IMPLEMENTASI TWO FACTOR AUTHENTICATION DAN ALGORITMA RSA SEBAGAI METODE AUTENTIKASI LOGIN PADA SI-ABKA (SISTEM AMAL BAKTI KEMENTERIAN AGAMA)

PROPOSAL SKRIPSI

diajukan guna memenuhi salah satu syarat
untuk melaksanakan seminar proposal

oleh

Ahmad Choirul Mustaqim

NIM 152410101155

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER

UNIVERSITAS JEMBER

2019

A. Judul

"Implementasi Two Factor Authentication Dan Algoritma RSA Sebagai Metode Autentikasi Login Pada Si-Abka (Sistem Amal Bakti Kementerian Agama)"

B. Latar Belakang

Di era teknologi internet sekarang ini, semua informasi dapat dikirim dengan bebas melalui suatu jaringan dengan tingkat keamanan yang rentan dan memungkinkan terjadinya penyadapan suatu informasi. Hal tersebut secara langsung maupun tidak langsung mempengaruhi sistem perdagangan, transaksi, bisnis, perbankan, industri dan pemerintahan yang umumnya mengandung informasi rahasia. Keamanan data saat ini sangat penting mulai dari mengamankan data yang disimpan sampai data yang dikirim. Data yang bersifat rahasia perlu dibuatkan suatu sistem penyimpanan dan pemrosesan khusus agar data tersebut tidak mudah di baca atau diubah oleh pihak yang tidak berwenang.

Berbagai hal telah dilakukan untuk mendapatkan jaminan keamanan informasi rahasia. Faktor utama yang harus dipenuhi dalam mengamankan data rahasia adalah tingkat keamanan teknologi informasi yang tinggi. Data tidak hanya berupa file atau text, login ke dalam suatu sistem perlu di enkripsi agar hanya orang yang memiliki akses yang dapat masuk ke dalam sistem.

Proses autentikasi pada prinsipnya berfungsi sebagai kesempatan user dan pemberi layanan dalam proses pengaksesan resource. User harus mampu memberikan informasi yang dibutuhkan pemberi layanan untuk berhak mendapatkan resourcenya. Sedangkan pihak pemberi layanan harus mampu menjamin bahwa pihak yang tidak berhak tidak akan dapat mengakses resource ini (Khairina 2011). Jika seseorang sudah mengetahui password kita ,maka akun tersebut mudah sekali disalah gunakan tanpa sepengatahuan pemilik aslinya.

Salah satu cara yang digunakan adalah dengan menyandikan isi informasi menjadi suatu kode-kode yang tidak dimengerti sehingga penyadap akan kesulitan untuk mengetahui isi informasi yang sebenarnya. Dari masalah tersebut perlu adanya suatu metode login yang dapat mengamankan akun dari adanya percobaan pembobolan. Salah satu sistem yang memerlukan pengamana ekstra antara lain

sistem perbankan, karena perbankan menyimpan banyak data nasabah dan data transaksi sampai data keuangan yang rentan terhadap perubahan sekecil apapun.

SI-Abka (sistem amal bakti kementerian agama jember) merupakan sistem yang mengelola data koperasi dari seluruh anggota yang bekerja dibawah instansi kementerian agama jember. Sistem ini berfungsi sebagai pengelola data mulai dari data anggota, data simpanan, sampai data pinjaman. Data-data tersebut sangat rentan terhadapa perubahan karena menyangkut keuangan nasabah dan koperasi. Saat ini SI-Abka hanya menggunakan username dan password untuk metode autentikasi nya. Penggunaan username dan password rentan terhadap pembobolan, sehingga perlu adanya teknologi tambahan untuk meningkatkan keamanan saat melakukan otentikasi ke sistem. Teknologi yang dibutuhkan yaitu OTP (one time password).

Proses login yang sebelumnnya hanya mengandalkan username dan password akan ditambah dengan memasukan kode OTP. Proses tersebut dinamakan two factor authentication, yaitu menggunakan kode OTP sebagai pengaman tambahan (Sudiarto Raharjo, E.K. Ratri, dan Susilo 2017). Kode OTP ini otomastis generate sesuai dengan waktu dan parameter tertentu dan dapat di akses dengan menggunakan aplikasi android, sms, atau hardware khusus. Kelebihan OTP berbasis waktu adalah tidak mengandalkan server saat pembangkitan kode otp sehingga meminimalisir adanya kode otp yang lama tersampaikan dan tidak perlu adanya penyimpanan kode OTP ke dalam database.

Proses pembangkitan kode otp juga menggunakan algoritma RSA sehingga hasil pembangkitan kode otp sangat susah di prediksi dan bersifat sangat random. Algoritma RSA juga berjalan di dua sisi yaitu di sisi server dan sisi hardware client yang berupa android. Kode OTP berbasis waktu memiliki pola tersendiri dan jika terdapat orang yang berniat jahat dan mengetahui pola tersebut maka rawan akan terjadinya pembobolan. Oleh karena itu terdapat algoritma RSA yang akan mengenkripsi kode OTP sehingga data yang ditampilkan bukan kodenya secara langsung.

C. Rumusan Masalah

Berdasarkan latar belakang masalah penelitian, maka muncul perumusan masalah sebagai berikut.

1. Seberapa besar dampak keamanan menggunakan kode OTP dan algoritma RSA untuk login kedalam sistem ?
2. Apa saja *resource* yang digunakan untuk pengimplemetasian Two Factor Authentication dalam sistem SI-Abka?

D. Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Mengimplementasikan Two Factor Authentication ke dalam sistem SI-Abka
2. Meningkatkan keamanan transaksi pada SI-Abka dengan menggunakan *two factor authentication.*

E. Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Bagi Akademis

   Penelitian yang dilakukan diharapkan memberikan hasil yang mampu memberikan masukan informasi yang terkait dengan judul penelitian kepada pembaca pada umumnya dan pada Program Studi Sistem Informasi Universitas Jember pada khususnya.
2. Bagi Peneliti

   Mengimplementasikan two factor autenticatio di SI-abka dan menerapkan ilmu yang didapatkan ke dalam dunia kerja.
3. Bagi Objek Penelitian

   Menambahakan metode autentikasi agar lebih aman dalam bertransaksi di SI-Abka.

F. Batasan Masalah

Peneliti memberikan batasan masalah untuk objek dan tema yang dibahas sehingga tidak terjadi penyimpangan dalam proses penelitian dan menganalisis

1. Bahasa pemrograman yang digunakan adalah PHP unruk sistem SI-Abka dan java android untuk membangkitkan kode otp.
2. Algoritma kriptografi yang di gunakan adalah RSA.
3. Nasabah dapat mengoperasikan android.
4. Tahapan testing menggunakan teknik brute force terhadap token TOTP

G. Tinjauan Pustaka

Pada bagian ini dipaparkan tinjauan yang berkaitan dengan masalah yang dibahas, serta kajian teori yang dikaitkan dengan permasalahan yang dihadapi. Teori yang di dapatkan berupa pembangkitan OTP dan penerapanya yang dapat membantu peneliti dalam penelitian ini. Selain pembangkitan OTP penulis juga memelajari algoritma RSA. Perhitungan yang di dapatkan akan membantu peneliti dalam menghitung kode OTP yang akan di generate secara berkala oleh server dan client. Hasil perhitungan akan di proses oleh client dan server yang akan digunakan untuk proses autentikasi OTP di sistem SI-ABKA.

G.1 Password dan username

G.1.1 Password

Password atau kata sandi dapat digunakan untuk layanan otentikasi, yaitu layanan yang berhubungan identifikasi, baik mengidentifikasi kebenaran pihak – pihak yang berkomunikasi (user authentication atau entity authentication) maupun mengidentifikasi kebenaran sumber pesan. Otentikasi sumber pesan secara benar memberikan kepastian integritas data (Inayatullah 2007). Password bersifat statis atau sama, maksud statis disini adalah nilai atau values dari password tersebut sama dengan password sebelumnya hingga user menggantinya. Biasanya user mengganti password ketika sudah merasa bahwa akun dia sudah tidak aman atau sudah diketahui oleh orang lain.

G.1.2 Otentikasi

Password Menurut Rizka Putra Mustofa (Mustofa 2003) bahwa otentikasi (Authentication) adalah proses untuk memastikan bahwa kedua ujung koneksi dalam keadaan benar atau sama. Seperti password pada umumnya, syarat agar otentikasi berhasil adalah password yang dikirimkan client harus sama dengan

password yang disimpan di server. Dengan alasan keamanan jarang sekali server menyimpan password user dalam bentuk plain text. Biasanya server menyimpan password user dalam bentuk hash sehingga tidak bisa dikembalikan dalam bentuk plain text. Jadi syarat otentikasi berhasil di atas bisa diartikan sebagai hasil penghitungan hash dari passwordyang dikirim klien harus sama dengan nilai hash yang disimpan dalam server.

G.2 *One Time Password*

Dikutip dari (Musliyana, Arif, dan Munadi 2016) bahwa One Time Password (OTP) merupakan metode otentikasi yang menggunakan password yang selalu berubah setelah setiap kali login, atau berubah setiap interval waktu tertentu. One-time password ini haruslah password yang acak sehingga sulit ditebak oleh orang lain. Keuntungan dari one time password adalah pencegahan penyalahgunaan username dan password yang biasanya statis. Dengan tambahan one-time password ini maka login tidak bisa ditiru oleh orang lain. Keuntungan ini berarti jika berhasil seorang mendapatkan username dan password, maka tidak dapat digunakan karena dia harus memasukkan one-time password yang lain.

G.3 *Time-Based OTP*

OTP jenis ini berbasis sinkronisasi waktu yang berubah secara konstan pada setiap satuan interval waktu tertentu. Proses ini memerlukan sinkronisasi antara token milik client dengan server otentikasi. Pada jenis token yang terpisah (disconnected token), sinkronisasi waktu dilakukan sebelum token diberikan kepada client (Kim dkk. 2009). Tipe token lainnya melakukan sinkronisasi saat token dimasukkan dalam suatu alat input.

Di dalam token terdapat sebuah jam akurat yang telah disinkronisasikan dengan waktu yang terdapat pada server otentikasi. Pada sistem OTP ini, waktu merupakan bagian yang penting dari algoritma password, karena pembangkitan password baru didasarkan pada waktu dan kunci rahasia saat itu dan bukan pada password sebelumnya .

Pada OTP jenis ini sudah mulai diimplementasikan terutama pada remote Virtual Private Network (VPN), dan keamanan jaringan Wi-Fi dan juga pada berbagai aplikasi Electronic Commerce (E-commerce). Ukuran standar

penggunaan waktu pada algoritma ini adalah 30 detik (M'Raihi dkk. 2011). Nilai ini dipilih sebagai keseimbangan antara keamanan dan kegunaan. Pada penelitian ini, OTP yang digunakan berbasis sinkronisasi waktu dengan kombinasi Algoritma RSA.

G.4 *Algoritma RSA*

Rivest Shamir Adleman (RSA) adalah salah satu algoritma kriptografi asimetris (kriptografi kunci - publik) yaitu menggunakan dua kunci yang berbeda (private key dan public key). Kekuatan algoritma RSA tidak hanya terletak pada panjang kuncinya (semakin panjang kunci, maka semakin lama waktu kerja) dan penggunaan kunci - publik dan kunci privat pada umumnya (Muchlis, Budiman, dan Rachmawati 2007). Algoritma ini membantu dalam pembangkitan kode OTP agar lebih aman dan tidak mudah di tebak. Pembangkitan OTP dibangun berdasarkan algoritma tersendiri jika algoritma tersebut diketahui maka kode OTP sangat mudah di ketahui, oleh karena itu dibutuhkan algoritma kriptografi agar hasil OTP lebih aman.

G.5 Penelitian Terdahulu

Penelitian dengan judul "Implementasi Algoritma Time-Based One Time Password Dalam Otentikasi Token Internet Banking" (Ungkawa, Dewi, dan Putra t.t.). Penelitian ini melakukan penerapan TOTP dalam pembangkitan token OTP nya. Token tersebut tidak langsung dikirim ke user tetapi mengirim nilai hash nya. Penelitian ini menggunakan hash SHA256 sebagai metode hashingnya dan emkripsi AES. Penelitian ini diaplikasikan pada sistem internet banking di mana antara token virtual dan server dipasang algoritma TOTP untuk menghasilkan password sebagai otentikasi tambahan . Dari hasil pengujian yang dilakukan bahwa password OTP tidak muncul secara berulang dan secret key yang dihasilkan secara acak juga tidak muncul secara berulang tetapi mempunyai prosentasi kemiripan tertinggi sebesar 0,03%.

Penelitian dengan judul "Aplikasi Algoritma RSA untuk Keamanan Data pada Sistem Informasi Berbasis Web" (Rosnawan 2011). Untuk menjaga keamanan dari password dan pesan berupa file, biasanya digunakan teknik enkripsi

agar kerahasiaan data terebut terjamin. Salah satu algoritma enkripsi yang sering digunakan adalah algoritma RSA. Pada kesempatan ini penulis tertarik mengkaji tentang aplikasi pengamanan data pada sistem informasi berbasis web. Permasalahan dalam skripsi ini adalah bagaimana implementasi algoritma RSA untuk keamanan data pada sistem informasi berbasis web.

Penelitian dengan judul "Implementasi Algoritma RSA Untuk Enkripsi Dan Dekripsi Sms (Short Message Service) Pada Ponsel Berbasis Android" (Sardju, Magdalena, dan Atmaja 2015). Penelitian ini membahas tentang keamanan dalam penggunaan servis sms. Peneliti mengamankan pesan sms dengan menggunakan algoritma RSA. Hasil keluaran dari sistem ini yaitu pada pengiriman sms yang telah terenkripsi akan terkirim apabila $\leq$ 160 karakter, dan sms tidak akan terkirim apabila $\geq$ 160 karakter, pada proses enkripsi dan dekripsi membutuhkan waktu rata-rata 0,18 detik, pada pengujian *avalanche effect* dengan menggunakan masukan plaintext yang berbeda tiap percobaan akan menghasilkan chipert ext yang berbeda dengan presentase rata-rata sebesar 10,35 %, sedangkan pada pengujian *brute force* membutuhkan waktu selama 1,652 x tahun untuk mencoba semua kemungkinan kunci yang ada.

Penelitian - penelitian di atas dapat disimpulkan bahwa *two factor autentication* dan algoritma RSA sesuai untuk mengamankan fungsi login di sistem SI-Abka. Diharapkan dengan penelitian ini keamanan transaksi di sistem tersebut lebih tinggi lagi dan aman.

.

H. Metodologi Penelitian

Tahap ini menjelaskan mengenai metode penelitian yang digunakan untuk menganalisa data.

H.1 Objek Penelitian

Objek penelitian merupakan sistem SI-Abka yang merupakan sistem koperasi di kementeriam agama jember. Aplikasi tersebut penggunakan web php dan database mysql. Proses autentikasi dari seluruh akun hanya

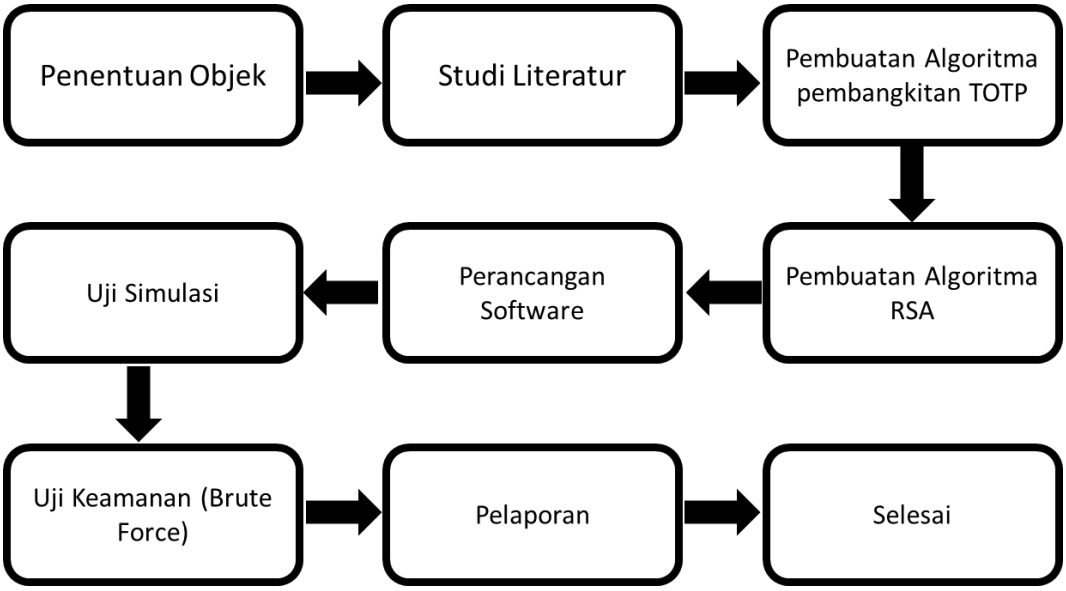
menggunakan username dan password. Dari sistem tersebut akan ditambah *two factor authentication* berupa TOTP dan algoritma RSA. Sistem authenticaton tambahan tersebut diharapkan dapat memperkuat keamanan sistem SI-Abka. Kode OTP akan di generate atau dibangkitkan menggunakan aplikasi di HP android atau sebuah alat portable. Kode di bangkitkan dengan cara memasukan public key ke dalam sistem SI-Abka saat meregistrasikan aplikasi android dengan sistem agar dapat selarah.

H.2 Tempat Penelitian

Tempat dilaksanakan penelitian yaitu di Universitas Jember. Sistem si-Abka akan di modifikasi dan dilakukan testing keamanan sistemnya.

H.3 Tahapan Penelitian

Tahapan Penelitian yang akan dilakukan dapat dilihat dalam diagram alur di bawah ini



H.4 Studi literatur

Tahapan ini merupakan tahapan mengumpulkan dan mengkaji *literature* tentang konsep dan metode pengerjaan yang digunakan untuk menyelesaikan permasalahan yang diangkat pada penelitian ini. Permasalahan pada penelitian ini didapatkan dari membaca jurnal penelitian terdahulu yang terkait penggunaaan Time-based one-time password dan

algoritma RSA yang berupa jurnal ilmiah, artikel ilmiah, buku maupun informasi dari situs-situs internet yang dapat dijadikan referensi dalam pengerjaan tugas akhir ini.

H.5 Pembuatan Algoritma Pembangkitan T-OTP

Algoritma TOTP bergangtung kepada beberapa faktor antara lain password, public key, username , kunci rahasia bersama dan faktor bergerak (moving factor), yaitu faktor waktu . Pada TOTP moving factor akan terus berganti tergantung pada waktu generate.. Standar yang digunakan atau interval waktu adalah setiap 30 detik. Jadi dengan mengisi interval waktu selama 30 detik , kita mengizinkan sebuah OTP hanya valid selama 30 detik.

H.6 Penerapan Algoritma RSA

Setelah kode OTP dibangkitkan maka dalam penggunaanya perlu di enkripsi agar pola pembangkitan tidak langsung di ketahui. Saat dilakukan pairing (inisialisasi pertama) sistem akan menampilkan sebuah barcode yang berisi public key. Public key ini didapat dengan cara sistem membuat sebuah public key dan private key secara random. Setelah didapat private key akan disimpan ke database sesuai dengan data penggunanya dan public key akan diberikan ke pengguna melalui barcode atau inputan secara langsung.

H.7 Perancangan software

Terdapat dua software yang di rancang yaitu berupa aplikasi android untuk pengguna dan modul aplikasi untuk sistem SI-ABKA. Kedua software ini akan digunakan untuk mengamankan proses login dan proses lainya sesuai dengan kebutuhan sistem yang akan di impelementasikan.

Saat pengguna akan meninputkan kode OTP maka aplikasi android akan membangkitkan TOTP berdasarkan data yang sama dengan server meskipun tidak berkomunikasi secara langsung. Setelah kode OTP berhasil dibangkitkan maka aplikasi android akan menengripsi kode tersebut menggunakan publik key yang didapat sebelumnya. Hasil enkripsi akan digunakan oleh pengguna dan dimasukan ke dalam sistem SI-ABKA. Saat sistem menerima inputan kode OTP maka akan di dekripsi dan dicocokan

dengan hasil pembangkitan yang dilakukan oleh sistem. Jika sesuai maka perintah akan di loloskan jika tidak maka akan invalid dan gagal.

H.8 Uji Simulasi

Uji simulasi dilakukan dengan menggunakan semua kemungkinan model login sistem dengan berbagai cara, status, dan kemungkinan, antara lain:

Username	**Password**	**OTP**	**Status**
Salah	Salah	Salah	Gagal
Salah	Salah	Benar	Gagal
Salah	Benar	Salah	Gagal
Salah	Benar	Benar	Gagal
Benar	Salah	Salah	Gagal
Benar	Salah	Benar	Gagal
Benar	Benar	Salah	Gagal
Benar	Benar	Benar	**Berhasil**

H.9 Uji keamanan

Uji keamanan dilakukan untuk mencoba keamanan sistem saat password dan username telah diketahui. Saat password dan username digunakan untuk login, sistem akan menampilkan form input kode OTP. Uji keamana kan di lakukan dengan cara memasukan kode OTP secara random dan cepat menggunakan metode brute force dengan bantuian aplikasi burp suite.

H.10 Pelaporan

Terdapat dua pelaporan yaitu untuk penelitian skripsi di universitas jember dan laporan untuk Kementerian Agama Kabupaten jember tentang penambahan modul autentikasi. Pelaporan di universitas berguna untuk menampilkan hasil penelitian berupa tugas akhir. Sedangkan untuk Kementerian agama berupa user guide/ tutorial dan modul yang akan digunakan untuk penambahan keamanan di sistem SI-ABKA

I. Luaran Yang Diharapkan

Dalam penelitian ini diharapkan dapat menghasilkan luaran antara lain :

1. Skripsi
2. Jurnal yang dipublikasikan
3. Sistem Si-Abka yang sudah menerapkan Two Factor Autentication dan Algoritma RSA

J. Jadwal Penelitian

Tabel 1 Jadwal Penelitian

NO	Tahapan Penelitian	2019				
		1	2	3	4	5
1	Penyusunan dan pengajuan Proposal					
2	Seminar Proposal					
3	Analisis Kebutuhan					
4	Pengumpulan data dan Pembuatan Sistem					
5	Penyusunan dan perbaikan skripsi					
6	Presentasi sidang skripsi					

Daftar Pustaka

Inayatullah. 2007. "Analisis Penerapan Algoritma MD5 Untuk Pengamanan Password." *jurnal ilmiah STMIK GI MDP* 3(3):1–5.

Khairina, Dyna Marisa. 2011. "ANALISIS KEAMANAN SISTEM LOGIN." *Jurnal Informatika Mulawarman* 6:64–67.

Kim, HyunChul, Young-Gu Lee, Kying-Seok Lee, dan Moon-Seog Jun. 2009. "Design and Implementation of Multi Authentication Mechanism for Secure Electronic Commerce." Hlm. 215–19 dalam *2009 10th ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing*. Daegu, Korea: IEEE.

M'Raihi, D., S. Machani, M. Pei, dan J. Rydell. 2011. *TOTP: Time-Based One-Time Password Algorithm*. RFC6238. RFC Editor.

Muchlis, Budi Satria, M. Andri Budiman, dan Dian Rachmawati. 2007. "Teknik Pemecahan Kunci Algoritma Rivest Shamir Adleman(RSA) dengan Metode Kraitchik." *jurnal & Penelitian Teknik Informatika* 2:2.

Musliyana, Zuhar, Teuku Yuliar Arif, dan Rizal Munadi. 2016. "Peningkatan Sistem Keamanan Autentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus: SSO Universitas Ubudiyah Indonesia." *Jurnal Rekayasa Elektrika* 12(1):21.

Mustofa, Rizka Putra. 2003. *APLIKASI MOBILE ANDROID "ONE TIME PASSWORD(OTP)" UNTUK MENINGKATKAN KEAMANAN OTENTIKASI*. yogyakarta: SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER A MIKOM YOGYAKARTA.

Rosnawan, Dadan. 2011. "Aplikasi Algoritma RSA untuk Keamanan Data pada Sistem Informasi Berbasis Web." *Universitas Negeri Semarang*. 1–25.

Sardju, Erick Ruliyanto, Ir. Rit. Magdalena, dan RatriDwi Atmaja. 2015. "IMPLEMENTASI ALGORITMA RSA UNTUKENKRIPSI DAN DEKRIPSI SMS (SHORT MESSAGE SERVICE) PADA PONSEL BERBASIS ANDROID." *e-Proceeding of Engineering* 2:2435.

Sudiarto Raharjo, Willy, Ignatia Dhian E.K. Ratri, dan Henry Susilo. 2017. "IMPLEMENTASI TWO FACTOR AUTHENTICATION DAN PROTOKOL ZERO KNOWLEDGE PROOF PADA SISTEM LOGIN." *Jurnal Teknik Informatika dan Sistem Informasi* 3(1).

Ungkawa, Uung, Irma Amelia Dewi, dan Kurnia Ramadhan Putra. t.t. "IMPLEMENTASI ALGORITMA TIME-BASED ONE TIME

PASSWORD DALAM OTENTIKASI TOKEN INTERNET BANKING.” *nstitut Teknologi Nasional Bandung* 1–10.