Penerapan Kombinatorial dalam Menentukan Tingkat Keamanan Password PIN dan *Pattern* Handphone

Ananda Yulizar Muhammad 13518088
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13518088@std.stei.itb.ac.id

***Abstract*—Zaman sekarang, *smartphone* sudah menjadi sebuah barang yang dimiliki oleh hampir semua orang, mulai dari anak-anak sampai orang dewasa. Hal tersebut dikarenakan fungsi *smartphone* yang beragam mulai dari bermain *game,* menonton video, menyimpan data, mengurus bisnis, dan lain-lain. Tidak jarang pula sebuah *smartphone* mengandung data-data yang krusial bagi pemilik *smartphone* tersebut. Oleh karena itu, dibutuhkan keamanan yang mumpuni bagi *smartphone* tersebut dalam bentuk *password* supaya *smartphone* tersebut tidak dibuka oleh sembarang orang. Bentuk *Password* yang tersedia pada suatu *smartphone* beragam dengan tingkat keamanan yang berbeda-beda. Pada makalah ini, saya akan mengaplikasikan teori kombinatorial untuk menentukan bentuk *password* yang lebih aman dibanding yang lain.**

***Keywords—Smartphone, Password,* Keamanan, Kombinatorial**

I. PENDAHULUAN

Pada zaman sekarang, *smartphone* sudah menjadi sebuah barang yang dimiliki oleh hampir semua orang, mulai dari anak-anak hingga orang dewasa. Hal tersebut dikarenakan smartphone sudah hampir menjadi seperti sebuah komputer versi kecil yang lebih mudah untuk digunakan. Smartphone dapat digunakan untuk memenuhi berbagai macam keperluan, seperti bermain *game*, menonton video, mengurus pekerjaan, sumber bahan belajar, dan lain-lain. *Smartphone* sudah menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari kita.

Tidak jarang pula sebuah *smartphone* mengandung data-data yang krusial bagi pemiliknya yang akan membahayakan dirinya apabila dilihat atau bahkan dicuri oleh pihak lain. Oleh karena itu, sebuah *smartphone* membutuhkan sistem keamanan yang mumpuni untuk mencegah terjadinya hal seperti itu. Salah satu sistem keamanan yang disediakan oleh *smartphone* adalah *password* untuk dapat mengakses *smartphone* tersebut. Jenis *password* pada *smartphone* pun beragam, terdapat *Fingerprint Lock*, *Pin*, *Pattern*, dan *Password* (gabungan antara alfabet, angka, dan karakter khusus). *Fingerprint Lock* dapat dijadikan sebuah pilihan kedua untuk menjadi *password smartphone* tidak seperti tiga lainnya. Di antara tiga lainnya, jelas bentuk Password lebih aman dibandingkan pin dan pattern karena kemungkinan yang jelas lebih banyak. Namun, antara pattern dan pin, yang manakah yang lebih aman? Apabila ada seseorang yang memiliki banyak waktu luang dan mencoba segala jenis kemungkinan yang ada dalam kedua jenis *password* tersebut, yang manakah yang membutuhkan waktu lebih lama untuk dicoba semua kemungkinannya sehingga lebih aman?

Pada makalah ini, penulis akan membahas masalah ini dengan mengaplikasikan ilmu yang didapat dari ata kuliah IF2120 Matematika Diskrit, yaitu materi kombinatorial untuk menentukan tingkat keamanan *password smartphone.*

II. LANDASAN TEORI

A. Kombinatorial

Kombinatorial *(combinatoric)* adalah cabang matematika yang mempelajari mengenai pengaturan objek-objek. Kombinatorial bertujuan untuk mencari solusi jumlah cara dalam mengatur objek-objek yang bersangkutan dalam himpunannya. Sebenarnya, pengaturan objek-objek dapat diselesaikan dengan menggunakan metode enumerasi, yaitu menghitung atau mencacah semua kemungkinan jawaban yang ada. Metode ini masih dapat digunakan untuk persoalan dengan jumlah objek yang sedikit, tetapi untuk persoalan dengan jumlah objek yang banyak, metode enumerasi sudah tidak lagi efektif karena kemungkinan jawaban yang banyak juga. Oleh karena itu, dengan menggunakan kombinatorial, kita dapat menyelesaikan persoalan seperti ini dengan cepat tanpa perlu mencacah satu persatu kemungkinan jawaban yang ada.

1. Kaidah Dasar Menghitung

   Dalam menghitung semua kemungkinan pengaturan objek dengan menggunakan kombinatorial, terdapat 2 kaidah dasar. Kedua kaidah dasar tersebut adalah kaidah perkalian (*rule of product)* dan kaidah penjumlahan (*rule of sum).*

   a. Kaidah Perkalian (Rule of Product)

      Apabila pada percobaan 1 terdapat p kemungkinan jawaban, dan pada percobaan 2 terdapat q kemungkinan jawaban, maka apabila percobaan 1 dan percobaan 2 dilakukan, maka percobaan tersebut akan menghasilkan sebanyak $p \times q$ kemungkinan jawaban . Kata kunci dari kaidah perkalian adalah kata ‘dan’.

   b. Kaidah Penjumlahan (Rule of Sum)

      Apabila pada percobaan 1 terdapat p kemungkinan jawaban, dan pada percobaan 2 terdapat q kemungkinan jawaban, maka apabila

percobaan 1 atau percobaan 2 dilakukan (hanya satu saja percobaan yang dilakukan), maka terdapat $p + q$ kemungkinan jawaban yang dapat dihasilkan. Kata kunci pada kaidah penjumlah adalah kata 'atau'.

Apabila terdapat lebih dari 2 percobaan, misalkan terdapat *n* buah percobaan dan masing-masing percobaan mempunyai $p_1, p_2, ..., p_n$ kemungkinan yang dapat terjadi yang setiap p_i tidak bergantung satu sama lain, maka jumlah hasil percobaan yang mungkin terjadi adalah:

1. $p_1 \times p_2 \times ... \times p_n$ untuk kaidah perkalian.
2. $p_1 + p_2 + ... + p_n$ untuk kaidah penjumlahan.

2. Teori Permutasi

Menurut referensi [1], permutasi adalah jumlah urutan berbeda dari pengaturan objek-objek. Permutasi merupakan bentuk khusus aplikasi aturan perkalian. Misalkan jumlah objek adalah *n*, maka urutan pertama dipilih dari *n* objek, urutan kedua dipilih dari $n - 1$ objek, urutan ketiga dipilih dari $n - 2$ objek, begitu seterusnya, dan urutan terakhir dipilih dari 1 objek yang tersisa. Menurut kaidah perkalian, permutasi dari *n* objek adalah

$$n(n-1)(n-2)\ldots(2)(1) = n!$$

Apabila terdapat penyusunan sebanyak *r* objek yang dipilih dari *n* objek, banyaknya sususan berbeda dari penyusunan *r* objek yang diambil dari *n* objek dilambangkan dengan *P(n, r)* yang dapat dihitung dengan

$$P(n,r) = \frac{n!}{(n-r)!}$$

3. Teori Kombinasi

Terdapat bentuk lain dari permutasi, yaitu kombinasi. Apabila permutasi memperhitungkan urutan dalam penyusunan objek, maka pada kombinasi urutan kemunculan tidak diperhitungkan. Misalkan urutan *abc* dan *bca* dianggap sama dalam kombinasi.

Dalam penyusunan *r* objek yang dipilih dari *n* objek, banyaknya kemungkinan jawaban yang berbeda dari penyusunan *r* objek yang diambil dari *n* objek apabila urutan penempatan objek diabaikan dilambangkan dengan *C(n, r)* yang dapat dihitung dengan

$$C(n,r) = \frac{n!}{r!\,(n-r)!}$$

4. Peluang Diskrit

Peluang merupakan seberapa besar kemungkinan suatu kejadian yang diinginkan dapat terjadi dari sejumlah kejadian-kejadian lain yang mungkin terjadi. Peluang terkait erat dengan kombinatorial.

Himpunan semua kemungkinan hasil dari percobaan diseut ruang contoh (*sample space)* dari percobaan yang bersangkutan. Setiap anggota dari himpunan tersebut yang merupakan hasil dari percobaan disebut dengan titik contoh (*sample point).* Tiap-tiap dari titik contoh bersifat saling terpisah karena dari seluruh ruang contoh, hanya satu titik contoh yang muncul.

Misalkan ruang contoh dilambangkan dengan S dan titik-titik contohnya dilambangkan dengan $x_1, x_2, ...$, maka

$$S = \{x_1, x_2, ..., x_i, ...\}$$

Menyatakan ruang contoh S yang terdiri dari titik-titik contoh $x_1, x_2, ..., x_i$ dan seterusnya. Ruang contoh yang jumlah titik contohnya terbatas disebut dengan ruang contoh diskrit (*discrete sample space).* Peluanh terjadinya sebuah titik contoh dinamakan peluang diskrit yang dilambangkan dengan $p(x_i)$.

Menurut referensi [1], misalkan x_i adalah sebuah titik contoh di dalam ruang contoh S. Peluang bagi x_i adalah ukuran kemungkinan terjadinya atau munculnya x_i di antara titik-titik contoh yang lain di dalam S.

Peluang diskrit mempunyai sifat-sifat sebagai berikut:

1. $0 \leq (x_i) \leq 1$, yaitu nilai peluang adalah bilangan positif dan selalu lebih kecil atau sama dengan 1.
2. $\sum_{i=0}^{S} p(x_i) = 1$, yaitu jumlah dari peluang semua titik contoh dalam ruang contoh S adalah 1.

Kejadian (*event)* adalah himpunan bagian dari ruang contoh yang dilambangkan dengan *E.* Kejadian yang hanya menganfung satu titik contoh disebut kejadian sederhana (*simple event)* dan kejadian yang mengandung lebih dari satu titik contoh disebut kejadian majemuk (*compound event).*

Peluang kejadian *E* di dalam ruang contoh *S* adalah

$$p(E) = |E|/|S|$$

Konsep-konsep dari teori himpunan dapat diterapkan pada peluang diskrit. Misalkan terdapat dua buah himpunan A dan B yang merupakan dua buah kejadian di dalam ruang contoh S.

1. Kejadian bahwa A dan B terjadi sekaligus berarti sama dengan munculnya salah satu titik contoh dalam himpunan $A \cap B$. Peluang terjadinya kejadian A dan B adalah

$$P(\mathrm{A} \cap \mathrm{B}) = \sum_{x_i \in A \cap B} p(x_i)$$

2. Kejadian bahwa A atau B atau keduanya terjadi berarti sama dengan munculnya salah satu titik contoh di A *U* B. Peluang terjadinya kejadian A atau B atau keduanya adalah

$$P(\mathrm{A} \cup \mathrm{B}) = \sum_{x_i \in A \cup B} p(x_i)$$

3. Kejadian bahwa A terjadi tetapi B tidak berarti sama dengan munculnya salah satu titik contoh di dalam *A – B.* Peluang terjadinya kejadian A tetapi

B tidak adalah

$$P(\mathrm{A}-\mathrm{B}) = \sum_{x_i \in A-B} p(x_i)$$

4. Kejadian bahwa salah satu dari A dan B terjadi namun bukan keduanya berarti sama dengan munculnya salah satu titik contoh di dalam A $\oplus$ B. Peluang terjadinya salah satu dari A dan B namun bukan keduanya adalah

$$P(\mathrm{A} \oplus \mathrm{B}) = \sum_{x_i \in A \oplus B} p(x_i)$$

5. Peluang bahwa kejadian komplemen dari A terjadi adalah

$$P(\bar{A}) = 1 - p(A)$$

B. *Smartphone*

Smartphone adalah sebuah telepon seluler yang memiliki tambahan-tambahan fitur yang bukan untuk telepon seluler pada umumnya, seperti sistem operasi, *web browser*, dan aplikasi-aplikasi lainnya. *Smartphone* dapat digunakan baik untuk keperluan konsumsi maupun untuk keperluan bisnis dan sekarang merupakan suatu hal yang tidak dapat dilepaskan dari kehidupan sehari-hari.

1. Penggunaan *Smartphone*

Pada umumnya, *Smartphone* digunakan untuk berkomunikasi dengan teman, keluarga, dan lainnya melalui media sosial. Media-media sosial seperti Facebook, Instagram, Twitter dan lain-lain termasuk ke dalam aplikasi-aplikasi yang dapat dijalan oleh sebuah *smartphone* yang dapat diunduh dari *app store* yang tersedia.

Penggunaan *smartphone* lainnya adalah untuk kesehatan, seperti melacak aktivitas olahraga dari pengguna, detak jantung pengguna, berat badan, dan lain-lain. Biasanya, hal ini didukung oleh perangkat lain seperti *smartwatch* untuk memonitor hal-hal tersebut.

M-banking juga merupakan suatu nilai tambah dari *smartphone*. Hal ini memudahkan pengguna saat ingin mentransfer ke rekening lain ataupun untuk sekedar cek saldo dari rekening tanpa harus keluar rumah dan mencari ATM. Selain *m-banking*, sekarang juga sudah terdapat 'dompet digital' sehingga kita dapat bertransaksi tanpa menggunakan uang fisik. Beberapa contoh dari 'dompet digital' adalah Ovo, Gopay, dan lain-lain.

2. Fitur Utama *Smartphone*

Hal yang membedakan *smartphone* dengan telepon seluler biasa adalah fitur-fiturnya. *Smartphone* bisa dibilang sebagai sebuah komputer versi kecil yang dapat dibawa dan digunakan di semua tempat dengan mudah. Berikut merupakan beberapa fitur utama yang ada dalam sebuah *smartphone*.

- Koneksi internet
- *Browser*
- *Touchscreen*
- Koneksi Wi-fi
- Kamera
- GPS
- Fitur keamanan

3. Fitur Keamanan *Smartphone*

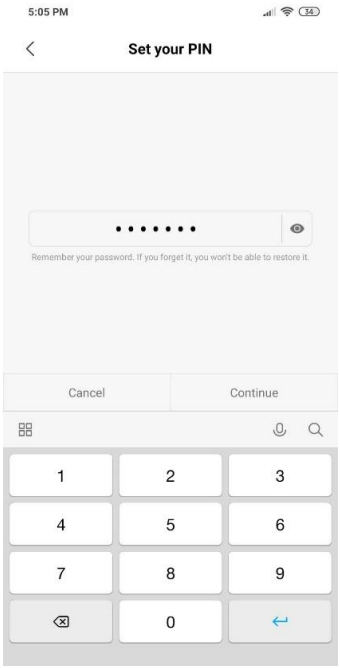
Karena *Smartphone* digunakan untuk berbagai macam hal mulai dari keperluan pribadi hingga keperluan bisnis, sebuah *smartpone* pasti memiliki data-data yang krusial bagi pemiliknya. Apabila data-data tersebut dicuri oleh pihak lain, maka akan berakibat buruk bagi pemiliknya. Oleh karena itu, diperlukan sistem keamanan yang mumpuni bagi sebuah *smartphone* untuk melindungi jatuhnya data-data tersebut ke pihak yang salah. Salah satu fitur keamanan dari smartphone adalah *screenlock.*

Screenlock atau layar kunci adalah saat sebuah *smartphone* ingin dinyalakan kembali setelah di-*lock* atau dikunci diperlukan sebuah *password* atau kata sandi untuk membuka kunci tersebut. Saat ini, bentuk *password* yang dimiliki oleh suatu *smartphone* sudah sangat mumpuni, seperti *facial recognition, fingerprint scanner, iris scanning* dan bentuk *password* lainnya. Namun, dalam makalah ini akan dibahas bentuk *password* yang tergolong lebih sederhana, yaitu PIN dan *Pattern.*

a. PIN

PIN (*Personal Identification Number)* merupakan bentuk *password* yang berbentuk serangkaian angka. PIN tergolong memiliki tingkat keamanan yang sedang hingga tinggi, tergantung dari panjang dan kompleksitasnya.

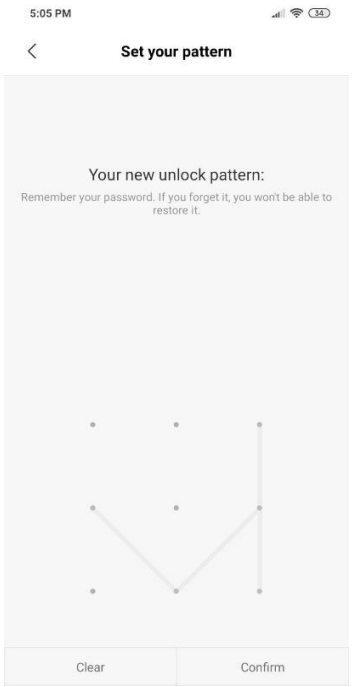
PIN populer di kalangan pengguna karena serangkaian angka yang digunakan mudah untuk diingatnya. Hal tersebut karena biasanya pengguna menggunakan serangkaian angka yang penting bagi mereka, seperti tanggal ulangtahun, tanggal pernikahan, dan lain-lain.



Gambar 1. Pengaturan password PIN pada Xiaomi Pocophone F1
(Sumber : Penulis)

b. *Pattern*

Patterm merupakan bentuk *password* yang menerima sebuah pola yang dibuat oleh pengguna. Pola tersebut dibuat dengan membuat serangkaian garis yang menghubungkan titik-titik yang tersedia. Jumlah titik-titik yang tersedia berjumlah 9 . *Pattern* tergolong keamanan tingkat sedang karena mayoritas pengguna memilih untuk menggunakan pola yang relatif mudah, tetapi *pattern* pun dapat dibuat sedemikian rupa sehingga terbentuk pola yang sulit.



Gambar 2. Screenshot Pengaturan password pattern pada Xiaomi Pocophone F1
(Sumber: Penulis)

Untuk menambah keamanan *smartphone,* apabila dalam memasukkan *password* terjadi kesalahan selama beberapa kali, maka sebuah tindakan tertentu akan dilakukan sesuai dengan prosedurnya pada tiap *smartphone*. Untuk *smarpthone* jenis *iPhone,* apabila salah memasukkan *password* untuk ke-6 kalinya, maka *iPhone* akan masuk mode *disabled* (tidak bisa dimasukkan *password* atau digunakan untuk apapun) selama 1 menit. Apabila 7 kali, akan *disabled* selama 5 menit. Untuk ke-8 kalinya, akan *disabled* selama 15 menit. Untuk ke-9 kalinya, selama 60 menit. Apabila telah salah selama 10 kali, kita harus menyambungkan *iPhone* kepada akun *iTunes* atau di-reset akan tetapi data pada *iPhone* akan hilang. Sedangkan untuk *smartphone* jenis *android*, apabila salah memasukkan *password* untuk ke-5 kalinya, *android* akan *disabled* selama 30 detik. Apabila salah memasukkan *password* untuk ke-10 kalinya, maka data dalam *android* tersebut akan dihapus dan *android* tersebut akan di-reset. Hal ini bertujuan untuk mencegah pihak yang tidak diinginkan dari mencoba-coba memasukkan semua kemungkinan kombinasi *password* yang ada.

III. PEMBAHASAN

Pada makalah ini, penulis akan menerapkan teori kombinatorial untuk mencari berapa banyak kemungkinan yang terdapat pada *password* bentuk PIN dan *pattern.* Penulis akan menggunakan *Smartphone* Xiaomi Pocophone F1 sebagai *smartphone* referensi pada makalah ini.

A. PIN

PIN menerima serangkaian angka sebagai bentuk *password*-nya. Banyak angka yang diterima berada dalam rentang 4 – 16 angka. Oleh karena itu, kita perlu banyaknya kemungkinan PIN yang dapat terbentuk pada setiap banyaknya angka yang digunakan kemudian dijumlahkan. Untuk mencari banyaknya kemungkinan PIN yang dapat dibentuk pada setiap banyaknya angka dapat kita hitung dengan menggunakan kaidah perkalian.

Misalkan banyaknya angka yang digunakan adalah n, banyaknya kemungkinan tiap angka dalam PIN adalah p_n ,dan banyaknya kemungkinan saat n adalah x_n ,maka banyaknya kemungkinan pada tiap banyaknya angka yang digunakan dengan menggunakan kaidah perkalian adalah

$$x_n = p_1 \times p_2 \times \ldots \times p_n$$

Karena banyaknya angka yang dapat digunakan berjumlah 10 angka, maka nilai p_i pasti selalu 10, sehingga persamaan x_n dapat diubah menjadi

$$x_n = 10^n$$

Berikut merupakan hasil perhitungan banyaknya kemungkinan PIN yang dapat dibuat berdasarkan nilai n dalam bentuk tabel.

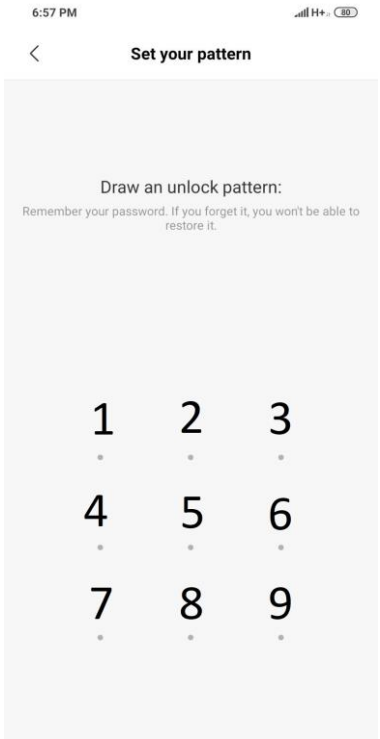
n	x_n
4	10^4
5	10^5
6	10^6
7	10^7
8	10^8
9	10^9
10	10^{10}
11	10^{11}
12	10^{12}
13	10^{13}
14	10^{14}
15	10^{15}
16	10^{16}

Tabel 1 Perhitungan banyaknya kemungkinan password jenis PIN

Dengan menggunakan kaidah penjumlahan, maka banyaknya kemungkinan *password* yang dapat dibentuk dengan PIN adalah $10^{16} + 10^{15} + 10^{14} + 10^{13} + 10^{12} + 10^{11} + 10^{10} + 10^9 + 10^8 + 10^7 + 10^6 + 10^5 + 10^4$ = 11.111.111.111.110.000 kemungkinan.

B. *Pattern*

Pattern menerima bentuk pola garis yang dibuat oleh pengguna dengan menghubungkan titik-titik yang disediakan. Terdapat 9 titik yang dapat digunakan, jumlah minimal titik-titik yang digunakan adalah sebanyak 4 titik, dan setiap titik hanya bisa digunakan sekali. Untuk mempermudah penghitungan, kita nomori setiap titik yang tersedia seperti pada gambar di bawah ini.



Gambar 3 Penomoran pada titik-titik password pattern pada Xiaomi Pocophone F1
(Sumber: Penulis)

Misalkan banyaknya titik yang digunakan adalah *n*, banyaknya kemungkinan tiap titik yang masih dapat digunakan adalah p_n ,dan banyaknya kemungkinan bentuk pola saat *n* adalah x_n , maka banyaknya kemungkinan pada tiap banyaknya titik yang digunakan dengan menggunakan kaidah perkalian adalah

$$x_n = p_1 \times p_2 \times \ldots \times p_n$$

Berbeda dengan PIN yang dapat menggunakan angka yang sama, jika dalam *pattern* titik yang telah digunakan tidak bisa digunakan lagi sehingga $p_i = p_{i-1} - 1$ untuk $i > 1$ dan $i \leq n$. Berikut merupakan hasil perhitungan banyaknya kemungkinan *pattern* yang dapat dibuat berdasarkan nilai *n* dalam bentuk tabel.

n	$p_1 \times p_2 \times \ldots \times p_n$	x_n
4	$4 \times 3 \times 2 \times 1$	4!
5	$5 \times 4 \times 3 \times 2 \times 1$	5!
6	$6 \times 5 \times 4 \times 3 \times 2 \times 1$	6!
7	$7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$	7!
8	$8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$	8!
9	$9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$	9!

Tabel 2 Perhitungan banyaknya kemungkinan password jenis pattern

Dengan menggunakan kaidah penjumlahan, maka banyaknya kemungkinan *password* yang dapat dibentuk dengan *pattern* adalah 9! + 8! + 7! + 6! + 5! + 4! = 409.104 kenungkinan.

IV. KESIMPULAN

Smartphone mengandung data-data yang krusial bagi penggunanya. Oleh karena itu, dibutuhkan sistem keamanan yang mumpuni bagi setiap *smartphone* supaya data-data milik penggunanya dapat dijamin keamanannya.

Dalam makalah ini, ditunjukkan mengenai berapa banyak kemungkinan *password* keamanan membuka *lock smarphone* dari jenis PIN dan *pattern.* Dari hasil perhitungan pada Bab III, dapat dilihat bahwa PIN memiliki kemungkinan *password* yang lebih banyak daripada *pattern* sehingga tingkat keamanan PIN lebih tinggi.

V. UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa karena atas rahmat dan karunia-Nya penulis dapat menyelesaikan makalah yang berjudul "Penerapan Kombinatorial dalam Menentukan Tingkat Keamanan Password PIN dan *Pattern* Handphone". Penulis ingin berterima kasih kepada Dr. Ir. Rinaldi Munir, MT. Yang telah membimbing penulis selama pembelajaran mata kuliah IF2120 Matematika Diskrit pada program studi teknik informatika Institut Teknologi Bandung. Penulis juga ingin

berterima kasih kepada seluruh sumber referensi yang dicamtumkan pada makalah ini sehingga makalah ini dapat mencantumkan informasi yang sebenar-benarnya.

REFERENSI

[1] Munir, Rinaldi. Matematika Diskrit, Bandung: Informatika, 2012, edisi ketiga.

[2] Rouse, Margaret. 2019. Smartphone. Diakses 4 Desember, 2019 pukul 14.00. https://searchmobilecomputing.techtarget.com/definition/smartphone

[3] Agumuoh, Fionna. 2019. Common Smartphone Security Features and How They Work. Diakses 4 Desember, 2019 pukul 14.10. https://www.online-tech-tips.com/smartphones/common-smartphone-security-features-and-how-they-work/

[4] Kobble, Matt. 2019. What Happens if You Enter The Wrong Password Into an iPhone Too Many Times?. Diakses 5 Desember 2019, 19.45 https://itstillworks.com/happens-enter-wrong-password-iphone-many-times-12293302.html

[5] Wallen, Jack. 2016. How to reset your Android lock screen password/PIN/pattern. Diakses 5 Desember 2019, 19.50. https://www.techrepublic.com/article/pro-tip-how-to-reset-your-android-lock-screen-passwordpinpattern/

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 5 Desember 2019

Ananda Yulizar Muhammad - 13518088