

Pengamanan Kunci Pintu Brankas Menggunakan Kriptografi One Time Pad (OTP) Berbasis Android

Munjiat Setiani Asih^{1*)}, Ade Zulkarnain Hasibuan²

^{1,2} Universitas Harapan Medan, Medan, Indonesia

¹munjiat.stth@gmail.com^{*)}, ²ade.stth@gmail.com

Abstrak— Brankas merupakan tempat yang digunakan untuk menyimpan benda-benda berharga. Pada umumnya brankas menggunakan tombol untuk membuka pintu brankas. Hanya saja penggunaan tombol yang hanya memasukkan password tersebut masih dianggap kurang aman. Oleh sebab itu dibuatlah sebuah alat yang dapat melakukan pengamanan pada password yang diinputkan. Alat yang dibuat menggunakan arduino sebagai pusat pemrosesan data yang diinputkan oleh pengguna dan smartphone android sebagai perangkat untuk memasukkan password. Pengamanan yang dilakukan menggunakan teknik kriptografi yaitu metode One Time Pad, pengguna diminta untuk menginput password yang akan digunakan. Saat proses penyimpanan password, password akan dienkripsi terlebih dahulu sebelum disimpan. Kemudian untuk menggunakannya pengguna cukup memasukkan password yang telah disimpan kedalam rangkaian. Jika perangkat dibobol paksa maka pencuri yang mencoba untuk mengambil password tersebut tidak akan dapat memahami password yang tersimpan didalam perangkat tersebut, hal ini disebabkan password sudah melalui proses enkripsi. Dengan adanya pengamanan ganda ini diharapkan brankas akan semakin aman.

Kata Kunci: Pintu Brankas, Kriptografi, One Time Pad, Arduino, Smartphone Android

Abstract— A safe is a place used to store valuable items. Generally, safes use buttons to open the door. However, using buttons that only require entering a password is considered less secure. Therefore, a device has been created to enhance the security of the entered password. The device utilizes Arduino as the central data processing unit for user input and an Android smartphone as the device for entering the password. The security is implemented using the cryptographic technique known as One Time Pad, where the user is prompted to input the password to be used. During the password storage process, the password is encrypted before being stored. To use it, the user simply enters the stored password into the system. If the device is forcefully tampered with, a thief attempting to retrieve the password will be unable to understand the stored password within the device, as it has undergone encryption. With this dual security measure in place, it is expected that the safe will be even more secure.

Keywords: Safe Door, Cryptography, One Time Pad, Arduino, Android Smartphone

1. PENDAHULUAN

Kemajuan teknologi, terutama dalam sistem keamanan berlapis pada pintu brankas, akan memberikan manfaat yang signifikan bagi keamanan barang berharga yang disimpan di dalamnya. Secara praktis, teknologi ini menjadi kebutuhan sekunder yang diterima baik secara personal maupun universal, memungkinkan pengguna untuk dengan mudah melaksanakan aktivitas di luar tanpa khawatir terhadap barang yang tertinggal di dalam brankas. Selain sebagai sistem keamanan, teknologi dalam lingkup ini juga dapat digunakan sebagai alat yang mempermudah aktivitas sehari-hari. Brankas merupakan tempat yang sering digunakan oleh banyak orang untuk menyimpan benda berharga yang dimiliki. Saat ini, ada dua model penguncian yang umum digunakan dalam brankas yang ada di pasaran, yaitu model penguncian yang harus diputar dan model penguncian menggunakan keypad sebagai perangkat untuk memasukkan kunci.

Penelitian yang dilakukan oleh Erlina Cahaya Setianingrum dan Bambang Eka Purnama dari Universitas Surakarta melibatkan pengembangan sistem mikrokontroler untuk keamanan brankas. Dalam sistem ini, ketika password yang dimasukkan benar, pintu brankas akan terbuka, dan jika password salah, pemilik brankas akan menerima pesan teks melalui ponsel. Namun, penelitian ini mengungkapkan kelemahan pada password yang digunakan, karena jika seseorang mengetahui password, mereka dapat mengakses sistem dengan mudah karena password yang digunakan selalu sama.[1]

Dengan berkembangnya teknologi, maka pengamanan pada pintu brankas juga dapat dikembangkan menjadi lebih baik dan lebih efektif lagi. Salah satunya dengan membuka brankas menggunakan teknologi mikrokontroler dan smartphone android. Mikrokontroler adalah chip atau IC (*Integrated Circuit*) yang bisa diprogram menggunakan komputer, yang terintegrasi dari sebuah sistem yang tertanam (*embedded system*) untuk melakukan satu atau lebih fungsi tertentu. Mikrokontroler di desain menggunakan teknologi CMOS (*Complementary Metal Oxide Semiconductor*), mikrokontroler Atmega328P merupakan kelompok keluarga AVR 8 bit yang memiliki feature harvard (pemisah memory kode program dan memory data, serta bekerja secara paralelisme). Tujuan menanamkan program pada mikrokontroler adalah agar rangkaian elektronik dapat membaca input, memproses input tersebut dan kemudian menghasilkan output sesuai yang diinginkan [2]. Mikrokontroler

memiliki jalur-jalur masukan (port masukan) serta jalur-jalur kelauran (port keluaran) yang memungkinkan mikrokontroler tersebut untuk bisa digunakan dalam aplikasi pembacaan data, pengontrolan serta penyajian informasi. Port masukan digunakan untuk memasukkan informasi atau data dari luar ke mikrokontroler. Contoh informasi yang dimasukkan ke mikrokontroler ini adalah informasi kondisi saklar yang dihubungkan ke kaki mikrokontroler, apakah sedang terbuka atau tertutup. Jalur masukan umumnya berupa jalur digital, dimana jalur ini digunakan oleh mikrokontroler untuk membaca keadaan digital (apakah logika 0 atau 1) yang diberikan oleh perangkat di luar mikrokontroler. Mikrokontroler tertentu berisikan ADC dengan sebagian dari jalur-jalur I/O-nya yang digunakan sebagai masukan analog. Jalur-jalur ini selanjutnya bisa digunakan untuk keperluan seperti pembacaan tegangan dari sensor suhu analog. Port keluaran digunakan untuk mengeluarkan data atau informasi dari mikrokontroler. Adanya port keluaran ini memungkinkan mikrokontroler untuk mengendalikan perangkat seperti LED, motor, relay dan menyajikan informasi melalui perangkat seperti seven-segment dan LCD. Untuk bisa bekerja, mikrokontroler perlu diberikan tegangan dari luar. Umumnya IC mikrokontroler dapat bekerja pada tegangan 5V, namun demikian, sebagian IC mikrokontroler seperti ATMEGA16L dapat dioperasikan dengan tegangan 3V [3].

Pada saat ini mikrokontroler sudah dikemas dalam berbagai macam platform untuk memudahkan penggunaannya, salah satu platform mikrokontroler yang populer digunakan dipasaran yaitu arduino. Arduino adalah papan pengendali mikro yang bersifat open source, dirancang untuk memudahkan pengguna elektronik dalam pembuatan berbagai proyek elektronik. Perangkat keras arduino menggunakan prosesor Atmel AVR dan memiliki perangkat lunak sendiri yang disebut sebagai arduino IDE. Arduino memiliki berbagai macam model, saat sekarang ini model yang paling sering digunakan di pasaran yaitu arduino uno. Dikutip dari website arduino.cc, arduino memiliki beberapa jenis produk yang dijual dipasaran terdiri dari papan utama, papan modul (memiliki bentuk lebih kecil), shields (elemen yang dapat dipasang ke papan untuk memberikan fungsi tambahan) dan kits. Arduino adalah nama keluarga papan mikrokontroler yang awalnya dibuat oleh perusahaan Smart Project. Salah satu tokoh penciptanya adalah Massimo Banzi. Papan ini merupakan perangkat keras bersifat "open source" sehingga boleh dibuat oleh siapa saja [4]. Arduino Uno memiliki 14 pin digital (6 pin dapat digunakan sebagai output PWM), 6 input analog, sebuah 16 MHz osilator kristal, sebuah koneksi USB, sebuah konektor sumber tegangan, sebuah header ICSP, dan sebuah tombol reset. Arduino Uno memuat segala hal yang dibutuhkan untuk mendukung sebuah mikrokontroler. Hanya dengan menghubungkannya ke sebuah komputer melalui USB atau memberikan tegangan DC dari baterai atau adaptor AC ke DC sudah dapat membuatnya bekerja. Arduino Uno menggunakan ATmega16U2 yang diprogram sebagai USB to serial converter untuk komunikasi serial ke komputer melalui port USB. "Uno" berarti satu di Italia dan diberi nama untuk menandai peluncuran Arduino 1.0. Versi 1.0 menjadi versi referensi Arduino ke depannya. Arduino Uno R3 adalah revisi terbaru dari serangkaian board Arduino, dan model referensi untuk platform Arduino [5].

Dengan memanfaatkan smartphone android pemilik brankas bisa langsung membuka brankas dengan mudah, hanya saja pengguna harus tetap memasukkan password untuk membuka brankas tersebut. Android merupakan sistem operasi dengan sumber terbuka, dan Google juga merilis kodenya di bawah Lisensi Apache. Kode dengan sumber terbuka dan juga lisensi perizinan pada Android, memungkinkan perangkat lunak dapat dimodifikasi secara bebas dan dapat didistribusikan dengan mudah. Android juga memiliki komunitas pengembang aplikasi yang memperluas fungsionalitas perangkat, umumnya ditulis dalam bahasa pemrograman Java. Andy Rubin, Chris White, dan Nick Sears merupakan pencipta android, yang awalnya mereka ingin menciptakan perangkat kamera digital. Kemudian dialihkan penggunaannya menjadi smartphone. Tahun 2007 android dirilis secara resmi oleh google yang telah membelinya pada tahun 2005 dengan suntikan dana 50 juta dolar. Setelah mendapat dana dari google, para pendiri android kemudian bergabung dengan google dan membuat sebuah prototipe. Pada tahun 2006, prototipe pertama yang dibuat yaitu Blackberry, yaitu smartphone yang memiliki keyboard. Setahun kemudian, perusahaan apple merilis smartphone dengan keyboard layar sentuh pertama, yaitu iPhone. Dengan demikian, google mulai mengembangkan smartphone yang dia miliki dengan menggunakan keyboard layar sentuh agar dapat menyaingi iPhone. Setelah lama bersaing, pada 2010 merupakan tahun dimana android pertama kalinya mengambil alih pangsa pasar yang sebelumnya diambil alih oleh apple. Mengapa apple bisa kalah dari android yaitu karena ketersediaan dan harga android yang murah membuat apple kalah dalam pasar smartphone. Selain itu android juga memiliki sistem operasi yang memiliki lisensi *open source*. Dengan itu banyak perusahaan smartphone yang bekerja sama dengan android. Android merupakan sistem yang berbasis linux yang dirancang untuk perangkat layar sentuh seperti smartphone dan komputer tablet [6].

Dalam penelitian yang dibuat menggunakan teknologi smartphone android dan arduino, cara kerja dari brankas ini ketika brankas dibuka secara paksa maka perangkat arduino yang terhubung pada brankas akan mengaktifkan buzzer. Buzzer adalah sebuah komponen elektronika yang berfungsi untuk mengubah getaran listrik menjadi getaran suara. Pada dasarnya prinsip kerja buzzer hampir sama dengan loud speaker, jadi buzzer juga terdiri dari kumparan yang terpasang pada diafragma dan kemudian kumparan tersebut dialiri arus sehingga menjadi elektromagnet, kumparan tadi akan tertarik ke dalam atau keluar, tergantung dari arah arus dan polaritas magnetnya, karena kumparan dipasang pada diafragma maka setiap gerakan kumparan akan menggerakkan diafragma secara bolak-balik sehingga membuat udara bergetar yang akan menghasilkan suara. Suara yang

dihasilkan tergolong sederhana yakni monofonik, berbeda dengan speaker yang dapat mengeluarkan suara yang lebih variatif (polifonik) [7]. Buzzer akan berbunyi terus menerus sebagai indikator peringatan bahwa terjadi pembobolan brankas tersebut. Arduino tidak dapat begitu saja mengetahui pintu brankas terbuka atau tidak, dibutuhkan sensor untuk memberikan masukan ke arduino agar arduino mengetahui informasi tersebut. Pada brankas yang dibuat pada penelitian ini digunakan sensor hall effect, sensor hall effect pada dasarnya terdiri dari potongan tipis semikonduktor yang bertipe P dengan bentuk persegi panjang. Bahan semikonduktor yang digunakan biasanya adalah gallium arsenide (GaAs), indium antimonide (InSb), indium phosphide (InP) atau indium arsenide (InAs). Potongan tipis semikonduktor tersebut dilewati oleh arus listrik secara berkesinambungan (terus-menerus). Ketika didekatkan dengan medan magnet atau ditempatkan pada lokasi yang bermedan magnet, garis fluks magnetik akan menggunakan gaya pada semikonduktor tersebut untuk mengalihkan muatan pembawa (elektron dan holes) ke kedua sisi pelat semikonduktor. Gerakan pembawa muatan ini merupakan hasil dari gaya magnet yang melewati semikonduktor tersebut [8].

Arduino dan smartphone akan saling berkomunikasi melalui jaringan bluetooth, Bluetooth adalah teknologi LAN nirkabel yang dirancang untuk menghubungkan perangkat berbagai fungsi seperti telepon, notebook, komputer (desktop dan laptop), kamera, printer, dan sebagainya. LAN Bluetooth bahkan dapat terhubung ke Internet jika salah satu gadget memiliki kemampuan ini. Jika ada banyak gadget yang mencoba terhubung, akan terjadi kekacauan. Teknologi bluetooth memiliki beberapa aplikasi. Perangkat periferal seperti mouse atau keyboard nirkabel dapat berkomunikasi dengan komputer melalui teknologi ini. Perangkat keamanan rumah dapat menggunakan teknologi ini untuk menghubungkan berbagai sensor ke pengontrol keamanan utama [9]. Arduino tidak mempunyai fasilitas komunikasi bluetooth, oleh karena itu arduino membutuhkan perangkat tambahan untuk dapat berkomunikasi dengan smartphone. Perangkat tambahan tersebut yaitu HC-05, Modul HC-05 mendukung komunikasi UART, USB serta SPI dan tergantung pada aplikasinya, pin yang diperlukan dapat digunakan. Modul bluetooth HC-05 dapat dikonfigurasi dalam dua mode operasi yaitu mode command dan mode data. Dalam mode command, anda dapat berkomunikasi dengan modul bluetooth melalui perintah AT untuk mengkonfigurasi berbagai pengaturan dan parameter modul seperti mendapatkan informasi firmware, mengubah UART baud rate, mengubah nama modul, mengaturnya sebagai master ataupun slave, dll [10].

Untuk mengunci pintu brankas dibutuhkan kunci elektrik yaitu solenoid door lock, Solenoid pengunci pintu adalah perangkat elektronik kunci pintu dengan menggunakan tegangan listrik sebagai pengendalinya. Alat ini banyak diaplikasikan pada pintu otomatis. Solenoid pengunci pintu bekerja jika diberi tegangan. Dalam keadaan normal tuas pada Solenoid pengunci pintu akan memanjang, dan jika diberi tegangan tuas pada alat ini akan memendek. Tegangan listrik yang diberikan akan membuat medan magnet sehingga tuas pada Solenoid pengunci pintu akan tertarik oleh medan magnet [11]. Solenoid ini mempunyai dua sistem kerja, yaitu *Normaly Close* (NC) dan *Normaly Open* (NO). Perbedaan cara kerja keduanya yaitu jika solenoid NC diberi tegangan, maka tuas pada solenoid akan memanjang (tertutup) sedangkan cara kerja dari Solenoid NO adalah kebalikan dari Solenoid NC. Kebanyakan solenoid Door Lock membutuhkan input atau tegangan kerja 12V DC tetapi ada juga solenoid Door Lock yang hanya membutuhkan input tegangan 5V DC sehingga dapat langsung bekerja dengan tegangan output dari pin IC digital [12].

Untuk menambah keamanan pada password yang digunakan maka dapat menggunakan teknik kriptografi. Algoritma kriptografi dibagi menjadi tiga bagian berdasarkan kunci yang dipakainya diantaranya yaitu algoritma simetris, algoritma asimetris, dan fungsi hash [13]. Salah satu metode yang dapat digunakan untuk mengamankan password brankas yaitu metode One Time Pad. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Namun, tidak semua aspek keamanan informasi ditangani oleh kriptografi. Enkripsi erat kaitannya dengan dekripsi, untuk itulah muncul istilah kriptanalisis. Kriptanalisis adalah ilmu dan seni untuk memecahkan informasi yang telah dienkripsi tanpa mengetahui kunci yang digunakan. Pelaku kriptanalisis disebut dengan kriptanalisis [14]. Kriptografi bagi kebanyakan orang adalah sesuatu yang sangat sulit dan kita sebagai pemula cenderung malas untuk mempelajarinya. Namun ada sebuah metode kriptografi yang agak mudah untuk dipelajari dan para ahlipun telah menyatakan bahwa metode ini merupakan metode kriptografi yang cukup aman untuk digunakan. Metode tersebut biasa dikenal dengan nama One Time Pad (OTP) atau yang lebih dikenal dengan sebutan Vernam Cipher. Vernam Cipher diciptakan oleh Mayor J. Maugborne dan G. Vernam pada tahun 1917. Algoritma One Time Pad (OTP) merupakan algoritma berjenis symmetric key yang artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama [15]. Sandi One Time Pad merupakan sandi yang mencapai kerahasiaan sempurna (perfect secrecy) yaitu menghasilkan teks sandi yang tidak memiliki hubungan statistik terhadap teks asli sehingga analisa statistik tidak dapat dilakukan. Sandi One Time Pad bekerja dengan menghasilkan kunci yang berbeda setiap karakternya untuk semua teks asli, kunci dibangkitkan secara acak dan deretan kunci digunakan hanya sekali saja.

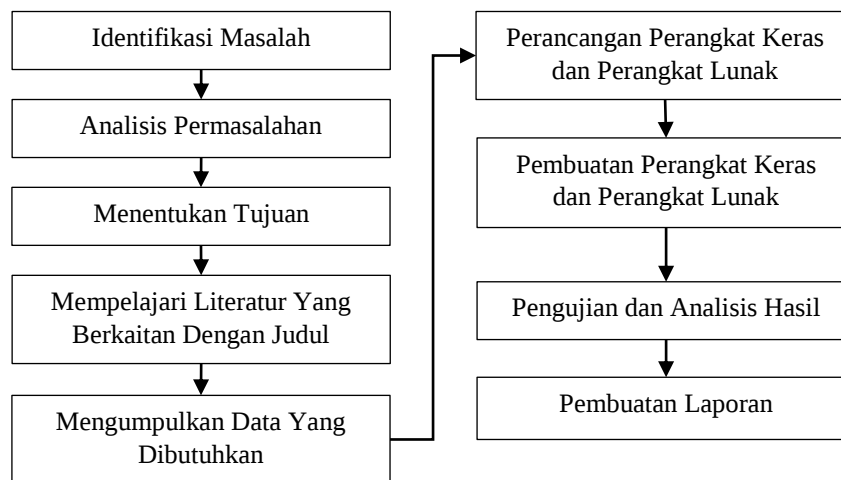
Aplikasi untuk smartphone Android dibuat menggunakan MIT App Inventor. MIT App Inventor adalah sebuah alat pemrograman berbasis blok yang dirancang untuk memungkinkan pemula memulai pemrograman dan membangun aplikasi untuk perangkat Android. Blok di sini merujuk pada kumpulan kode grafis yang disusun seperti puzzle, dengan berbagai komponen seperti Logika, Kontrol, Matematika, Teks, Daftar, Warna, Variabel,

dan Prosedur. MIT App Inventor dijalankan melalui layanan web dan awalnya dikembangkan oleh Profesor Hal Abelson dan tim dari Google Education saat Profesor Abelson sedang cuti panjang dari Google Inc. Kemudian, alat ini dikelola oleh staf Pusat Pembelajaran Seluler MIT bekerja sama dengan *Massachusetts Institute of Technology* (MIT), Program Studi Ilmu Komputer, dan Laboratorium Kecerdasan Buatan (CSAIL) [16]. Adapun tujuan dari penelitian yang dibuat yaitu untuk mengamankan pin pada penyimpanan brankas untuk menambah tingkat pengamanan dengan menggunakan algoritma one time pad dengan memanfaatkan smartphone android sebagai akses untuk membuka kunci brankas tersebut.

2. METODE PENELITIAN

2.1 Tahapan Penelitian

Dalam Penelitian yang dibuat terdapat beberapa tahapan yang harus dilakukan, adapun tahapan tersebut dapat dilihat pada gambar berikut:



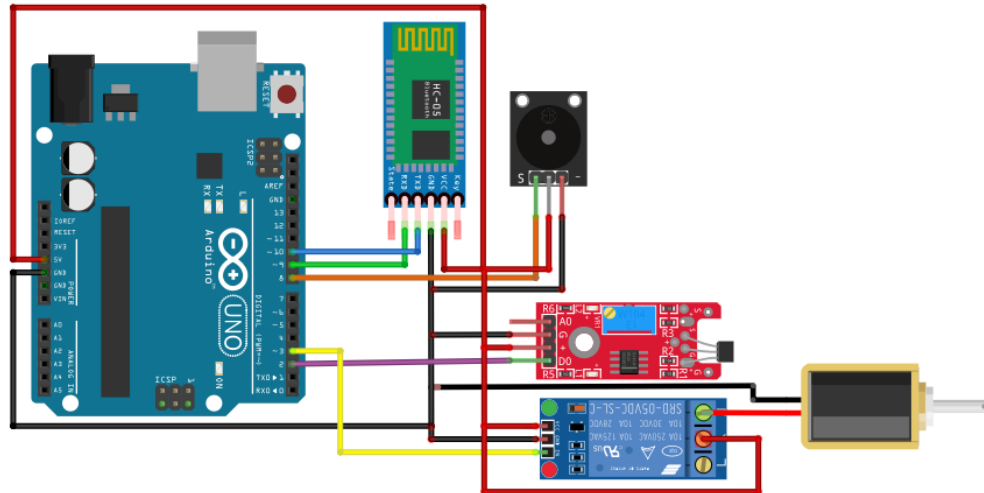
Gambar 1. Tahapan Penelitian

Penjelasan gambar 1 dapat diuraikan sebagai berikut:

1. Identifikasi masalah: tahap ini merupakan tahapan dimana peneliti melakukan identifikasi permasalahan yang ada
2. Analisis permasalahan: setelah dilakukan identifikasi masalah, selanjutnya dilakukan analisis terhadap masalah yang ada. Hal ini bertujuan untuk mendapatkan solusi dari masalah yang telah diidentifikasi
3. Menentukan tujuan: tahap ini merupakan tahap yang digunakan untuk menentukan tujuan dari penelitian yang dibuat
4. Mempelajari literatur yang berkaitan dengan judul: tahap ini dilakukan pengumpulan literatur seperti buku, jurnal, prosiding, dll. Kemudian seluruh literatur ini dipelajari untuk memperkuat teori yang ada untuk menyelesaikan permasalahan yang dihadapi
5. Mengumpulkan data: tahap ini digunakan untuk mengumpulkan seluruh data yang dibutuhkan ketika penelitian ini dilakukan, misalnya pada penelitian ini data yang akan dikumpulkan yaitu komponen-komponen yang akan digunakan dalam pembuatan perangkat, desain pemasangan perangkat ke pintu brankas, penerapan algoritma kriptografi One Time Pad pada perangkat dan data lainnya yang dibutuhkan selama penelitian
6. Perancangan Perangkat Keras dan Perangkat lunak: tahap ini merupakan tahap dimana peneliti mulai merancang perangkat keras untuk mengunci pintu brankas dan merancang perangkat lunak yang digunakan untuk memasukkan password brankas. Rancangan menggunakan perangkat lunak seperti fritzing, sketchup, app inventor dan perangkat lunak lainnya
7. Pembuatan Perangkat Keras dan Perangkat Lunak: tahap ini merupakan tahap dimana perangkat keras dan perangkat lunak mulai dibuat, diawali dari pembuatan/perakitan rangkaian, pembuatan program, pemasangan perangkat ke pintu, dan beberapa tahapan lainnya. Perangkat lunak yang dibuat dari sisi arduino dan dari sisi smartphone android. Algoritma One Time Pad akan dibuat di perangkat lunak smartphone android.
8. Pengujian dan Analisis Hasil: tahap ini merupakan tahap dimana dilakukan pengujian terhadap perangkat pengunci pintu dimana yang akan diuji yaitu kemampuan perangkat dalam mengunci pintu, analisis informasi yang dikirimkan oleh smartphone ke arduino dan beberapa variabel penilaian lainnya yang dibutuhkan dimana data tersebut nantinya digunakan untuk perbaikan perangkat pengunci pintu brankas
9. Pembuatan Laporan: tahap ini merupakan tahap akhir dari penelitian, dimana pada tahap ini disusun laporan dari penelitian yang telah dilakukan

2.2 Rancangan Rangkaian

Dalam pembuatan rangkaian sistem pengamanan brankas pada penelitian ini diperlukan rancangan rangkaian, rancangan rangkaian dibuat menggunakan *software* fritzing. Adapun rancangan rangkaian sistem pengamanan brankas dapat dilihat pada gambar 2.



Gambar 2. Rancangan Skema Rangkaian

Pada gambar 2 terlihat untuk menghubungkan arduino dengan smartphone dibutuhkan rangkaian HC-05 sebagai rangkaian perantara untuk komunikasi bluetooth. Rangkaian HC-05 merupakan rangkaian bluetooth yang dapat dijadikan sebagai master maupun slave. Dengan memanfaatkan rangkaian bluetooth HC-05 arduino dapat berkomunikasi dua arah dengan smartphone. Pin VCC pada bluetooth HC-05 dihubungkan ke pin 5V arduino, kemudian pin GND pada bluetooth HC-05 dihubungkan ke pin GND arduino. Selanjutnya pin TXD pada bluetooth HC-05 dihubungkan ke pin 10 arduino dan pin RXD pada bluetooth HC-05 dihubungkan dengan pin 9 arduino. Rancangan berikutnya yaitu rancangan skema buzzer, buzzer ini nantinya digunakan sebagai peringatan ketika pengguna mencoba mengunci pintu brankas sedangkan brankas masih dalam kondisi terbuka maka buzzer akan berbunyi sebanyak dua kali. Rangkaian buzzer ini terdiri dari tiga pin, pin VCC pada buzzer di hubungkan pada pin 5V pada arduino. Kemudian pin negatif (-) pada buzzer dihubungkan ke pin GND di arduino dan pin data (S) pada buzzer dihubungkan ke pin 8 pada arduino. Hall sensor digunakan untuk membaca medan magnet disekitarnya. Tujuan penggunaan hall sensor ini agar rangkaian mendapatkan informasi apakah pintu brankas dalam kondisi terbuka atau tertutup, informasi ini nantinya akan dikirimkan ke smartphone pengguna. Hall sensor memiliki empat pin yaitu pin VCC, GND, A0 dan D0, pin A0 digunakan untuk membaca sinyal masukan berupa sinyal analog sedangkan pin D0 digunakan untuk membaca sinyal masukan berupa sinyal digital. Dalam penelitian ini pin yang digunakan hanya tiga pin yaitu pin VCC, GND dan D0. Pin VCC pada hall sensor dihubungkan ke pin 5V arduino dan pin GND pada hall sensor dihubungkan ke pin GND pada arduino. Selanjutnya pin D0 pada hall sensor dihubungkan ke pin dua pada arduino. Dalam pembuatan alat digunakan magnet jenis neodymium sebagai pemicu agar hall sensor mendeteksi adanya medan magnet.

Rancangan selanjutnya yaitu rancangan skema relay dan solenoid door lock, solenoid door lock tidak dapat dikendalikan langsung oleh arduino uno. Oleh sebab itu dibutuhkan rangkaian tambahan untuk menjalankan solenoid door lock tersebut, rangkaian yang digunakan sebagai pengendalinya yaitu modul relay. Pada modul relay terdapat tiga pin, dimana pin VCC pada relay dihubungkan ke pin 5V arduino dan pin GND pada relay dihubungkan ke pin GND pada arduino. Selanjutnya pin IN pada relay dihubungkan pada pin 3 arduino. Solenoid door lock memiliki dua kabel yaitu kabel positif dan kabel negatif, kabel positif pada solenoid door lock dihubungkan ke terminal normally open (NO) pada relay, kemudian terminal COM pada relay dihubungkan ke tegangan sumber (VCC). Kabel negatif pada solenoid door lock dihubungkan ke sumber tegangan yang memberikan titik referensi nol (GND). Solenoid door lock akan bekerja ketika relay aktif, dimana tuas pada solenoid door lock akan ditarik kedalam sehingga tuas akan memendek, sedangkan jika solenoid door lock tidak diberikan tegangan maka tuas pada solenoid door lock akan memanjang.

2.3 Analisa Kriptografi One Time Pad

Sebelum membuat program kriptografi one time pad, terlebih dahulu dilakukan analisa algoritma kriptografi ini. Algoritma kriptografi one time pad akan dijalankan di smartphone, ketika password yang dimasukkan benar maka smartphone akan memberikan instruksi ke arduino untuk mengunci ataupun membuka kunci brankas. Pertama

sekali dibuat tabel karakter yang akan digunakan dalam proses enkripsi dan dekripsi menggunakan algoritma one time pad. Adapun tabel karakter tersebut sebagai berikut.

Tabel 1. Karakter

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
R	S	T	U	V	W	X	Y	Z	a	b	c	d	e	f	g	h
34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y
51	52	53	54	55	56	57	58	59	60	61	62					
z	0	1	2	3	4	5	6	7	8	9	spasi					

Pada tabel 1 terdapat 63 karakter yang dapat diproses untuk enkripsi maupun dekripsi. Algoritma One Time Pad dapat dirumuskan sebagai berikut:

$$C_i = E(p_i) = (p_i + k_i) \bmod n \quad (1)$$

Dimana:

C_i = Cipherteks

$E(p_i)$ = Enkripsi plainteks

p_i = Plainteks

k_i = Kunci

n = jumlah karakter yang dapat di enkripsi/dekripsi

Proses dekripsi One Time Pad dapat dirumuskan sebagai berikut

$$P_i = D(C_i) = (C_i - k_i) \bmod n \quad (2)$$

Dimana:

C_i = Cipherteks

$D(C_i)$ = Dekripsi cipherteks

C_i = Cipherteks

k_i = Kunci

n = jumlah karakter yang dapat di enkripsi/dekripsi

Untuk contoh perhitungan algoritma kriptografi one time pad dapat dilihat sebagai berikut:

Plainteks: Kriptografi

Kunci: UnHar

Dari kasus diatas diperoleh panjang kunci lebih kecil dari panjang plainteks, oleh karena itu ulangi kunci sepanjang plainteks. Hasil perulangan kunci dapat dilihat sebagai berikut.

Kunci: UnHarUnHarU

Selanjutnya dilakukan proses enkripsi terhadap plainteks, proses enkripsi dapat dilihat sebagai berikut:

$$C_1 = (K+U) \bmod 63 = (10+20) \bmod 63 = 30 \bmod 63 = 30 = e$$

$$C_2 = (r+n) \bmod 63 = (43+39) \bmod 63 = 82 \bmod 63 = 19 = T$$

$$C_3 = (i+H) \bmod 63 = (34+7) \bmod 63 = 41 \bmod 63 = 41 = p$$

$$C_4 = (p+a) \bmod 63 = (41+26) \bmod 63 = 67 \bmod 63 = 4 = E$$

$$C_5 = (t+r) \bmod 63 = (45+43) \bmod 63 = 88 \bmod 63 = 25 = Z$$

$$C_6 = (o+U) \bmod 63 = (40+20) \bmod 63 = 60 \bmod 63 = 60 = 8$$

$$C_7 = (g+n) \bmod 63 = (32+39) \bmod 63 = 71 \bmod 63 = 8 = I$$

$$C_8 = (r+H) \bmod 63 = (43+7) \bmod 63 = 50 \bmod 63 = 50 = y$$

$$C_9 = (a+a) \bmod 63 = (26+26) \bmod 63 = 52 \bmod 63 = 52 = 0$$

$$C_{10} = (f+r) \bmod 63 = (31+43) \bmod 63 = 74 \bmod 63 = 11 = L$$

$$C_{11} = (i+U) \bmod 63 = (34+20) \bmod 63 = 54 \bmod 63 = 54 = 2$$

Setelah dilakukan proses enkripsi diperoleh cipherteks yaitu "eTpEZ8Iy0L2". Untuk mengembalikan cipherteks menjadi plainteks dilakukan proses dekripsi, adapun proses dekripsi tersebut dapat dilihat sebagai berikut.

$$P_1 = (e-U) \bmod 63 = (30-20) \bmod 63 = 10 \bmod 63 = 10 = K$$

$$P_2 = (T-n) \bmod 63 = (19-39) \bmod 63 = -20 \bmod 63 = 43 = r$$

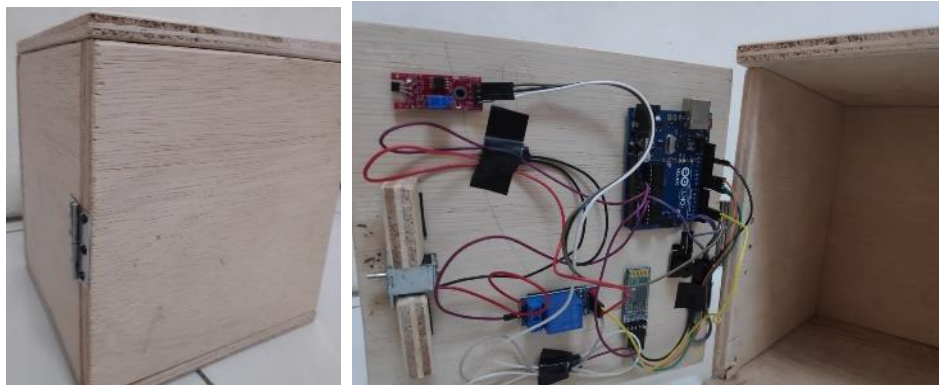
$$P_3 = (p-H) \bmod 63 = (41-7) \bmod 63 = 34 \bmod 63 = 34 = i$$

$P_4 = (E-a) \bmod 63 = (4-26) \bmod 63 = -22 \bmod 63 = 41 = p$
 $P_5 = (Z-r) \bmod 63 = (25-43) \bmod 63 = -18 \bmod 63 = 45 = t$
 $P_6 = (8-U) \bmod 63 = (60-20) \bmod 63 = 40 \bmod 63 = 40 = o$
 $P_7 = (I-n) \bmod 63 = (8-39) \bmod 63 = -31 \bmod 63 = 32 = g$
 $P_8 = (y-H) \bmod 63 = (50-7) \bmod 63 = 43 \bmod 63 = 43 = r$
 $P_9 = (0-a) \bmod 63 = (52-26) \bmod 63 = 26 \bmod 63 = 26 = a$
 $P_{10} = (L-r) \bmod 63 = (11-43) \bmod 63 = -32 \bmod 63 = 31 = f$
 $P_{11} = (2-U) \bmod 63 = (54-20) \bmod 63 = 34 \bmod 63 = 34 = i$

Setelah dilakukan proses dekripsi diperoleh plainteks “Kriptografi”, hasil dekripsi ini sesuai dengan teks asli yang sebelum proses enkripsi.

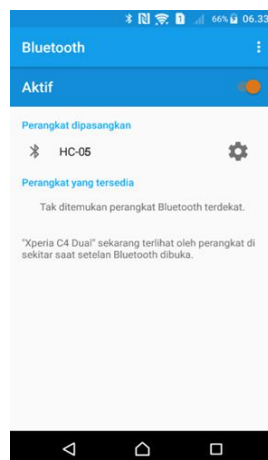
3. HASIL DAN PEMBAHASAN

Tahapan berikutnya yaitu implementasi terhadap alat yang telah dibuat, pertama sekali aktifkan alat pengunci dan membuka kunci pintu brankas dengan menghubungkan alat tersebut dengan sumber tegangan baik adaptor ataupun baterai.



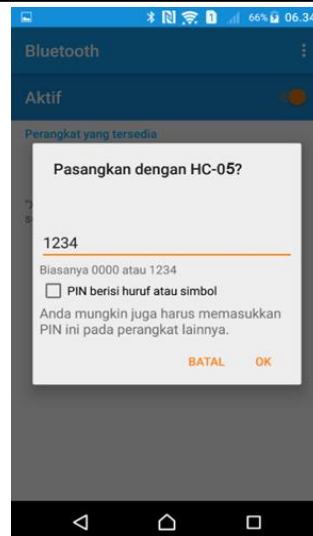
Gambar 3. Prototype Brankas

Gambar 3 sebelah kiri merupakan gambar dari hasil prototype brankas, gambar sebelah kanannya menampilkan rangkaian dari alat yang digunakan untuk mengunci dan menutup kunci brankas, serta melakukan komunikasi ke smartphone untuk mengirim dan menerima password yang di masukkan dari smartphone. Setelah perangkat hidup langkah selanjutnya aktifkan bluetooth di smartphone, cari nama perangkat HC-05 seperti yang terlihat pada gambar 4.



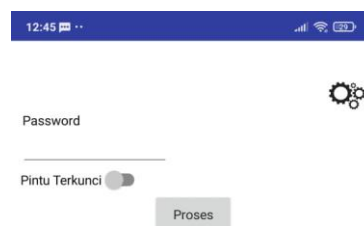
Gambar 4. Pairing Smartphone dengan Alat

Langkah selanjutnya yaitu klik HC-05 kemudian akan muncul jendela dimana perangkat meminta pin bluetooth. Masukkan angka “1234” kemudian tekan tombol “OK” untuk melanjutkan proses pairing seperti yang terlihat pada gambar 5.



Gambar 5. Pemasangan Pin Bluetooth

Setelah proses pairing berhasil, langkah selanjutnya membuka aplikasi pengendalinya di smartphone. Buka aplikasi dengan nama "One Time Pad". Jika proses pairing berhasil maka aplikasi akan tampil seperti yang terlihat pada gambar 6.



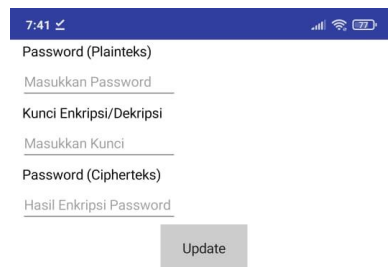
Gambar 6. Tampilan Utama

Ketika pertama kali menjalankan aplikasi, pengguna tidak dapat langsung memasukkan password. Jika pengguna memasukkan password dan menekan tombol "Proses" maka akan muncul pesan seperti yang terlihat pada gambar 7.



Gambar 7. Pesan Pengaturan Awal

Pada gambar 7 menunjukkan pesan bahwa pengguna diminta untuk masuk ke jendela pengaturan. Untuk masuk ke jendela pengaturan pengguna harus menekan tombol gear yang terletak di sebelah kanan atas. Kemudian pengguna akan diarahkan ke halaman pengaturan seperti yang terlihat pada gambar berikut.



7:41

Password (Plainteks)

Masukkan Password

Kunci Enkripsi/Dekripsi

Masukkan Kunci

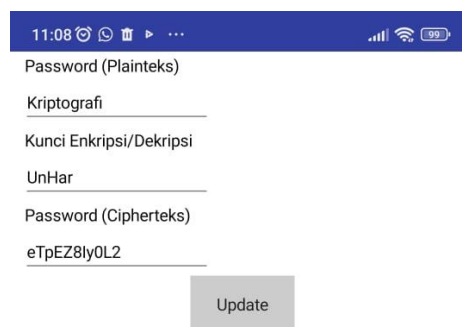
Password (Cipherteks)

Hasil Enkripsi Password

Update

Gambar 8. Halaman Pengaturan

Pada gambar 8 pengguna diminta untuk memasukkan password untuk membuka dan menutup kunci brankas, kemudian pengguna juga diminta untuk memasukkan kunci untuk proses enkripsi dan dekripsi. Selanjutnya tekan tombol “Update”.



11:08

Password (Plainteks)

Kriptografi

Kunci Enkripsi/Dekripsi

UnHar

Password (Cipherteks)

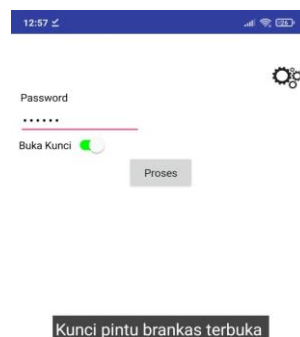
eTpEZ8ly0L2

Update

S

Gambar 9. Proses Enkripsi Kunci

Proses enkripsi dan dekripsi password berada pada tampilan pengaturan ini seperti yang terlihat pada gambar 9, ketika pengguna memasukkan password (plainteks) dan kunci yang digunakan untuk enkripsi/dekripsi, selanjutnya untuk melihat hasil proses enkripsi menggunakan algoritma one time pad pengguna harus menekan tombol “Update”, selain untuk melakukan proses pengamanan menggunakan algoritma one time pad tombol ini juga digunakan untuk menyimpan password yang telah di enkripsi.



12:57

Password

Buka Kunci

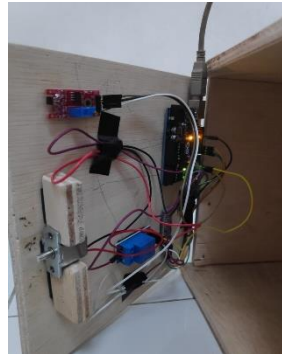
Proses

Kunci pintu brankas terbuka

Gambar 10. Pesan Proses Penguncian/Membuka Kunci Brankas

Setelah itu pengguna akan diarahkan kembali ke tampilan utama seperti yang terlihat pada gambar 10, disini pengguna sudah dapat mengunci dan membuka kunci pintu brankas. Jika pengguna menekan tombol “Proses” sebelum memasukkan password maka akan muncul pesan agar pengguna memasukkan password terlebih dahulu.

Untuk membuka kunci ataupun mengunci pintu brankas pengguna terlebih dahulu harus memasukkan password, selanjutnya pengguna harus menggeser tombol switch sesuai kebutuhan (kunci atau buka kunci). Kemudian langkah terakhir yaitu tekan tombol “Proses”, jika proses pengiriman instruksi melalui bluetooth berhasil maka akan muncul pesan “Kunci pintu brankas terbuka”.



Gambar 11. Pintu Brankas Terbuka

Jika proses berhasil maka solenoid pada alat akan ditarik dan pintu brankas dapat dibuka seperti yang terlihat pada gambar 11. Jika pengguna mengirimkan instruksi untuk membuka kunci brankas dan ternyata pintu brankas tidak terkunci maka buzzer akan berbunyi sebanyak dua kali, hal ini menandakan pintu brankas sudah terbuka.

4. KESIMPULAN

Kriptografi one time pad diterapkan di smartphone untuk mengamankan password brankas, proses enkripsi dan dekripsi dilakukan melalui smartphone. Ketika pengguna pertama kali menjalankan aplikasi, disini aplikasi meminta pengguna untuk memasukkan password (plaintexts) dan kunci untuk dilakukan proses enkripsi yang nantinya hasil enkripsi akan disimpan di dalam smartphone. Ketika pengguna memasukkan password yang benar, aplikasi yang terdapat di smartphone akan mengirimkan instruksi untuk membuka/mengunci pintu brankas melalui jaringan bluetooth yang terhubung ke alat. Selanjutnya alat akan mengerjakan instruksi yang diberikan untuk mengunci maupun membuka kunci pintu brankas.

UCAPAN TERIMA KASIH

Terima kasih disampaikan kepada Universitas Harapan Medan yang telah mendukung terlaksananya penelitian ini.

REFERENCES

- [1] E. C. Setianingrum and B. E. Purnama, “SISTEM PENGAMAN BRANKAS DENGAN MENGGUNAKAN HANDPHONE BERBASIS MIKROKONTROLER AT89S51,” in *Seminar Riset Unggulan Nasional Informatika dan Komputer FTI UNSA*, 2013, pp. 1–7.
- [2] A. Z. Hasibuan, H. Harahap, and Z. Sarumaha, “Penerapan Teknologi RFID Untuk Pengendalian Ruang Kelas Berbasis Mikrokontroler,” *Jutikomp*, vol. 1, no. 1, pp. 71–77, 2019.
- [3] H. A. Dharmawan, *Mikrokontroler Konsep Dasar dan Praktis*. Malang: UB Press, 2017.
- [4] M. S. Asih, A. Z. Hasibuan, and N. I. Syahputri, “Pendingin Otomatis Akuarium Menggunakan Mikrokontroler,” *Jutikomp*, vol. 1, no. 1, pp. 66–70, 2019.
- [5] M. A. Basith, “Penerapan Sensor Ultrasonik HC-SR04 pada Sistem Pengukuran Volume pada Mobil Tangki Air Bersih,” *Politeknik Negeri Sriwijaya*.
- [6] S. F. Pane, I. H. Hardy, and E. C. Sujadi, *Pengembangan Smart Conveyor Dengan Arduino (Menggunakan GPS Tracking Berbasis Android)*. Bandung: Buku Pedia, 2022.
- [7] Y. D. Shandy, A. Rakhmatsyah, and N. A. Suwastika, “No Title,” in *e-Proceeding of Engineering*, 2015, pp. 6395–6407.
- [8] D. Kho, “Pengertian Sensor Efek Hall (Hall Effect Sensor) dan Prinsip Kerjanya,” 2022. .
- [9] J. Al Amien, H. Mukhtar, and E. Arribe, *Komunikasi Data*. Yogyakarta: DEEPUBLISH, 2021.
- [10] A. Nugroho, K. E. Susilo, S. Winardi, and A. Budijanto, *Buku Petunjuk Praktikum Mikrokontroler Arduino*. Surabaya:



-
- Scopindo, 2020.
- [11] A. Apriansyah, Ilhamsyah, and T. Rismawan, "Prototype Kunci Otomatis Pada Pintu Berdasarkan Suara Pengguna Menggunakan Metode KNN (K-Nearest Neighbor)," *J. Coding, Sist. Komput. Untan*, vol. 4, no. 1, pp. 45–56, 2016.
 - [12] S. Octaviany, "Rancang Bangun Feeder Machine Berbasis KTP Elektronik," Pancabudi, 2020.
 - [13] Y. P. Wiranto, "Perancangan Aplikasi Kriptografi DES dan RSA Sebagai Media Belajar Kriptografi Berbasis Mobile," Amikom, 2014.
 - [14] H. Kurniadi, "Implementasi Algoritma Kriptografi Elgamal Untuk File Citra 2 Dimensi," Universitas Brawijaya, Malang, 2015.
 - [15] M. Sholeh and J. V Hamokwarong, "Aplikasi Kriptografi Dengan Metode Vernam Cipher Dan Metode Permutasi Biner," *Momentum*, vol. 7, no. 2, pp. 8–13, 2011.
 - [16] A. Suharto, *Tutorial Mudah Membuat Aplikasi Android dengan MIT App Inventor (AI2)*. Indramayu: Indramayu, 2021.