkripsi plainteks yang dikirimkan via komputer melalui UART. Tak lupa juga, penulis melakukan dekripsi balik, seperti yang terlihat pada kata “halo” di atas sana. Penulis juga akan melakukan uji lanjutan dengan Kembali menginput kata ‘cipher’.



Gambar 14: Hasil pengujian kedua(sumber: dokumentasi pribadi)

Pada pengujian kedua, setelah melakukan input kembali pada Arduino, didapatkan penulis berhasil menenkripsi dan mendekripsi plainteks yang penulis kirim sebelumnya.

Apabila kita meninjau string ‘cipher’, dapat kita jabarkan dalam bentuk biner sesuai kode ASCII masing-masing karakter sebagai berikut:

01100011	01101001	01110000	01101000	01100101	01110010
c	*i*	*p*	*h*	*e*	*r*

Dengan menggunakan karakter ‘@’ (dengan nilai ASCII 64) sebagai kunci enkripsi maupun dekripsi, berikut merupakan kalkulasi dari metode enkripsi yang dilakukan oleh program tersebut dengan menggunakan prinsip logika XOR.

01100011	01101001	01110000	01101000	01100101	01110010
01000000	01000000	01000000	01000000	01000000	01000000 ⊕
00100011	00101001	00110000	00101000	00100101	00110010
#	)	0	(	%	2

Untuk melakukan dekripsi kode, dilakukan operasi XOR kembali dari cipherteks dan kunci.

00100011	00101001	00110000	00101000	00100101	00110010
01000000	01000000	01000000	01000000	01000000	01000000 ⊕
01100011	01101001	01110000	01101000	01100101	01110010
c	*i*	*p*	*h*	*e*	*r*

D. Analisis hasil

Pada makalah ini penulis menggunakan Arduino Nano yang diprogram menggunakan Arduino IDE. Perancangan perangkat lunak untuk proses enkripsi-dekripsi dilakukan dengan Arduino IDE dengan menggunakan bahasa c++ sebagai bahasa pemrograman.

Enkripsi menggunakan XOR cipher terbilang cukup aman apabila implementasi perangkat pada skala kecil. Memang, algoritma kriptografi modern seperti RSA jauh lebih aman dan kompleks, namun bukan berarti XOR cipher tidak dapat digunakan sebagai sistem pengamanan dalam transmisi data. XOR cipher termasuk algoritma yang jauh lebih sederhana dibandingkan RSA, karena waktu komputasi pada mikrokontroler sendiri jauh lebih lambat dibandingkan pada komputer modern pada saat ini sehingga menggunakan algoritma yang jauh lebih kompleks dinilai kurang efisien.

Cara memecahkan XOR cipher akan mudah apabila kita dapat menemukan key-nya. Hal ini yang menjadi salah satu titik kelemahan dari XOR cipher. Namun, apabila memecahkan secara manual, diperlukan teknik *brute-force* untuk mencoba segala kemungkinan, dimana kompleksitas waktunya mencapai $O(2^n)$ karena pergantian tiap biner yang ada saat proses mengenkripsi pesan. Kompleksitas waktu yang bersifat eksponensial tergolong dalam algoritma yang pelan.

IV. KESIMPULAN

Perkembangan teknologi tak luput dari transmisi data yang perlu pengamanan data sebagai jaminan privasi pada masa kini. Penerapan kriptografi pada mikrokontroler menjamin baik pengguna maupun pengembang untuk semakin terjamin keamanan datanya. Dari sekian banyak algoritma Kriptografi, penulis memilih enskripsi menggunakan XOR cipher.

Penerapan algoritma enkripsi menggunakan XOR cipher merupakan salah satu penerapan salah satu subjek Matematika Diskrit, Aljabar Boolean, untuk diterapkan pada bidang kriptografi dan piranti cerdas(mikrokontroler). XOR cipher merupakan alternatif pilihan algoritma kriptografi yang cukup ampuh dan sederhana untuk mengamankan transmisi data pada mikrokontroler, khususnya Arduino, dari atau ke komputer maupun piranti berbasiskan mikrokontroler lainnya.

V. UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa yang telah memberikan karunia, sehingga penulis dapat

menyelesaikan makalah yang berjudul “Enkripsi Transmisi Data pada Mikrokontroler Arduino Menggunakan XOR Cipher Sederhana” yang selesai tepat pada waktunya. Tak lupa juga penulis mengucapkan terima kasih kepada Ibu Fariska Zakhralativa Ruskanda, S.T., M.T. sebagai dosen pengampu mata kuliah IF2120 Matematika Diskrit Kelas 2 atas bimbingan dan pengajaran yang telah dilakukan di kelas Matematika Diskrit ini. Penulis juga mengucapkan terima kasih kepada Bapak Dr. Ir. Rinaldi Munir, MT. sebagai salah satu dosen pengampu Matematika Diskrit yang memberikan referensi dan sumber pembelajaran Matematika Diskrit melalui situs beliau. Terakhir, penulis mengucapkan terima kasih kepada orang tua, keluarga, dan seluruh pihak yang membantu penulis dalam menyelesaikan makalah ini

REFERENSI

[1] Rinaldi Munir, “Aljabar Boolean (Bag. 1)”, https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Aljabar-Boolean-(2020)-bagian1.pdf, diakses 11 Desember 2022 pukul 21.00 .

[2] Rinaldi Munir, “Teori Bilangan (Bag. 3)”, https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian3.pdf, diakses 11 Desember 2022 pukul 21.00 .

[3] MA Budiman, JT Tarigan dan AS Winata, “Arduino UNO and Android Based Digital Lock Using Combination of Vigenere Cipher and XOR Cipher”, https://iopscience.iop.org/article/10.1088/1742-6596/1566/1/012074/pdf, diakses 11 Desember 2022 pukul 21.00 .

[4] https://docs.arduino.cc/hardware/nano, diakses 12 Desember 2022.

[5] https://litikd3tt.wordpress.com/2017/11/24/komunikasi-serial-uart-pada-arduino-uno/, diakses 12 Desember 2022.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 12 Desember 2022

Jeremya Dharmawan Raharjo
13521131