JUIT Vol 1 No. 1 Januari 2022 | P-ISSN: 2828-6936 E-ISSN: 2828-6901, Page 42-46

HAKIKAT DAN FILSAFAT ILMU KRIPTOGRAFI

Rizki Ariyani
Ilmu Komputer dan Teknologi Informasi, rizkiariyani@staff.gunadarma.ac.id, Universitas Gunadarma

ABSTRAK

The foundation of a science is a fundamental thing that must be known. The essence of a science is the foundation of that science. The essence and philosophy are interconnected in knowledge, so in a science, the origins of the development of knowledge can be understood. The science that is currently developing is certainly driven by the nature and philosophy of that science, which serves as the basis for research development. Cryptography is one of the sciences developed based on mathematics applied to the security of communication. Cryptography currently encompasses the security of communication in information technology. The discussion of this research is about the thoughts and opinions from the literature related to the nature and philosophy of cryptography, its history, development, and its application as security in information technology.

Keywords: Essence, Philosophy, Cryptography

Abstrak

Dasar dari sebuah ilmu merupakan hal pokok yang harus diketahui. Hakikat dari sebuah ilmu merupakan hal yang menjadi dasar dari ilmu tersebut. Hakikat dan filsafat saling berkaitan dalam pengetahuan sehingga dalam sebuah ilmu dapat diketahui asal muasal perkembangan ilmu pengetahuan. Ilmu yang berkembang saat ini pasti didorong oleh hakikat dan filsafat ilmu tersebut yang menjadi basis perkembangan penelitian. Ilmu kriptografi merupakan salah satu ilmu yang dikembangkan berdasarkan ilmu matematika yang diterapkan untuk keamanan dari sebuah komunikasi. Kriptografi saat ini meliputi keamanan komunikasi dari teknologi informasi. Pembahasan penelitian ini tentang pemikiran dan pendapat dari litaratur yang berkaitan dengan hakikat dan filsafat ilmu kriptografi, sejarahnya, perkembangan hingga pemanfaatannya sebagai keamanan pada teknologi informasi.
Kata Kunci: Hakikat, Filsafat, Kripografi

1. PENDAHULUAN

Ilmu yang berkembang saat ini merupakan hasil proses perjalanan pemikiran dari orang terdahulu yang terus dipelajari dan dikembangkan sedemikian rupa. Sebuah ilmu terdiri dari tiga landasan pemikiran yaitu hakikat (ontologis) pengetahuan, bagaimana pengetahuan tersebut (epistimologis), dan nilai guna pengetahuan (aksiologis) untuk kehidupan manusia [1]. Hakikat dari suatu ilmu juga selalu mendasari dalam perkembangan ilmu tersebut. Hal ini berlaku untuk semua bidang ilmu pengetahuan.

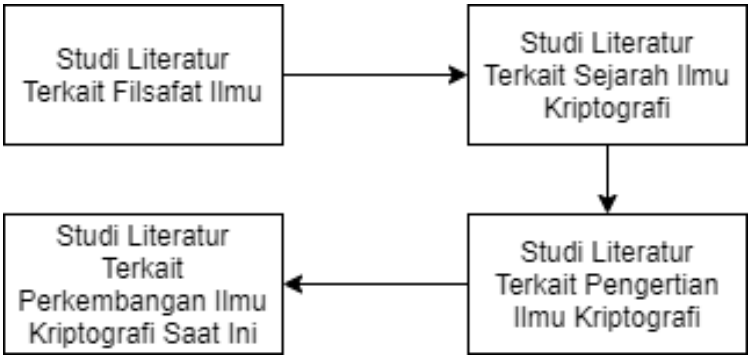
Perkembangan suatu ilmu selalu berlandaskan filsafat ilmu. Filsafat merupakan suatu dogma untuk mencari suatu keabsahan objek dengan dasar berpikir secara radikal [1]. Filsafat memiliki ciri yaitu menyeluruh, mendasar, dan spekulatif. Filsafat ilmu ditujukan untuk mendapatkan penafsiran tentang ilmu secara jelas, benar dan lengkap [2]. Filsafat ilmu merupakan pengetahuan metodis, sistematis dan koheren tentang seluruh kenyataan dalam suatu bidang ilmu [3].

Filsafat ilmu adalah cabang dari ilmu filsafat dimana sebuah ilmu secara khusus diletakkan sebagai objek meterial [4]. Filsafat ilmu selalu berkontribusi dalam terciptanya suatu ilmu. Hal ini berlaku untuk semua bidang ilmu termasuk bidang ilmu kriptografi. Bidang ilmu kriptografi mencakup semua aspek keamanan dalam komunikasi dalam berbagai media.

Paper ini akan membahas tentang hakikat dan filsafat ilmu kriptografi yang diuraikan secara singkat tentang materi yang terdapat didalamnya yaitu diantaranya pembahasan tentang sejarah, pengertian, serta pemikiran para filsafat terhadap ilmu kriptografi dan perkebangannya saat ini.

2. METODOLOGI PENELITIAN

Dalam pengumpulan data digunakan metode penelitian dengan studi literatur yaitu kajian pada literatur seperti ebook, jurnal, proceeding dan paper. Berikut metode penelitian yang digunakan pada penelitian ini terdapat pada Gambar 1.



Gambar 1. Metode Penelitian

Studi literatur terkait filsafat ilmu dilakukan dengan kajian literatur mengenai pendapat para filsuf, sejarah, dan perkembangan filsafat ilmu. Studi literatur terkait sejarah ilmu kriptografi diambil dari sejarah terdahulu hingga saat ini dari berbagai literatur. Studi literatur terkait pengertian kriptografi diambil dari berbagai pendapat para ilmuwan. Studi literatur terkait perkembangan ilmu kriptografi saat ini dilihat dari hasil penelitian yang sudah dipublikasi mengenai penerapannya terhadap teknologi informasi.

3. HASIL DAN PEMBAHASAN

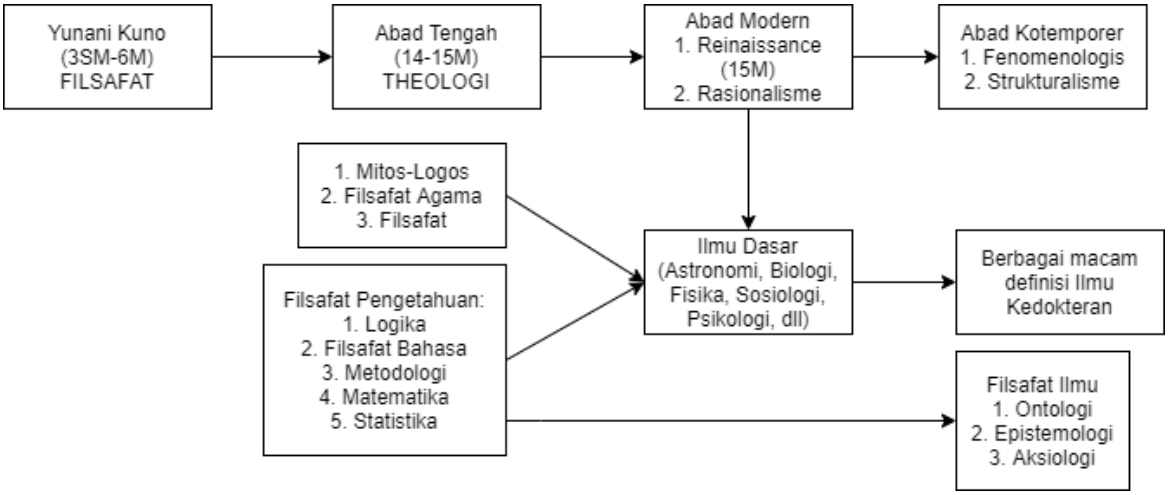
Hakikat dan filsafat ilmu merupakan landasan dari perkembangan suatu ilmu. Perkembangan dari pemikiran para filsuf terdahulu menjadikan ilmu saat ini dapat diterapkan pada berbagai bidang keilmuan. Penerapan keilmuan tersebut dapat dimanfaatkan pada kehidupan manusia yang akan mempemudah semua kegiatan manusia.

3.1. Filsataf Ilmu

Filsafat pada dasarnya terkait dengan kebijaksanaan yang sesuai dengan arti kata yang sebenarnya yaitu philos dan shopos yang berarti cinta akan kebijaksanaan. Filsafat merupakan disiplin yang mengajarkan dan menghantarkan manusia pada tindakan yang manusiawi. Filsafat memiliki cabang keilmuan yang disebut dengan filsafat ilmu. Berikut beberapa pendapat filsafat ilmu menurut para ahli.

1. Menurut Robert Ackerman, Filsafat ilmu adalah suatu pandangan kritis dari gagasan ilmiah saat ini dengan perbandingan terhadap gagasan terdahulu yang telah dibuktikan.
2. Menurut Lewis White Back, Filsafat ilmu adalah gagasan dan evaluasi metode-metode pemikiran ilmiah serta usaha menemukan nilai serta pentingnya upaya ilmiah sebagai suatu keseluruhan.
3. Menurut A. Cornelius Benjamin, Filsafat ilmu merupakan kajian sistematis mengenai ilmu pada metode, konsep dan gagasan serta kerangka umum cabang-cabang pengetahuan intelektual.
4. Menurut V. Berry, Filsafat ilmu merupakan kajian tentang logika dari teori-teori ilmiah serta hubungan antara eksperimen dan teori seperti metode ilmiah.
5. May Brodbeck, Filsafat ilmu merupakan analisis yang independen secata etis dan filosofis serta deskriptif dalam pemaparan keilmuan dengan jelas.

Perkembangan ilmu karena dua hal yaitu metode berfikir dan metode pengamatan. Berikut merupakan gambar pekembangan ilmu berdasarkan filsafat ilmu terdapat pada Gambar 2.



Gambar 2. Perkembangan Ilmu Berdasarkan Filsafat Ilmu

Perkembangan ilmu berdasarkan filsafat ilmu yaitu dimulai dari zaman Yunani kuno tahun 3SM – 6M dimana filsafat dicetuskan. Kemudian pada abad tengah pada tahun 14-15M filsafat terkait dengan teologi. Pada abad modern terciptanya ilmu dasar yang yang berlandaskan filsafat pengetahuan dan dipengaruhi oleh mitos-logos, filsafat agama dan filsafat. Pada abad kotemporer adanya fenomenologis dan strukturisme untuk mengkaji fenomena berdasarkan keilmuan.

3.2. Sejarah Ilmu Kriptografi

Kriptografi menurut catatan sejarah telah eksis sejak masa kejayaan Yunani atau kurang lebih sekita tahun 400 sebelum masehi. Scytale adalah alat yang digunakan untuk membuat pesan tersembunyi di Yunani pada waktu itu. Scytale merupakan batangan silinder dengan kombinasi 18 huruf.

Pada masa romawi di bawah kekuasaan Julius Caesar, penggunaan kriptografi semakin intens karena pertimbangan stabilitas negara. Teknik kriptografi yang digunakan pada masa Romawi tidak serumit pada masa Yunani, namun untuk pemahaman pesan kriptografi pada masa Romawi masih cukup sulit.

3.3. Pengertian Ilmu Kriptografi

Kriptografi merupakan salah satu metode untuk mencegah kebocorat data yang bersifat rahasia [5]. Kriptografi merupakan ilmu matematika yang berhubungan dengan transformasi data untuk membuat artinya tidak dipahami (untuk menyembunyikan maknanya), mencegahnya dari perubahan tanpa izin, atau mencegahnya dari penggunaan yang tidak sah. Kriptografi menggunakan berbagai macam teknik matematika untuk menjaga konten pada pesan terenkripsi [6]. Jika transformasinya dapat dikembalikan, kriptografi juga bisa diartikan sebagai proses mengubah kembali data yang terenkripsi menjadi bentuk yang dapat dipahami. Menezes, Oorschot dan Vanstone (1996) menyatakan bahwa kriptografi adalah suatu studi teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi entitas dan otentikasi keaslian data [7]. Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi:

- *Plaintext* (M) adalah pesan yang hendak dikirimkan (berisi data asli).
- *Ciphertext* (C) adalah pesan terenkrip (tersandi) yang merupakan enkripsi.
- Enkripsi (fungsi E) adalah proses pengubahan *plaintext* menjadi ciphertext
- Dekripsi (fungsi D) adalah kebalikan dari enkripsi yaitu mengubah *ciphertext* menjadi *plaintext* (data awal/asli).
- Kunci adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

Tujuan kriptografi yang juga merupakan aspek keamanan informasi adalah sebagai berikut:

- Kerahasiaan *(confidentiality)* adalah layanan yang digunakan untuk menjaga isi informasi dari semua pihak kecuali yang memiliki otoritas terhadap informasi. Ada beberapa pendekatan untuk menjaga kerahasiaan yaitu pengemanan secara fisik hingga pengamanan secara algoritma matematika yang membuat data tidak dipahami. Istilah lain yang senada dengan *confidentiality* adalah *secrecy* dan *privacy.*
- Integritas data adalah layanan penjagaan pengubahan data dari pihak yang tidak berwenang. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi pesan oleh pihak-pihak yang tidak berhak seperti penyisipan, penghapusan, dan pensubstitusian data lain ke

dalam pesan yang sebenarnya. Di dalam kriptografi, layanann ini direalisasikan dengan menggunakan tanda-tanda digital *(digital signature).* Pesan yang telah ditandatangani myiratkan bahwa pesan yang dikirim adalah asli.

- Otentikasi adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi *(user authentication atau entity authentication)* maupun mengidentifikasi sumber pesan *(data origin authentication).* Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain sehingga dapat dipastikan sumber pesannnya. Pesan yang dikirim melalui saluran komunikasi juga memberikan kepastian integritas data, sebab jika pesan telah dimodifikasi berarti sumber pesan sudah tidak benar. Oleh karena itu, layanan integritas data selalu dikombinasikan dengan layanan otentikasi sumber pesan.
- Nirpenyangkalan *(non-repudiation)* adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal pengiriman atau penerima pesan menyangkal telah menerima pesan.

3.4. Perkembangan Ilmu Kriptografi Saat Ini

Perkembangan ilmu kriptografi saat ini sudah dapat diterapkan pada berbagai media. Ilmu kriptografi dapat dilakukan pada media suara, gambar, teks, dan vidio. Penelitian terkini terkait kriptografi dilakukan oleh Tobias K. et al. mengenai kriptografi pada jaringan saraf tiruan. Penelitian ini menghasilkan sistem yang aman terhadap serangan yang terjadi pada jaringan saraf tiruan [8].

Penelitian terkait kriptografi dan steganografi dilakukan oleh Daewon L. et al. mengenai kriptografi menggunakan jaringan saraf tiruan pada media suara [9]. Penelitian ini menghasilkan model deep learning untuk steganografi pada media audio.

Penelitian lainnya terkait kriptografi dilakukan oleh Rachid A. dan Mohammad T.A mengenai visualisasi pembelajaran algoritma DES [10]. Penelitian ini menghasilkan pembelajaran animasi mengenai algoritma kriptografi.

4. KESIMPULAN DAN SARAN

Filsafat ilmu adalah cabang dari filsafat yang merupakan gagasan untuk mempelajari metode-metode pemikiran ilmiah dengan kajian secara sistematis untuk menemukan pentingnya upaya ilmiah sebagai suatu keseluruhan. Filsafat ilmu kriptografi adalah adalah pemikiran yang sedalam-dalamnya untuk memperoleh kebenaran, makna, tujuan serta nilai-nilai ilmu kriptografi bagu kehidupan manusia. Hakikat ilmu kriptografi merupakan landasan untuk mengembangkan penelitian terkait kriptografi. Perkembangan ilmu kriptografi sudah diterapkan pada berbagai media seperti gambar, teks, vidio, dan audio. Ilmu kriptografi bertujuan untuk menciptakan suatu sistem yang aman dari serangan yang berusaha mengambil data privasi atau rahasia.

DAFTAR PUSTAKA

[1] Suaedi. *Pengantar Filsafat Ilmu*. IPB Press. Bogor, 2016.
[2] Paulus W. *Filsafat Ilmu Pengetahuan*. Pustaka Diamond. Yogyakarta, 2016.
[3] Raja O.T dan Carolus S. *Pengantar Filsafat Untuk Psikologi*. Kanisius.Yogyakarta. 2017.
[4] Husain et al. "Filsafat Ilmu Komputer dan Cloud Computing Secara Etimologis." *Jurnal Mantik Penusa*, Volume 2 (1), Pages 15-21. Retrieved from http://ejurnal.pelitanusantara.ac.id/index.php/mantik/article/view/377. 2018.
[5] Mohammad N. "Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi dan Dekripsi Data Ofice Menggunakan Metode Blowfish dengan Bahasa Pemrograman Java." *Jurnal Ilmiah Teknik Informatika FORMAT,* Volume 6(1), Pages 87-105. Retrieved from https://publikasi.mercubuana.ac.id/index.php/format/article/view/1532. 2017.
[6] M.R. Joshi and R.A. Karkade. "Network Security with Cryptography." *International Journal of Computer Science and Mobile Computing*, Volume 4(1). Pages 201-204. 2015.
[7] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone. Handbook of Applied Cryptography. Bosa Roca: CRC Press. 1996.
[8] Tobias K, Cecilia P, and Rainer B. "On the Difficulty of Hiding Keys in Neural Networks." In *Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security*

(IH&MMSec '20). Association for Computing Machinery, New York, NY, USA, 73–78. DOI:https://doi.org/10.1145/3369412.3395076. 2020.

[9] Daewon L, Tae W. O, and Kibom K. "Deep Audio Steganalysis in Time Domain." In *Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec '20).* Association for Computing Machinery, New York, NY, USA, 11–21. DOI:https://doi.org/10.1145/3369412.3395064. 2020.

[10] Rachid A and Mohammad T. A. "A Dynamic Visualisation of the DES Algorithm and a Multi-faceted Evaluation of Its Educational Value." In *Proceedings of the 2020 ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE '20).* Association for Computing Machinery, New York, NY, USA, 370–376. DOI:https://doi.org/10.1145/3341525.3387386. 2020.