# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Seiring dengan semakin besar ketergantungan terhadap inovasi teknologi informasi, website menjadi sarana penyimpan dan pertukaran data serta layanan yang semakin digunakan, hampir setiap sektor layanan hingga sistem informasi akademik mengandalkan sistem login sebagai gerbang pertama akses pengguna terhadap informasi sensitif, kemudahan ini membawa konsekuensi meningkatnya risiko keamanan terutama terhadap pencurian identitas dan akses ilegal melalui manipulasi data login, salah satu contoh yang nyata adalah terjadinya peretasan akun yang dapat bermula dari celah keamanan pada sistem login[1].

Website Ti polbeng adalah portal resmi Jurusan Teknik Informatika Politeknik Negeri Bengkalis website ini berfungsi sebagai pusat informasi akademik, administrasi, dan layanan digital bagi mahasiswa, dosen, calon mahasiswa yang terdapat informasi lengkap tentang profil jurusan, program studi D3 dan D4 serta kurikulum kegiatan akademik, prestasi, serta publikasi ilmiah Selain itu, website ini menyediakan akses ke layanan elektronik seperti SIAKAD, e-journal, dan sistem layanan yang terpadu.

Dalam kurun waktu satu tahun terakhir, website resmi Teknik Informatika Politeknik Negeri Bengkalis telah 5 kali mengalami peretasan dan gangguan keamanan yang signifikan tidak hanya mengganggu operasional layanan akademik tetapi juga menimbulkan kekhawatiran akan kebocoran data, khususnya data login seperti *username* dan *password* admin.

Pengamanan login dengan menggunakan algoritma blowfish adalah pengamanan melalui enkripsi dengan algoritma kriptografi yaitu mengubah kata sandi asli atau password yang kita ingin amankan (plaintext) menjadi pesan acak atau informasi yang susunan kalimatnya sulit dipahami (chipertext) dengan menggunakan kunci (key), Pihak yang tidak berwajib akan kesulitan mengetahui isi dari kata sandi atau password, Apabila informasi tersebut menjadi algoritma enkripsi yang mengubah data (plaintext) menjadi ciphertext ingin diubah menjadi

pesan aslinya (plaintext) maka dilakukan proses dekripsi dengan menggunakan kunci (key).[2] Pemilihan dengan menggunakan metode ini dikarenakan Blowfish dinilai sebagai salah satu algoritma kriptografi symetris yang cepat dan kompak, mempunyai perhitungan sederhana sedangkan panjang kunci yang biasa digunakan yaitu bervariasi mulai dari 32 bit sampai 448 bit, Blowfish dioptimasikan untuk berbagai aplikasi dimana kunci tidak sering berubah, seperti pada jaringan komunikasi atau enkripsi file secara otomatis[3].

Blowfish adalah algoritma simetris 64-bit yang menggunakan panjang kunci bervariasi dari 32-bit sampai 448-bit (14 bytes), Blowfish dirancang untuk mengenkripsi plain text 64-bit ke cipher text 64-bit secara efisien dan aman, Operasi yang digunakan dalam prosesnya berupa lookup table, modulus, penambahan dan XOR untuk meminimalisir waktu yang dibutuhkan dalam mengenkripsi dan mendekripsi data pada prosesor 32-bit[4]

Masalah keamanan login website merupakan sesuatu yang sangat penting dalam era saat ini terutama bagi website TI polbeng. Kerahasiaan password merupakan salah satu masalah yang penting dalam keamanan data terutama pada kata sandi, password menjadi salah satu hal yang penting dalam website, Ketika password kirim dari website menuju data base tanpa adanya proses enkripsi kemungkinan terdapat beberapa ancaman yang dapat merusak keamanan yakni serangan Brute Force Attack, sehingga keamanan kata sandi data tersebut mudah untuk di retas, untuk melindungi data penting tersebut maka data dapat dienkripsi dan didekripsi atau diubah menjadi kode yang tidak dapat diketahui orang lain[4].

Message Digest Algorithm 5 (MD5) merupakan salah satu algoritma hash kriptografis populer. Algoritma ini diciptakan dengan nilai hash 128 bit oleh Ronald Rivest pada 1991 untuk menggantikan MD4. Pada tahun 1996 ditemukan lubang keamanan pada desainnya, dan pada 2004 beberapa masalah keamanan serius ditemukan menjadikan tingkat keamanan algoritma ini sangat dipertanyakan[5].

MD5, salah satu fungsi hash yang paling sering digunakan saat ini, sudah tidak lagi aman karena beberapa kelemahannya sudah ditemukan. Karena fungsi hash sering digunakan untuk menjaga keamanan (security) pengiriman data seperti otentikasi dan integritas pesan, penemuan kolisi akan memberikan efek yang sangat

besar terhadap keamanan pengiriman data. Berdasarkan hal tersebut, pada makalah ini, dilakukan studi dan implementasi kolisi pada fungsi hash MD5[6].

penelitian ini diperkuat dengan mengingat pentingnya menjaga integritas dan kerahasiaan data dalam lingkungan akademik yang mulai beralih ke sistem digital secara menyeluruh, Jika masalah ini tidak segera diatasi, maka risiko pencurian identitas modifikasi data akademik, dan akses ilegal terhadap sistem dapat semakin meningkat, Oleh karena itu, diperlukan penerapan metode pengamanan yang lebih andal dan terbukti efektif, seperti algoritma Blowfish, untuk memperkuat keamanan sistem login dan mencegah serangan siber yang lebih besar di masa mendatang

## 1.2 Rumusan Masalah

Dalam perkembangan teknologi saat ini, di mana hampir seluruh aktivitas administrasi dan layanan akademik telah bergantung pada sistem informasi berbasis web, keamanan data login menjadi salah satu aspek krusial yang tidak dapat diabaikan, Sistem login merupakan pintu utama yang menghubungkan admin untuk mengakses website teknik informatika politeknik negri bengkalis TI POLBENG Oleh karena itu, sistem login wajib dirancang dengan mempertimbangkan aspek keamanan yang kuat untuk mencegah perlindungan oleh pihak yang tidak bertanggung jawab.

Permasalahan ini menjadi semakin kuat ketika mempertimbangkan bahwa serangan siber seperti *brute force attac,* semakin marak terjadi, Serangan-serangan tersebut memanfaatkan celah pada sistem *autentikasi* dan kelemahan enkripsi untuk membobol sistem dan mendapatkan akses tidak sah, Misalnya, dalam serangan *Brute Force Attack*, penyerang mencoba berbagai kombinasi kata sandi hingga berhasil menebak yang benar, Tanpa adanya batasan login atau sistem keamanan yang terenkripsi.

Hal yang lebih perlu di perhatikan kurangnya penerapan Algoritma Enkripsi modern pada sistem login tersebut, Website resmi Teknik Informatika Politeknik Negeri Bengkalis hingga saat ini masih menggunakan algoritma hashing lama

seperti *MD5* yang sudah dianggap tidak aman karena rentan terhadap serangan *Brute Force Attack*, di samping itu kesadaran akan pentingnya aspek keamanan data login pada sistem tersebut belum menjadi perhatian utama, sehingga pengembangannya lebih menitikberatkan pada aspek fungsionalitas tanpa disertai perlindungan kriptografi yang memadai, Hal ini membuka potensi kerentanan yang cukup besar terhadap ancaman siber, terutama jika tidak segera dilakukan peningkatan pada sistem autentikasinya.

Jika masalah ini tidak segera diatasi dengan cara yang benar, maka tidak mungkin akan terjadi kebocoran data yang lebih besar di masa depan. Risiko-risiko seperti pengmabilan hak akses yang beralih ke dalam website judol Kondisi ini tidak hanya berdampak pada aspek teknis, tetapi juga dapat meningkatkan kredibilitas institusi pendidikan di mata masyarakat dan merugikan seluruh signifitas akademik secara keseluruhan.

## 1.3 Batasan Masalah

Berdasarkan latar belakang dan uraian di atas, skripsi ini memiliki beberapa batasan masalah yang dirumuskan untuk memperjelas ruang lingkup penelitian, sebagai berikut:

a) Penelitian ini fokus membahas keamanan data login admin pada TI polbeng, tidak mencakup pengguna umum atau mahasiswa.
b) Data yang diamankan dalam penelitian ini dibatasi pada data login, yaitu username dan password, serta mekanisme autentikasi tambahan berupa OTP One-Time Password.
c) Pengujian keamanan dilakukan terhadap algoritma Blowfish menggunakan simulasi serangan Sql injction dan bruteforce.
d) Mekanisme autentikasi OTP dalam penelitian ini dibatasi pada pengiriman melalui aplikasi WhatsApp, dan tidak mencakup pengiriman melalui SMS, email, atau media lainnya.

## 1.4 Tujuan

Tujuan dari penelitian ini adalah untuk mengimplementasikan algoritma Blowfish pada sistem login website Teknik Informatika Politeknik Negeri Bengkalis, implementasi ini bertujuan untuk meningkatkan keamanan data login khususnya username dan password dari berbagai potensi ancaman seperti serangan Brute Force Attack dengan penerapan algoritma Blowfish, diharapkan sistem login menjadi lebih aman dan andal dalam menjaga kerahasiaan data login serta mampu meminimalkan risiko kebocoran data username dan password akibat dari serangan atau akses yang tidak sah.

## 1.5 Manfaat

Manfaat penelitian ini:

1. Dapat meningkatkan keamanan data login (username dan password) dari serangan siber seperti serangan brute force.
2. Memberikan pengalaman dan pemahaman mendalam tentang penerapan algoritma Blowfish dalam mengamankan data login dan meningkatkan kemampuan dalam merancang sistem keamanan berdasarkan enkripsi.
3. Penelitian ini dapat sebagai referensi dalam pengembangan sistem keamanan data login berbasis enkripsi.
4. Memberikan kontribusi pada pengembangan literasi keamanan siber di kalangan akademik maupun instansi -instansi lainnya.