End-to-End Enkripsi dengan Menggunakan Diffie-Hellman *Key Exchange*

Ahmad Fajar Prasetiyo (13514053)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13514053@std.itb.ac.id

***Abstract*—Banyak aplikasi komunikasi yang ada pada saat ini. Hal ini terjadi karena banyak orang menggunakan internet. Internet digunakan karena murah jika dibandingkan dengan teknologi pendahulunya seperti SMS dan telepon. Tetapi kita harus dengan bijak dalam menggunakan internet. Ada beberapa skandal penyalahgunaan data kita. Salah satu contoh-nya adalah Facebook. Maka dari itu kita harus memilih aplikasi yang kita gunakan yang memperhatikan *security* data kita. Banyak cara dalam meningkatkan *security*. Salah satu cara untuk meningkatkan *security* adalah dengan menggunakan *end-to-end* enkripsi.**

***Keywords—Kriptografi, Kriptografi kunci publik, TCP/IP, Key Exchange*.**

I. Pendahuluan

Teknologi berkembang pesat pada zaman sekarang. Salah satu yang paling berkembang pesat adalah teknologi yang digunakan untuk berkomunikasi.

Teknologi komunikasi pertama kali adalah teknologi tradisional. Teknologi tradisional ini digunakan pada saat zaman kerajaan. Salah satu bukti teknologi ini pernah ada adalah ditemukan prasasti peninggalan kerajaan kuno.

Setelah dua setengah abad munculah mesin cetak. Mesin cetak ini ditemukan pada tahun 1688. Mesin cetak ini masuk ke Indonesia melalui Hindia Belanda. Setelah mesin cetak masuk ke Indonesia munculah surat kabar pertama yang berisi perjanjian antara Sultan Makasar dengan pemerintah Hindia Belanda.

Setelah mesin cetak masuk ke Indonesia, pada tahun 1855, masuk lagi Telegraf. Telegraf pertama kali digunakan untuk komunikasi antara Batavia (Jakarta) dan Buitenzorg (Bogor). Setelah itu Telegraf dapat dinikmati orang umum dengan adanya 28 kantor Telegraf berdiri di Nusantara.

Setelah itu masuk teknologi telepon pada tanggal 16 Oktober 1882. Awal mula telepon digunakan untuk menghubungkan wilayah Gambir dan Tanjung Priok. Setelah dua tahun dibangunlah jaringan telepon di daerah Semarang dan Surabaya.

Setelah itu munculah telepon genggam. Munculnya telepon genggam diawali dengan munculnya pager. Pada zaman sebelum reformasi pengguna pager ada sekitar 800.000 dan mulai mengalami penurunan terus menerus karena telepon genggam semakin berkembang.

Internet pertama kali muncul di Indonesia pada tahun 1990-an. Ameteur Radio Club ITB adalah meupakan cikal bakal dari munculnya Internet. Pada tahun 1992 munculah ITB bergabung ke dalam jaringan PaguyubanNet.

Munculnya internet merubah cara berkomunikasi. Awalnya internet pada saat itu hanya digunakan untuk mengirim *email*. Seiring dengan berjalannya waktu pada tahun 2007 Apple memperkenal iPhone yang merupakan *smartphone* yang ada pada saat ini. Pada saat itu menggeser pasar symbian yang menyebabkan Nokia menjadi bangkrut.

Smartphone lebih dipilih masyarakat karena murah dan memiliki banyak fitur jika dibandingkan dengan telepon genggam jaman dahulu. Jaman dahulu orang menggunakan SMS atau telepon untuk berkomunikasi. SMS dan telepon akan menjadi sangat mahal jika dilakukan berbeda *provider*.

Jika dibandingkan dengan *smartphone* yang menggunakan internet, *smartphone* akan sangat murah karena menggunakan internet. Jika menggunakan internet kita tidak perlu khawatir jika berkomunikasi dengan yang berbeda *provider* karena akan sama saja.

Dengan munculnya *smartphone* muncullah aplikasi-aplikasi untuk berkomunikasi. Ada yang berasal dari dalam negeri atau dari luar negeri. Aplikasi-aplikasi komunikasi ini akan memudahkan kita untuk berkomunikasi dengan orang yang memiliki aplikasi tersebut. Ada beberapa aplikasi yang terkenal salah satu contohnya Facebook.

Facebook merupakan social media yang sangat populer pada jaman sekarang. Tetapi pada tahun 2018 Facebook mendapatkan scandal karena telah menjual data pengguna Facebook ke pihak ketiga. Facebook memiliki semua data pengguna Facebook.

Dari kejadian Facebook kita harus belajar bahwa salah satu yang paling penting adalah *security*. Beberapa aplikasi untuk komunikasi menerapkan *security* yang sangat bagus, bahkan

ditaruh sebagai *tagline*-nya. Salah satu aplikasi komunikasi yang sangat memperhatikan *security* adalah Slack. Slack sangat konsentrasi dengan masalah *security*. Hal ini yang menyebabkan Slack dapat bersaing dengan perusahaan yang sudah besar duluan seperti Whatsapp, Line dan WeChat.

Salah satu yang diterapkan dalam Slack adalah *end-to-end* enkripsi sehingga Slack sendiri tidak mengetahui percakapan pengguna Slack. Sistem yang diterapkan Slack sangat bagus sehingga beberapa perusahaan besar di dunia lebih memilih menggunakan Slack dari pada aplikasi komunikasi yang lain.

Pada makalah ini akan dibahas sistem *end-to-end* enkripsi. *End-to-end* enkripsi ini terinspirasi dengan *handshake* yang dimiliki oleh TCP/IP. Pertukaran kunci yang digunakan menggunakan Diffie-Hellman *Key Exchange*. Sedangkan untuk enkripsi-nya menggunakan AES.

II. Dasar Teori

Pada bab ini akan dibahas teori-teori yang mendukung rancangan *end-to-end* enkripsi dengan menggunakan Diffie-Hellman *Key Exchange*. Hal yang akan dibahas pada bab ini adalah Diffie-Hellman *Key Exchange*, TCP/IP *handshake* dan algoritma enkripsi AES.

A. Diffie-Hellman Key Exchange

Algoritma ini ditemukan oleh dua orang kriptografer Amerika yang sangat terkenal yaitu Whitfield Diffie dan Martin Hellman. Kedua orang tersebut merupakan pelopor kriptografi kunci publik. Algoritma kunci publik muncul karena sulitnya untuk bertukar kunci rahasia.

Algoritma ini hanya digunakan untuk pertukaran kunci saja. Setelah orang yang akan berkomunikasi sama-sama mendapatkan kunci akan dilakukan enkripsi seperti biasa.

Algoritma ini kuat berdasarkan pada sulitnya untuk menghitung logaritma diskrit. Jadi ketika orang sudah menemukan cara yang cepat untuk menghitung logaritma diskrit algoritma ini sudah tidak dapat dipakai lagi atau sudah tidak aman lagi jika digunakan.

Misal Bob dan Alice ingin melakukan komunikasi. Pertama yang harus dilakukan adalah Bob dan Alice harus menyepakati bilangan prima yang besar n dan g. Bilangan prima n dan g harus memiliki sifat $g < n$.

Bilangan prima n dan g tidak bersifat rahasia. Alice dan Bob juga bisa menyepakati bilangan prima n dan g menggunakan jaringan komunikasi yang tidak aman.

Langkah-langkah Diffie-Hellman *Key Exchange*:

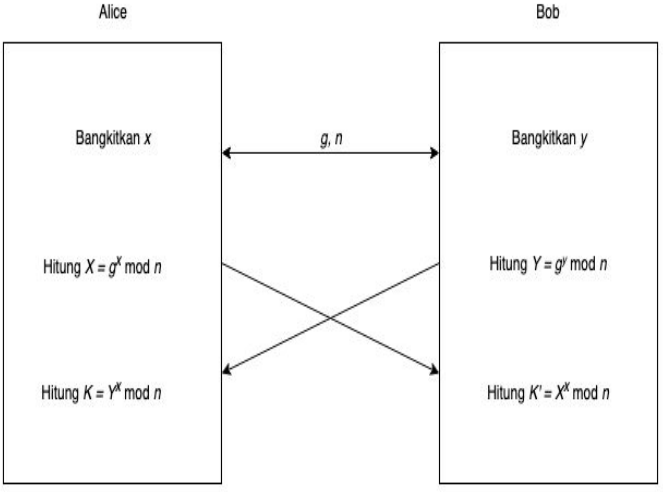
1. Pertama Alice akan membangkitkan bilangan acak yang besar x. Alice juga harus menghitung X yang mana:

   $X = g^x \bmod n$

   Hasil perhitungan dari Alice ini akan dikirimkan ke Bob.
2. Kedua Bob juga akan membangkitkan bilangan acak yang besar y. Bob juga harus menghitung Y yang mana:

   $Y = g^y \bmod n$

   Hasil perhitungan dari Bob akan dikirim ke Alice.
3. Ketiga setelah Alice mendapatkan Y dari Bob, Alice akan menghitung:
   $K = Y^x \bmod n$
4. Keempat setelah Bob mendapatkan X dari Alice, Bob akan menghitung:
   $K' = X^y \bmod n$



Sumber: Slide Kuliah IF4020 Kriptografi: Algoritma Pertukaran Kunci Diffie-Hellman

Gambar 1: Pertukaran Kunci Diffie-Hellman

Dari proses di atas dapat kita lihat bahwa nilai K dan nilai K' memiliki nilai yang sama. Karena nilai K dan nilai K' memiliki nilai yang sama maka mereka memiliki kunci yang sama sehingga Alice dan Bob dapat melakukan enkripsi dengan memiliki kunci yang sama.

Jika ada orang yang akan melakukan penyadapan, orang hanya akan mendapatkan g, n, X dan Y. Dari yang didapatkan orang tidak bisa untuk merekonstruksi nilai K. Untuk merekonstruksi nilai K orang harus memiliki x dan y. Untuk mendapatkan nilai x kita harus melakukan perhitungan logaritma nilai X, begitupun juga untuk mendapatkan nilai y.

Sehingga algoritma ini akan tetap aman jika orang belum bisa menghitung nilai logaritma dari suatu bilangan.

B. TCP/IP handshake

Dulu belum ada sebelum ada TCP/IP komputer berkomunikasi dengan cara yang berbeda-beda. Setiap komputer hanya terhubung ke jaringan lokal.

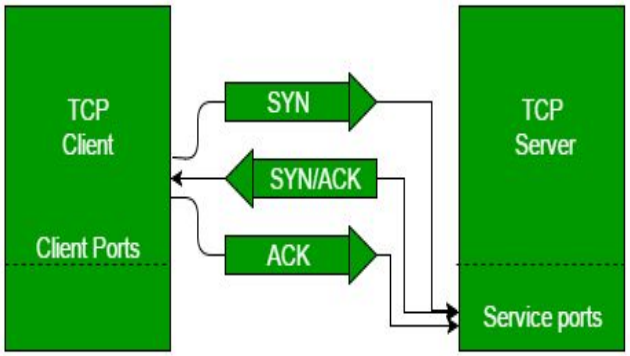
TCP/IP pertama kali ditulis pada 1973 dan diumumkan resmi di dokumen RFC 675, *Specification of Internet Transmission Control Program*, pada Desember 1974.

TCP/IP memungkinkan semua komputer dapat terhubung, karena semua komputer dapat terhubung maka munculah internet. Hampir semua komputer sekarang berkomunikasi dengan TCP/IP walaupun itu hanya untuk komunikasi jaringan lokal.

Sebelum komputer berkomunikasi satu dengan yang lain komputer akan melakukan *handshake*. *Handshake* ini dilakukan agar dapat tercipta koneksi antara dua komputer. *Handshake* pada TCP/IP biasa disebut dengan TCP 3-*Way Handshake*.

Proses dilakukannya TCP 3-*Way handshake:*

1. Client akan mengirimkan sinyal SYN.
2. Server yang menerima sinyal SYN dari client akan membalas dengan ACK/SYN.
3. Client yang menerima sinyal ACK/SYN dari server akan membalas dengan ACK.



Sumber:
https://www.geeksforgeeks.org/computer-network-tcp-3-way-handshake-process/

Gambar 2: Proses 3-*Way Handshake*

Setelah proses 3-*Way Handshake* dilakukan komputer akan bisa mengirim data dengan komputer lainnya. Proses ini terjadi 3 tahap sehingga proses ini dinamakan dengan 3-*Way Handshake*.

C. AES

AES (*Advanced Encryption Standard)* merupakan algoritma kriptografi standard pada saat ini. AES ada karena DES (*Data Encryption Standard)* dinilai sudah tidak aman lagi.

National Institute of Standards and Technology (NIST) mengusulkan untuk membuat algoritma kriptografi standard yang baru untuk menggantikan DES. NIST mengadakan lomba untuk membuat algoritma kriptografi standard yang baru yang kelak akan diberi nama AES.

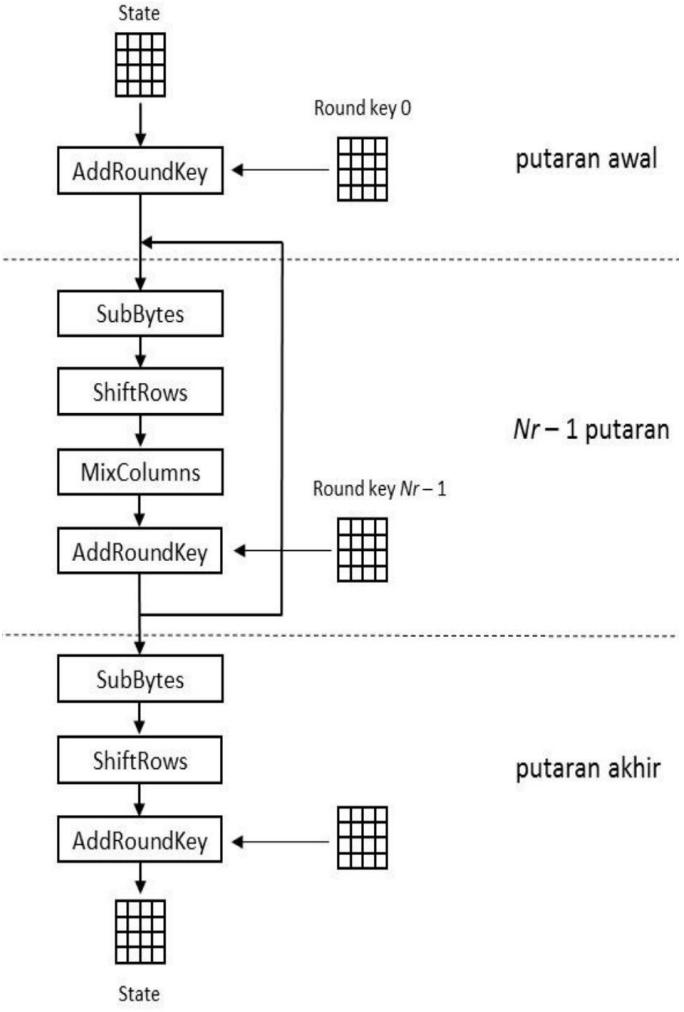
Persyaratan AES yang diberikan NIST adalah:

1. Algoritma harus merupakan algoritma simetris dan termasuk dalam kelompok *block cipher*.
2. Tidak ada yang dirahasiakan, seluruh rancangan algoritma yang digunakan harus publik.
3. Panjang kunci 128, 192, dan 256 bit.
4. Ukuran blok yang dienkripsi adalah 128 bit.
5. Algoritma dapat diimplementasikan secara efisien sebagai *software* maupun sebagai *hardware*.

Masuklah lima finalis yaitu *Rijndael* (dari Vincent Rijmen dan Joan Daemen – Belgia, 86 suara), *Serpent* (dari Ross Anderson, Eli Biham, dan Lars Knudsen – Inggris, Israel, dan Norwegia, 59 suara), *Twofish* (dari tim yang diketuai oleh Bruce Schneier – USA, 31 suara), *RC6* (dari Laboratorium RSA – USA, 23 suara), dan *MARS* (dari IBM, 13 suara). Pada bulan Oktober 2000 NIST mengumumkan bahwa *Rijndael* sebagai pemenangnya. Pada tahun 2001 November *Rijndael* ditetapkan sebagai AES.

Secara garis besar AES terdiri atas tiga tahapan yaitu :

1. Putaran awal yaitu melakukan XOR plaintext dengan Round key 0.
2. Putaran ke n-1 yaitu melakukan SubBytes, ShiftRows, MixColumns dan AddRoundKey.
3. Putaran ke n yaitu melakukan SubBytes, ShiftRows dan AddRoundKey.



Sumber: Slide Kuliah IF4020 Kriptografi: Advanced Encryption Standard

Gambar 3: Proses Enkripsi AES

Proses AddRoundKey merupakan proses untuk melakukan XOR antara Plaintext dengan RoundKey. Proses SubBytes merupakan proses melakukan substitusi *bytes* dengan menggunakan s-box. ShiftRows merupakan pergeseran baris-baris *array* secara *wrapping*. MixColumns merupakan data di masing-masing kolom.

III. Rancangan Algoritma

Pada bab ini akan dibahas secara detail rancangan dari *end-to-end* Enkripsi dengan Menggunakan Diffie-Hellman *Key Exchange* yang akan diterapkan pada aplikasi *chatting*. Terdapat tiga bagian pada bab ini yaitu Pertukaran Kunci, Rancangan Basis Data, Rancangan Arsitektur.

A. Pertukaran Kunci

Pertukaran kunci yang digunakan pada makalah ini sangat mirip dengan pertukaran kunci yang digunakan oleh Diffie-Hellman. Seandainya Alice ingin mengirim pesan kepada Bob, Alice akan menggunakan *share key* yang sudah dilakukan sebelumnya.

Jika Alice belum pernah mengirim pesan ke Bob, Alice akan melakukan proses pertukaran kunci. Prosesnya yang akan terjadi:

1. Alice akan membangkitkan *n,g,* dan *x*. Setelah itu Alice akan menghitung nilai $X = g^x \bmod n$.
2. Alice akan mengirimkan nilai *n, g* dan *X* ke Bob.
3. Setelah Bob menerima itu Bob akan membangkitkan nilai *y* dan Bob akan menghitung nilai $Y = g^y \bmod n$. Selain itu Bob akan menghitung nilai $K = X^y \bmod n$. Nilai *K* akan disimpan ke *device* Bob, sementara nilai *Y* akan dikirimkan ke Alice.
4. Alice yang mendapatkan nilai *Y* dari Bob akan melakukan perhitungan juga nilai $K' = Y^x \bmod n$. Setelah itu Alice akan menyimpan nilai *K'*.
5. Karena nilai $K = K'$ maka Bob dan Alice sudah memiliki kunci yang sama sehingga Bob dan Alice dapat berkomunikasi dengan menggunakan kunci tersebut.

B. Rancangan Basis Data

Pada rancangan basis data terdiri atas 3 bagian yaitu pengguna, pesan, dan token firebase.

Pesan
id_pengguna_pengirim: integer
id_pengguna_penerim: integer
pesan: string

Tabel 1: Basis Data Pesan

Pengguna
id: integer
nama: string

Tabel 2: Basis Data Pengguna

Token Firebase
id_pengguna: integer
token: string

Tabel 3: Basis Data Token Firebase

Pada tabel pesan berisi id_pengirim, id_penerima dan pesan yang dikirim. Pada kolom id_pengirim didapatkan pada tabel pengguna, begitupun id_penerima didapatkan dari tabel pengguna. Pesan yang disimpan dalam tabel pesan dalam bentuk *ciphertext* sehingga pemilik layanan tidak akan tahu pesan yang dikirim. Hanya yang memiliki kunci saja yang dapat melakukan dekripsi, sementara kunci hanya dimiliki di pengguna dan disimpan pada *device* pengguna sehingga hanya pengguna saja yang dapat melakukan dekripsi.

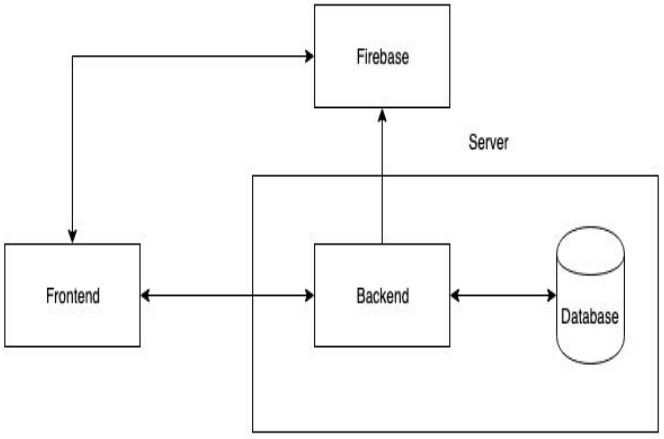
Pada tabel pengguna terdapat dua kolom yaitu kolom id dan kolom nama. Hal ini dilakukan untuk mengidentifikasi pengguna dalam melakukan pengiriman pesan. Kolom id merupakan *primary key* yang bernilai integer yang melakukan incremental setiap ada penambahan data pada tabel ini.

Pada tabel token firebase digunakan untuk menyimpan token firebase setiap pengguna. Token firebase ini digunakan untuk mengirim pesan secara *realtime* ke pengguna. Pada tabel token firebase berisi dua kolom yaitu id_pengguna yang didapatkan pada tabel pengguna dan token yang didapatkan pada saat pengguna melakukan *request* token ke Firebase.

C. Rancangan Arsitektur

Pada rancangan arsitektur ini merupakan rancangan yang digunakan untuk melakukan *chatting*. Aplikasi *chatting* yang

biasa juga bisa menggunakan rancangan ini.



Gambar 3: Rancangan Arsitektur Aplikasi *chatting*

Terdapat 3 komponen pada arsitektur ini. Komponen-komponen tersebut saling berkomunikasi seperti satu dengan yang lainya.

Komponen yang pertama adalah komponen Frontend. Frontend dapat berupa web ataupun aplikasi *mobile*. Frontend ini yang berhubungan langsung dengan pengguna.

Frontend terdapat beberapa hubungan. Pertama hubungan Frontend dengan Firebase yaitu Frontend melakukan request token ke Firebase yang akan digunakan untuk mengirim pesan. Selain itu Frontend juga menerima pesan yang dikirim oleh pengguna lain melalui Firebase. Frontend juga berhubungan dengan Server yang digunakan untuk menyimpan token Firebase yang digunakan dan Frontend jika ingin mengirim pesan akan pesan juga akan dikirim melalui Server.

Komponen yang kedua adalah Server. Komponen ini terdiri antara Backend dan Database. Backend digunakan untuk berhubungan dengan pihak lain sementara database digunakan untuk menyimpan data.

Backend berhubungan langsung dengan Frontend dan Firebase. Hubungan Backend dengan Frontend adalah untuk menyimpan data pengguna dan untuk menyimpan pesan yang dikirimkan oleh pengguna. Hubungan Backend dengan Firebase adalah untuk meneruskan pesan yang dikirimkan pengguna ke pengguna yang lain.

Firebase merupakan servis yang ditawarkan oleh Google dalam membantu kita untuk membuat aplikasi yang *realtime*. Banyak servis yang ditawarkan Firebase untuk membuat aplikasi yang *realtime* tetapi pada makalah kali ini hanya akan dipakai FCM. FCM digunakan untuk mengirim pesan antar *device* dengan melakukan identifikasi token yang digunakan.

IV. Kesimpulan

Disini dapat disimpulkan bahwa *security* merupakan hal yang penting saat ini. Hal ini dikarenakan semakin terbukanya akses ke dunia luar. Salah satu contoh meningkatkan *security* adalah dengan menggunakan *end-to-end* enkripsi sehingga pemilik server tidak mengetahui data yang dimiliki oleh pengguna.

Pada makalah ini dirancang bahwa server tidak pernah menyimpan kunci yang dimiliki oleh pengguna. Selain itu dengan menggunakan Diffie-Hellman *Key Exchange* server tidak pernah menerima kunci pengguna secara langsung.

References

[1] https://pakarkomunikasi.com/perkembangan-teknologi-komunikasi-di-indonesia diakses tanggal 09 Mei 2019.

[2] https://id.techinasia.com/talk/kejadian-penting-perkembangan-smartphone diakses tanggal 10 Mei 2019.

[3] https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook diakses tanggal 10 Mei 2019.

[4] http://www.tcpipguide.com/free/t_TCPIPOverviewandHistory.htm diakses tanggal 10 Mei 2019.

[5] https://www.geeksforgeeks.org/computer-network-tcp-3-way-handshake-process/ diakses tanggal 10 Mei 2019.

[6] Munir, Rinaldi. 2019. Slide Kuliah IF4020 Kriptografi: Algoritma Pertukaran Kunci Diffie-Hellman.

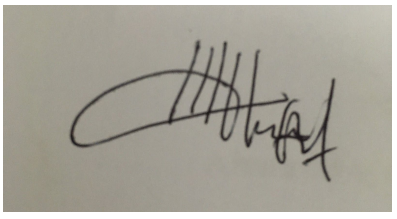
[7] Munir, Rinaldi. 2019. Slide Kuliah IF4020 Kriptografi: Secure Socket Layer.

[8] Munir, Rinaldi. 2019. Slide Kuliah IF4020 Kriptografi: Advanced Encryption Standard.

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, 10 Mei 2019



Ahmad Fajar Prasetiyo (13514053)