BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Kemampuan siswa dalam memahami suatu materi dapat dilihat dari kemampuan siswa tersebut dalam mengerjakan berbagai macam soal dalam materi yang sama. Jumlah soal, keragaman soal dan variasi kemunculan soal menjadi suatu hal yang patut diperhitungkan dalam pengelolaan soal-soal latihan.

Pengacakan soal dapat dilakukan dengan menggunakan suatu pembangkit bilangan acak. Dari sejumlah cara yang digunakan untuk membangkitkan bilangan acak, Blum Blum Shub merupakan salah satu diantaranya. Menurut Ferdian Thung (2009) *Blum Blum Shub* (BBS) adalah suatu sebuah pembangkit bilangan acak semu (*pseudo random generator*) yang aman secara kriptografi, diusulkan tahun 1986 oleh Lenore Blum, Manuel Blum dan Michael Shub. BBS memiliki suatu kelebihan dibandingkan metode pengacakan lainnya, yaitu terletak pada kesederhanaannya dalam melakukan pengacakan. BBS menggunakan fungsi yang berpacu pada dua buah bilangan prima rahasia, yang masing-masing dari bilangan tersebut kongruen dengan 3 modulo 4.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang ada maka dapat didefinisikan permasalahan dari penelitian ini yaitu;

1. Bagaimana menerapkan metode *Blum Blum Shub* (BBS) untuk mengacak soal pada aplikasi pembelajaran matematika.
2. Bagaimana pengaruh besarnya jumlah soal yang diminta user dan jumlah soal yang tersedia dalam *database* terhadap kemungkinan soal yang akan muncul.

1.3 Ruang Lingkup

Untuk memfokuskan penelitian maka diberikan ruang lingkup untuk penelitian ini yaitu ;

1. Parameter pengujian untuk pengacakan adalah jumlah soal yang diminta pengguna dan jumlah soal yang ada dalam dalam *database*.
2. Nilai p dan q akan dihasilkan secara *random* oleh program.

1.4 Tujuan

Pembuatan aplikasi ini bertujuan untuk ;

1. Menerapkan metode *Blum Blum Shub* (BBS) untuk pengacakan soal.

2. Mengetahui seberapa besar pengaruhnya jumlah soal yang diminta oleh pengguna dan jumlah soal yang berada dalam *database* terhadap kemunculan soal yang sama dalam periode tertentu menggunakan metode *Blum Blum Shub* (BBS).