KATA PENGANTAR

Puji syukur Alhamdulillah panjatkan kehadirat Allah SWT yang telah melimpahkan rahmatnya serta hidayahnya sehingga mampu menyelesaikan Proposal Tugas Akhir dengan judul "**Pembangkitan Kunci Untuk Penentuan Konstanta P dan Q yang Prima Berdasarkan Informasi Peranti**".

Selawat Salam semoga selalu tercurahkan kepada Nabi Muhammad SAW Beserta keluarga dan para sahabatnya hingga pada umatnya sampai akhir zaman.

Proposal Tugas Akhir ini disusun untuk memenuhi salah satu syarat dalam menyelesaikan jenjang pendidikan program Diploma III di Jurusan Teknologi Informasi, Politeknik Negeri Samarinda.

Dalam proses penyusunan Proposal Tugas Akhir ini, mendapatkan banyak sekali bantuan, bimbingan serta dukungan dari berbagai pihak, sehingga dalam kesempatan ini, bermaksud menyampaikan rasa terima kasih kepada:

1. Kedua orang tua dan keluarga yang selalu memberi dukungan moral dan materi.
2. Ansar Rizal, ST., M.Kom. selaku Ketua Jurusan Teknologi Informasi Politeknik Negeri Samarinda
3. Mulyanto, S.Kom., M.Cs. selaku promotor yang telah membimbing hingga terselesaikannya proposal tugas akhir ini.
4. Staf dosen, staf teknisi, dan staf administrasi jurusan yang telah membantu dalam segala hal yang berkaitan dengan perkuliahan.
5. Semua sahabat dan rekan-rekan mahasiswa jurusan Teknologi Informasi yang ikut memberi saran dan masukan.

6. Serta semua pihak lain yang ikut terlibat dalam penyelsaian Proposal Tugas Akhir ini

Semoga Allah SWT memberi balasan yang setimpal kepada semuanya.

Harapannya tugas akhir yang telah disusun ini bisa memberikan sumbangsih untuk menambah pengetahuan, dan perbaikan selanjutnya, selalu terbuka terhadap saran dan masukan, karena menyadari tugas akhir yang telah disusun ini memiliki banyak sekali kekurangan.

Samarinda, 07 September 2020

Yogi Arif Widodo

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

ABSTRAK

Jika difaktorkan hanya habis dibagi oleh angka 1 dan dengan dirinya sendiri disebut Bilangan Prima. Keunikanya selalu berbentuk antara 6k-1 atau 6k +1. Salah satu konsep atau metode berhubungan dengan bilangan yang prima dimiliki oleh Rivest Shamir Adleman (RSA), untuk pembangkitan kuncinya dibagi menjadi 2 buah pola yaitu variabel *p* dan *q*. Konstanta atau orde *p* dan *q* menjadi eksperimen aritmatika dalam kombinasi informasi peranti waktu pada *android mobile* dengan bentuk jam (HH), menit (mm) dan detik (ss). Greenwich Mean Time Zone (GMT) merupakan zona waktu informasi menjadikanya berpola determisitik menjadi probabilistik jika diolah menggunakan *pseudorandom* kemudian menghasilkan *index* waktu yang mengubah Zona Awal (ZA) 15:17:02 GMT + 8 ke Zona Lain (ZL) menjadi 10:17:03 GMT - 11. Waktu yang digunakan ketika terjadinya proses aritmatika yaitu ZL. HH berperan dalam pembentukan *p* sedangkan *q* dipengaruhi oleh mm dan ss dengan ketentuan sebagai *index* yang sedemikian rupa. Pembangkitan awal ditentukan dengan batas atas prima n = 512. Dengan teknik sederhana *naive solution* dimana 2 ke n – 1 menghasilkan *arrayListPrimeNumber* = 2,3,5,7,9..n. Kombinasi dan Aritmatika berhasil menentukan p = 179 dan q = 419. Hasil Entropi Enkripsi dari 4 sample (teks 1 = 4.035569614562073, teks 2 = 4.257107430057822, teks 3 = 3.77391380004984 dan teks 4 = 4.421087076196203) masing-masing menghasilkan nilai yang ekuivalen terhadap p dan q yang ditentukan dengan yang secara *default.* Hasil enkripsi dibantu dengan RSA dengan kunci 2 *bit* – 17 *bit*. Cara meningkatkan hasil Prima yang besar pada penelitian ini, dapat dilakukan dengan menaikan nilai *inisial* dan *n* yang ditetapkan pada rumus $P_{penentuan}$ dan $q_{penentuan}$. Seluruh proses, diuji keberhasilan program dengan pengecualian atau *Exception Handling*, hasilnya tidak ada *problem* pada *feedback monitoring* aplikasi android.

Kata kunci : *Bilangan Prima, Informasi Peranti Waktu, P dan Q*

ABSTRACT

If it is factored, it is only divisible by the number 1 and by itself it is called a prime number. The uniqueness is always in the form between 6k-1 or 6k +1. One of the concepts or methods related to prime numbers is owned by Rivest Shamir Adleman (RSA). The key generation is divided into 2 patterns, namely variables p and q. Constants or orders p and q become arithmetic experiments in a combination of time device information on an android mobile in the form of hours (HH), minutes (mm) and seconds (ss). Greenwich Mean Time Zone (GMT) is an information time zone making it a deterministic pattern to be probabilistic if processed using pseudorandom then producing a time index which changes the Initial Zone (ZA) 15:17:02 GMT + 8 to Other Zones (ZL) to 10:17: 03 GMT - 11. The time used when the arithmetic process occurs is ZL. HH plays a role in the formation of p while q is influenced by mm and ss provided that it is an index in such a way. Initial generation is determined with an upper limit of prime n = 512. With a simple naive solution technique where 2 to n - 1 results in arrayListPrimeNumber = 2,3,5,7,9..n. Combination and Arithmetic succeeded in determining p = 179 and q = 419. The results of the Encryption Entropy of 4 samples (text 1 = 4.035569614562073, text 2 = 4.257107430057822, text 3 = 3.77391380004984 and text 4 = 4.421087076196203) each yields a value equivalent to p and q which is specified by default. The results of the encryption are assisted by RSA with a key of 2 bits - 17 bits. How to increase the large Prima results in this study, can be done by increasing the initial value and n set in the formula $P_{penentuan}$ and $q_{penentuan}$. *The whole process, tested the success of the program with exception or Exception Handling, the result is that there are no problems in the android application monitoring feedback.*

***Keywords**: Prime Number, Information Time Device, P and Q*