Journal Sistem Informasi, dan Teknologi Informasi

Vol. 1, No 2, Agustus 2022

https://journal-siti.org/index.php/siti/ Published By HPTAI

Implementasi Algoritma Exclusive OR (XOR) Dalam Pengembangan Aplikasi Chat Berbasis Android

Pujo Hari Saputro

Universitas Sam Ratulangi, Manado, Indonesia
Email: pujoharisaputr@unsrat.ac.id

Abstract

Android merupakan sistem operasi yang banyak digunakan di era modern ini. Hal ini tidak terlepas dari fitur Android yang semakin banyak dikembangkan untuk memudahkan user experience. Seiring dengan perkembangan tersebut, muncul pula masalah keamanan saat bertukar informasi atau data. Keamanan merupakan aspek penting dari perkembangan era teknologi informasi modern, sehingga berkembanglah cabang ilmu yang mempelajari keamanan data atau yang dikenal dengan kriptografi.
Penelitian ini bertujuan untuk merancang dan membangun aplikasi chat yang aman berbasis Android dan menerapkan algoritma XOR. Algoritma ini digunakan untuk mengamankan informasi sehingga tidak dapat dibaca sebelum sampai ke penerima. Perhitungan algoritma ini menghasilkan pesan acak (ciphertext) yang hanya dapat dibaca oleh penerima.
Hasil dari pencarian ini adalah sebuah aplikasi chatting yang didalamnya terdapat fitur keamanan dimana penerima harus memasukkan key yang sama dengan pengirim agar pesan dapat dibaca. Pengujian aplikasi ini dilakukan dengan mengirimkan pesan kemudian memasukkan kunci yang sama antara pengirim dan penerima

Keywords: Aplikasi Chat, Kriptografi, Algoritma XOR

1. PENGANTAR

Kecenderungan kehidupan manusia saat ini sangat dipengaruhi oleh perkembangan teknologi informasi, hal ini terlihat pada beberapa tahun belakangan ini. Teknologi informasi merupakan perkembangan gabungan antara teknologi komputer dan telekomunikasi [1]. Salah satu teknologi yang pesat saat ini adalah pada bidang komunikasi. Komunikasi adalah kegiatan penyampaian informasi dari satu pihak ke pihak lain [2].Chat adalah program yang digunakan untuk berkomunikasi dengan pengguna internet lain yang sedang online [3].
Di balik kemudahan komunikasi, ada masalah yang sering diabaikan, yaitu keamanan. Seringkali, masalah keamanan data kurang mendapat perhatian dari perancang dan manajer sistem. Celah keamanan ini diperlukan. Salah satu cara

mengamankan data dan informasi adalah dengan menggunakan kriptografi, kriptografi adalah teknik yang berkaitan dengan kerahasiaan data agar data tidak mudah dibaca oleh orang yang tidak berada di bawah tanggung jawabnya. Selain itu, kriptografi dapat diartikan sebagai ilmu yang digunakan untuk mengamankan pesan. Ketika sebuah pesan dikirim oleh satu pihak ke pihak lain, isi pesan tersebut dapat diketahui oleh pihak lain. Oleh karena itu, untuk menjaga kerahasiaan, pesan tersebut dapat diubah menjadi kode acak yang hanya diketahui oleh pengirim dan penerima [4]

Salah satu algoritma kriptografi yang sering digunakan dalam pengamanan adalah algoritma XOR, Algoritma XOR merupakan algoritma yang sering digunakan pada cipher yang menggunakan operasi bitwise dan termasuk dalam kriptografi klasik [5]. Algoritma XOR juga merupakan algoritma sederhana yang menggunakan prinsip logika XOR. Untuk proses melakukan proses enkripsi dengan meng-XOR-kan kunci dengan plaintext sehingga diperoleh ciphertext. Sedangkan untuk proses dekripsi, cipherteks di-XOR dengan kunci untuk mendapatkan teks asli (plaintext). Proses enkripsi dan dekripsi kriptografi tidak sulit dan mudah untuk diimplementasikan [6].

2. METODE

2.1. Kriptografi

Kriptografi adalah cabang matematika yang berkaitan dengan teknik keamanan, aspek informasi seperti validitas data, integritas data, dan otentikasi entitas. Dalam kriptografi terdapat dua proses yaitu enkripsi dan dekripsi.

Kriptografi terbagi menjadi 2 aliran yaitu kriptografi klasik dan kriptografi modern. Dalam kriptografi klasik terdapat beberapa teknik enkripsi yaitu substitusi dan transposisi. Sedangkan kriptografi modern merupakan teknik kriptografi yang lebih rumit dibandingkan dengan kriptografi klasik, karena algoritma ini menggunakan komputer [7].

2.2. Enkripsi dan Dekripsi

Enkripsi dan Dekripsi merupakan dua hal yang tidak bisa dipisahkan dari kriptografi, karena dua hal tersebut adalah proses utama dari merubah teks tidak beraturan menjadi teks yang dapat dibaca dan sebaliknya. Enkripsi adalah proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut plaintext) menjadi pesan yang tersembunyi (disebut ciphertext) adalah enkripsi (encryption). Sedangkan dekripsi merupakan kebalikan dari proses enkripsi, untuk mengubah

ciphertext menjadi plaintext, disebut dekripsi (decryption). Terminologi yang lebih tepat untuk proses ini adalah "decipher" [8] . Pada proses enkripsi juga terdapat public key dan private key. Public key merupakan kunci yang bersifat rahasia dan diketahui oleh semua pihak yang bertujuan mengirim pesan kepada penerima, sedangkan private key hanya diketahui oleh pengirim dan penerima. [9]

2.3. ASCII

ASCII adalah Kode Standar Amerika untuk Pertukaran Informasi atau ASCII (Kode Standar Amerika untuk Pertukaran Informasi). ASCII adalah standar internasional dalam kode huruf dan simbol seperti Hex dan Unicode tetapi ASCII lebih universal, misalnya 124 untuk karakter "|". Kode ini masih digunakan oleh komputer dan perangkat komunikasi lainnya untuk merepresentasikan teks. Kode ASCII sebenarnya memiliki susunan bilangan biner 7 bit. Namun, ASCII disimpan sebagai kode 8-bit dengan menambahkan 0 sebagai bit yang paling signifikan. Bit ekstra ini sering digunakan untuk pengujian prioritas.
Karakter dalam ASCII dibagi menjadi 5 kelompok menurut penggunaannya, yang masing-masing meliputi komunikasi logis, kontrol perangkat, pemisah informasi, ekstensi kode, dan komunikasi fisik. Kode ASCII ini sering ditemukan pada keyboard komputer atau instrumen digital.

2.4. Algoritma Exclusive OR (XOR)

Operasi binner yang sering digunakan dalam cipher dalam mode bit adalah XOR. Simbol yang digunakan adalah "^". Pada algoritma XOR yang dioperasikan pada dua bit dengan aturan sebagai berikut.

Tabel 1. Aturan Operasi XOR

A	B	A^B
1	1	0
0	0	0
0	1	1
1	0	1

Sedangkan untuk operasinya algoritma XOR adalah dengan meng XOR kan plainteks dengan kunci (K) untuk menghasilkan cipherteks (C): C = P ^ K.

Untuk algoritma dekripsinya adalah dengan meng XOR kan cipherteks dengan kunci (K) untuk menghasilkan plainteks (P): P = C ^ K.

2.5. Metode Penelitian

Penelitian ini berfokus pada pengembangan aplikasin secure chat dengan mengimplementasikan algoritma XOR. Berikut adalah prosedur penelitian yang dilakukan.

Gambar 1. Prosedur Penelitian

3. HASIL DAN DISKUSI

3.1. Tampilan Aplikasi

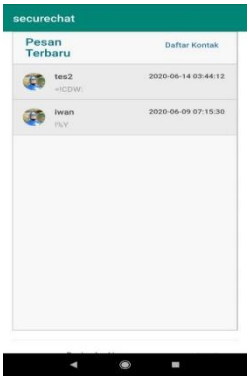
1. Tampilan Login

Gambar 2. Halaman Login

Proses dimulai ketika pengguna mengisi ID Pengguna serta password kemudian mengklik tombol login, apabila pengguna tidak mengisi kolom tersebut makan tidak akan terjadi proses dan apabila pengguna salah memasukkan ID Pengguna dan password maka proses login akan gagal.

2. Halaman Pesan

Apabila login telah berhasil maka akan muncul halaman pesan terbaru serta menu daftar kontak yang dapat diakses oleh pengguna..

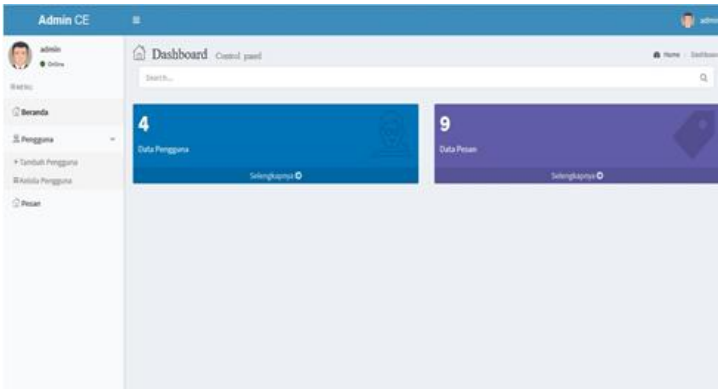


Gambar 3. Halaman pesan

3. Halaman Kontak
   Halaman kontak akan menampilkan daftar akun yang kita simpan pada aplikasi.

Gambar 4. Halaman Kontak

4. Dasboard admin
   Dasboard admin dapat diakses melalui browser, pada dashboard ini adalah control utama aplikasi. Admin mempunyai beberapa hak akses seperti Kelola pengguna dan Kelola pesan.



Gambar 5. Halaman Dasboard Admin

3.2. Pembahasan

Proses enkripsi merupakan suatu langkah untuk mengubah kata asli (plaintext) menjadi karakter acak (ciphertext) supaya isi dari kata tidak dapat terbaca oleh orang lain. Untuk proses enkripsi pada aplikasi ini menggunakan perhitungan algoritma XOR dengan tujuan untuk merubah karakter pesan menjadi rangkaian karakter acak (ciphertext) dengan menggabungkan isi pesan dan ID Pengguna sebagai karakter kunci (key) dan diubah terlebih dahulu menjadi bilangan biner, lalu masing-masing karakter dilakukan proses XOR supaya membentuk karakter baru dan karakter tersebut terdapat dalam tabel ASCII. Pada program kali ini, peneliti menggunakan ID Pengguna sebagai kunci default yang digabungkan dengan isi pesan sebagai proses algoritma XOR supaya membentuk rangkaian pesan berupa ciphertext. Sebagai contoh kita ingin mengirim pesan "makan" dengan kunci "ID002", tahapan perhitungannya adalah:

1. Pada tabel ASCII kita cari terlebih dahulu nilai per karakter lalu ubah menjadi desimal lalu biner kemudian ditemukan :
   m = 109 (desimal) 0110 1101 (biner)
   a = 97 (desimal) 0110 0001 (biner)
   k = 107 (desimal) 0110 1011 (biner)
   a = 97 (desimal) 0110 0001 (biner)
   n = 110 (desimal) 0110 1110 (biner).
   Sedangkan untuk karakter kuncinya, ditemukan :
   I = 73 (desimal) 0100 1001 (biner)
   D = 68 (desimal) 0100 0100 (biner)
   0 = 48 (desimal) 0011 0000 (biner)
   0 = 48 (desimal) 0011 0000 (biner)
   2 = 50 (desimal) 0011 0010 (biner)
2. Untuk proses enkripsi kita lakukan sesuai rumus C = P ^ K dan simbol (^) merupakan simbol untuk XOR, sehingga ditemukan sebagai berikut :
   m 0110 1101
   I 0100 1001 ^
   Hasil 0010 0100 (biner) = 36 (desimal)
   a 0110 0001
   D 0100 0100 ^
   Hasil 0010 0101 = 37 (desimal)
   k 0110 1011
   0 0011 0000 ^

Hasil 0101 1011 = 91 (desimal)
a 0110 0001
0 0011 0000 ^
Hasil 0101 0001 = 83 (desimal)
n 0110 1110
2 0011 0010 ^
Hasil 0101 1100 = 92 (desimal)

3. Setelah masing-masing karakter dilakukan operasi algoritma XOR dan telah dirubah terlebih dahulu ke desimal, maka selanjutnya dicari terlebih dahulu karakter pada ASCII supaya bisa membentuk sebuah rangkaian karakter acak (ciphertext) untuk ditampilkan pada pesan, kemudian ditemukan :
   36 (desimal) dengan karakter ASCII " $ "
   37 (desimal) dengan karakter ASCII " % "
   91 (desimal) dengan karakter ASCII " ["
   83 (desimal) dengan karakter ASCII " S "
   92 (desimal) dengan karakter ASCII " \ "
4. Hasil karakter acak (ciphertext) dari kata "makan" dengan kunci "ID002" adalah $%[S\ dan selanjutnya akan diteruskan kepada penerima.

4. KESIMPULAN

Dengan pengembangan aplikasi chat dengan memanfaatkan algoritma XOR dapat ditarik keseimpulan data yang dikirim dapat diamankan dengan baik dan dirubah sehingga data teks yang dikirim sudah berubah tidak sesuai dengan teks asli sehingga apabila data teks dilihat orang lain tidak dapat difakami secara langsung.

REFERENSI

[1] H. Budiman, "Peran Teknologi Informasi Dalam Pendidikan.," Al-Tadzkiyyah: Jurnal Pendidikan Islam, Vol. 8, No. 1, 2017.
[2] O. F, "Upaya Komunikasi Interpersonal Kepala Desa Dalam Memediasi Kepentingan Pt. Bukit Borneo Sejahtera Dengan Masyrakat Desa Long Lunuk," E Journal Ilmu Komunikasi, 2016.
[3] F. Kasih, "Perancangan Chating Room Berbasis Network," Cess (Journal Of Computer Engineering, System And Science), Vol. 1, No. 2, 2016.
[4] A. M, "Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks," Jurnal Pseudocode, Vol. 3, No. 2, 2016.

[5] Suhardi, "Aplikasi Kriptografi Data Sederhana Dengan Metode Exlusive Or (Xor)," Jurnal Teknovasi, 2016.
[6] R. Amalia, "Implementasi Algoritma Aes Dan Algoritma Xor Pada Aplikasi Pengaman Berbasis Mobile," Pamulang: Faktor Exata, 2018.
[7] N. M, "Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Pada Office Menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java," Jurnal Format, 2017.
[8] Primarta, "Penerapan Enkripsi Dan Dekripsi File Menggunakan Metode," Jurnal Sistem Informasi, 2011.
[9] A. F, "Desain Dan Implementasi Protokol Kriptografi Untuk Aplikasi Secure Chat Pada Multiplatform Sistem Operasi," Seminar Nasional Informatika, 2015.