BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Penggunaan PDF biasanya identik dalam dunia kerja yang mengarah pada pengolah data. Data yang sudah dibuat dalam *Microsoft Office*seperti *word*, *excel* dan lainnya biasa disimpan dalam ekstensi aslinya atau dalam ekstensi lain, salah satunya PDF. Banyaknya orang yang memilih menggunakan format ini adalah karena sangat praktis dan tidak memakan waktu lama untuk membukanya. Sehingga beberapa data penting dan rahasia juga dirubah kedalam bentuk PDF. Penggunaan praktis dokumen PDF juga dapat didistribusikan dengan jaringan internet, seperti pada aplikasi berbasis chat, facebook, whatsapp, dan media email, namun dokumen PDF yang dikirimkan melalui jaringan internet rentan terhadap serangan dan penyadapan, serta disimpan pada media penyimpanan yang rentan terhadap akses orang yang tidak berwenang.((Nasution et al., 2020)).

Ada ayat-ayat dalam Al-Qur'an yang membahas tentang mencuri hak orang lain

اِذْهَبْ بِّكِتٰبِيْ هٰذَا فَاَلْقِهْ اِلَيْهِمْ ثُمَّ تَوَلَّ عَنْهُمْ فَانْظُرْ مَاذَا يَرْجِعُوْنَ

“Pergilah dengan (membawa) suratku ini, lalu jatuhkanlah kepada mereka, kemudian berpalinglah dari mereka, lalu perhatikanlah apa yang mereka bicarakan ” (QS. An Naml: 28).

Pencurian dan penyalahgunaan dokumen PDF yang bersifat rahasia karena dokumen masih dapat dikenali dan dibaca oleh manusia, tentunya hal **tersebut** merugikan pihak yang memiliki akses terhadap data dokumen PDF tersebut. Dengan menerapkan teknik enkripsi kriptografi, penyadapan dan pencurian dokumen PDF dapat diminimalkan. Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi. Kriptografi memelurkan algoritma untuk melakukan proses enkripsi, salah satu algoritma

kriptografi yang dapat digunakan adalah algoritma *Data Encryption Standart* (DES).

Algoritma DES adalah algoritma simetris berdasarkan prinsip block cipher. Algoritma DES adalah algoritma enkripsi yang paling banyak digunakan di dunia dan telah diadopsi oleh NIST (National Institute of Standards and Technology) sebagai Standar Pemrosesan Informasi Federal AS ((Yanti et al., 2018)). Algoritma DES menggunakan kunci 64-bit untuk mengenkripsi blok 64-bit. Namun, karena 8 bit kunci digunakan sebagai paritas, kunci efektif hanya 65 bit. DES bekerja dengan melakukan hingga 16 putaran enkripsi menggunakan fungsi kriptografi f, setiap putaran menggunakan kunci 48-bit yang berbeda dan berdasarkan kunci DES. Efeknya adalah setiap blok dienkripsi secara bergantian, 8 kali per blok. ((Adhar, 2019))

Berdasarkan uraian latar belakang di atas, penulis menetapkan judul penelitian ini sebagai " "**Implementasi Algoritma *Data Encryption Standart (DES)* Untuk Pengamanan Data Pada Dokumen PDF**".

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang tersebut, maka pertanyaan penelitian dirumuskan sebagai berikut:

1. Bagaimana cara melindungi dokumen PDF dengan teknologi enkripsi kata sandi?
2. Bagaimana menerapkan algoritma DES untuk mengenkripsi dokumen PDF?
3. Bagaimana cara merancang dan membangun aplikasi yang dapat menggunakan algoritma DES untuk menjaga kerahasiaan informasi yang terdapat dalam dokumen PDF?

1.3 Batasan Masalah

Berdasarkan uraian rumusan masalah di atas, maka batasan masalah dalam penelitian ini adalah:

1. Enkripsi dan dekripsi hanya dilakukan pada string (8 karakter) dan hexa yang terdapat pada dokumen PDF.
2. Perangkat lunak yang digunakan untuk merancang dan membangun aplikasi adalah XAMPP, bahasa pemrograman PHP

1.4 Tujuan Penelitian

Berdasarkan rumusan pertanyaan di atas dan interpretasi keterbatasan, tujuan penelitian ini meliputi:

1.Lindungi dokumen PDF dengan teknologi enkripsi kata sandi.

2.Terapkan algoritma DES untuk perlindungan keamanan dokumen PDF.

3.Merancang dan membangun aplikasi yang dapat menjaga kerahasiaan informasi yang terdapat pada dokumen PDF dengan menggunakan algoritma DES.

1.5 Manfaat Penelitian

Sesuai dengan uraian tujuan di atas, maka manfaat yang diberikan oleh penelitian ini adalah:

1. Mengurangi terjadinya perusakan informasi yang terdapat dalam dokumen PDF.

2. Berikan informasi tentang bagaimana algoritma DES mengenkripsi dokumen PDF.

3.Meningkatkan pemahaman tentang cara merancang dan membangun aplikasi kriptografi dengan menggunakan bahasa pemrograman PHP Enkripsi untuk deskripsi dokumen PDF