

# Falsifikasi Karl Popper dalam Pembuktian Keamanan *Cipher*

Budi Sulistyono

School of Electrical Engineering and Informatics  
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia  
Tel. +62-22-425-4034  
Email: budi241@yahoo.com

**Abstract**—Tujuan utama dari *cipher* adalah merealisasikan aspek kerahasiaan data. Algoritma *cipher* melakukan pengacakan terhadap data dengan menggunakan kunci enkripsi sedemikian sehingga pihak lain sulit melakukan dekripsi tanpa mengetahui kunci tersebut. *Cipher* semakin aman jika setiap upaya untuk memecahkannya memerlukan sumber daya minimal yang semakin besar.

Dari sisi desain, algoritma *cipher* tertentu pada umumnya tidak dapat dibuktikan aman secara absolut namun hanya dibuktikan aman terhadap beberapa tipe serangan tertentu. Dari sisi kriptanalisis, serangan yang efektif terhadap suatu *cipher* membuktikan ketidakamanannya. Paper ini menunjukkan bahwa klaim keamanan dan pengujian keamanan *cipher* sejalan dengan prinsip falsifikasi yang dirumuskan oleh Karl Popper.

Prinsip ini menyatakan bahwa bahwa kebenaran suatu teori ilmiah mustahil untuk dibuktikan dan di sisi lain kesalahannya justru memiliki peluang untuk dibuktikan. Menurut Popper, ilmu pengetahuan mengalami kemajuan justru ketika teori-teori lama dibuktikan salah (difalsifikasi) dan ketika teori-teori baru dirumuskan untuk menggantikan teori-teori lama.

**Index Terms**—*Cipher*, keamanan, kriptanalisis, falsifikasi.

## I. PENDAHULUAN

Tujuan utama dari desain *cipher*<sup>1</sup> adalah untuk merealisasikan aspek kerahasiaan data. *Cipher* melakukan enkripsi terhadap data sehingga Alice dapat mengirimkan data kepada Bob melalui jalur komunikasi yang bersifat publik dan pihak ketiga, sebut saja Eve, yang memiliki akses terhadap jalur komunikasi yang digunakan Alice dan Bob, tidak dapat membaca data yang dikirimkan tersebut.

Berdasarkan fungsi utamanya, sebuah *cipher* dikatakan aman jika tidak ada upaya yang dapat dilakukan untuk mematahkan aspek kerahasiaan data yang direalisasikan. Para ahli, baik kriptografer<sup>2</sup> maupun kriptanalisis<sup>3</sup>, pada umumnya membagi keamanan *cipher* dalam beberapa kategori berdasarkan asumsi jumlah sumber daya yang dibutuhkan untuk menyerang *cipher* tersebut. Skenario serangan terhadap *cipher* juga dibagi dalam beberapa kelompok berdasarkan jenis data yang dibutuhkannya. Lalu, apa kaitan keamanan *cipher* dengan prinsip falsifikasi Karl Popper?

<sup>1</sup>*Cipher* merupakan salah satu komponen dalam sistem kriptografi yang seringkali disebut sebagai *primitives*. Yang termasuk dalam *primitives* selain *cipher* diantaranya adalah fungsi *hash* dan *signature*. Selain *primitives* sistem kriptografi juga meliputi protokol kriptografi.

<sup>2</sup>Kriptografer adalah orang yang memiliki keahlian untuk mendesain *cipher*

<sup>3</sup>Kriptanalisis adalah orang yang memiliki keahlian untuk menyerang atau menemukan kelemahan *cipher*

Prinsip falsifikasi menyatakan bahwa kebenaran suatu teori ilmiah mustahil untuk dibuktikan. Prinsip ini juga mengatakan bahwa kita hanya dapat membuktikan kesalahan teori tersebut atau merumuskan teori baru yang dapat menggantikan teori yang lama. Paper ini akan menunjukkan bahwa prinsip falsifikasi ini sangat sejalan prinsip umum yang digunakan untuk menguji keamanan *cipher*. Para desainer *cipher* hanya dapat membuktikan keamanan suatu *cipher* dengan batasan kondisi-kondisi tertentu. Di sisi lain para kriptanalisis berupaya mengeksploitasi batasan-batasan tersebut guna menemukan kelemahan *cipher*. Hal ini identik dengan upaya untuk membuktikan ketidakamanan *cipher* [5], [9], [1]. Dalam prinsip falsifikasi adalah yang menjadi obyek bahasan adalah kebenaran teori ilmiah secara umum, sedangkan dalam ranah *cipher* obyek bahasannya adalah keamanan *cipher*.

Bukankah metode falsifikasi sudah umum dalam dunia ilmiah?

Sebagai contoh sekaligus pembandingan, mari kita tinjau kasus dalam lingkup keilmuan teknik kendali, lebih khusus lagi, mengenai teori kestabilan dalam sistem kendali. Di sini, para desainer atau peneliti berupaya membuktikan kestabilan sistem *loop* tertutup dengan *plant* tertentu dan dengan metode kendali tertentu<sup>4</sup>. Pembuktian ini dapat menggunakan teori kestabilan *lyapunov* maupun turunan-turunannya. Dalam kasus ini, pembuktian kestabilan global mungkin dapat dilakukan. Jika kestabilan hanya dinyatakan secara lokal, batas-batas kestabilan pada umumnya dapat dinyatakan dengan jelas. Kemungkinan lainnya, kestabilan hanya berlaku untuk *plant* dengan model matematis tertentu [8].

Dalam kasus sistem kendali, kestabilan sebuah sistem memiliki kemungkinan untuk dibuktikan secara formal. Namun demikian, di kemudian hari mungkin saja ada orang lain yang menggugurkan teori kestabilan itu dengan cara menunjukkan kesalahan dalam pembuktian sebelumnya atau dengan mengajukan sebuah *counter example*. Pembuktian kebenaran teori kestabilan secara formal sangat lazim dilakukan dalam keilmuan teknik kendali. Hal ini agak tidak sejalan dengan prinsip falsifikasi yang menyatakan bahwa kebenaran sebuah teori ilmiah mustahil untuk dibuktikan.

Hal yang berbeda berlaku dalam kasus pembuktian keamanan *cipher*. Di sini, ketidakmungkinan pembuktian kea-

<sup>4</sup>Beberapa metode kendali yang dapat digunakan diantaranya adalah: metode *pole placement*, kendali *robust*, *sliding modes* dan *feedback linearization*

manan justru menjadi prinsip dasar dalam desain cipher dan kriptanalisis. Namun demikian, tidak semua kategori klaim keamanan memiliki karakter seperti itu. Bagian selanjutnya dari paper ini akan menjelaskan prinsip-prinsip umum pembuktian keamanan cipher dan juga keselarasannya dengan prinsip falsifikasi Popper.

## II. KEAMANAN CIPHER

Fungsi utama cipher adalah untuk mengacak data sedemikian sehingga data tersebut tidak dapat dibaca atau dimengerti oleh pihak lain yang tidak berhak. Berikut ini adalah beberapa terminologi penting yang menjelaskan cipher.

- $\mathcal{P}$  melambangkan ruang plaintext. Setiap anggota dari himpunan  $\mathcal{P}$  disebut sebagai plaintext. Sebagai contoh, anggota  $\mathcal{P}$  dapat berupa bilangan biner, teks dalam bahasa Inggris dan sebagainya
- $\mathcal{C}$  melambangkan ruang ciphertext. Setiap anggota dari himpunan  $\mathcal{C}$  disebut sebagai ciphertext.
- $\mathcal{K}$  melambangkan ruang kunci. Setiap anggota dari himpunan  $\mathcal{K}$  disebut sebagai kunci.
- Setiap elemen  $e \in \mathcal{K}$  menentukan secara unik sebuah transformasi *bijection* dari  $\mathcal{P}$  ke  $\mathcal{C}$  yang dilambangkan dengan  $E_e$  (yaitu,  $E_e : \mathcal{P} \rightarrow \mathcal{C}$ ).  $E_e$  disebut sebagai fungsi enkripsi atau transformasi enkripsi.  $E_e$  harus sebuah *bijection* agar transformasi tersebut dapat dibalikkan sehingga setiap ciphertext tertentu dapat dibalikkan ke satu plaintext yang unik.
- Untuk setiap  $d \in \mathcal{K}$ ,  $D_d$  melambangkan *bijection* dari  $\mathcal{C}$  ke  $\mathcal{P}$  (yaitu,  $D_d : \mathcal{C} \rightarrow \mathcal{P}$ ).  $D_d$  disebut sebagai fungsi dekripsi atau transformasi dekripsi.

*Definisi 1 (Cipher):* Cipher terdiri dari himpunan transformasi enkripsi  $\{E_e : e \in \mathcal{K}\}$  dan himpunan transformasi dekripsi  $\{D_d : d \in \mathcal{K}\}$  dengan sifat yaitu untuk setiap kunci enkripsi  $e \in \mathcal{K}$  selalu terdapat kunci dekripsi yang unik  $d \in \mathcal{K}$  sedemikian sehingga  $D_d = E_e^{-1}$ ; yaitu  $D_d(E_e(p)) = p$  untuk semua  $p \in \mathcal{P}$ .

Kapan sebuah cipher dikatakan aman? Apakah cipher yang aman berarti "tidak terpecahkan" (*unbreakable*)? Merujuk pada Shannon [7], terdapat tiga kategori keamanan cipher:

- 1) Keamanan berdasarkan asumsi kondisi tertentu (*conditional security*) yaitu klaim keamanan cipher yang menyertakan kondisi-kondisi yang menjadi batas keberlakuannya. Kondisi-kondisi ini diantaranya mencakup:
  - kompleksitas data, yaitu: berapa jumlah data minimal yang diperlukan untuk mematahkan cipher<sup>5</sup>.
  - kompleksitas komputasi, yaitu: berapa besar beban komputasi atau berapa jumlah operasi yang dibutuhkan untuk mematahkan cipher.
  - kompleksitas waktu, yaitu: berapa lama waktu yang diperlukan untuk mematahkan cipher.

Kompleksitas komputasi hampir selalu terkait dengan kompleksitas waktu.

<sup>5</sup>Kompleksitas data seringkali juga mempertimbangkan aspek skenario untuk mendapatkan data. Beberapa jenis serangan berdasarkan data yang dibutuhkan diantaranya adalah: *ciphertext-only attack*, *known-plaintext attack* dan *chosen-plaintext attack*

- 2) Keamanan tanpa syarat (*Unconditional security*) yaitu klaim keamanan yang menyatakan bahwa cipher tidak dapat dipatahkan dalam kondisi apapun meskipun dengan mengerahkan sumber daya yang tidak terbatas. Kategori ini dapat dipandang sebagai klaim keamanan yang bersifat absolut.
- 3) Keamanan yang dapat dibuktikan (*provable security*) yaitu klaim keamanan dengan cara mereduksinya menjadi permasalahan lain yang secara ilmiah telah dinyatakan sebagai *hard problem*<sup>6</sup>.

Klaim keamanan berdasarkan kondisi tertentu (*conditional security*) biasanya berupa pembuktian ketahanan cipher terhadap beberapa jenis teknik serangan atau kriptanalisis. Sebagai contoh, cipher AES 128 bit dinyatakan aman terhadap *brute force attack*<sup>7</sup> karena serangan ini membutuhkan waktu 1700 trilyun tahun dengan komputer berkemampuan  $10^{15}$  enkripsi per detik. Dalam [2], desainer BC2 membuktikan keamanan ciphernya terhadap beberapa jenis serangan, yaitu: kriptanalisis linear dan diferensial, *square attack*, *higher order differential attack*, *interpolation attack*, *related-key attack* dan *slide attack*.

Klaim keamanan absolut (*unconditional security*) saat ini hanya berlaku untuk cipher ideal yang disebut sebagai *one-time-pad*. Cipher ini termasuk dalam kategori *stream cipher*<sup>8</sup>. Proses enkripsi dilakukan dengan cara membangkitkan deret acak yang memiliki panjang yang sama dengan panjang *plaintext*  $p$  dan mengacak setiap suku dari  $p$  menggunakan suku deret acak secara berurutan. Pembuktian keamanan absolut secara teoritis misalnya dapat kita lihat di [9]. Keamanan absolut dari *one-time-pad* pertama kali didemonstrasikan oleh Gilbert Vernam pada tahun 1917 yang menggunakannya untuk melakukan enkripsi dan dekripsi otomatis dalam sistem telegram. Pembuktian keamanan secara formal baru diajukan tiga puluh tahun kemudian oleh Shannon dengan menggunakan konsep entropi dan keamanan sempurna (*perfect secrecy*).

Klaim keamanan yang dapat dibuktikan (*provable security*) banyak digunakan dalam cipher dengan kunci publik<sup>9</sup>. Dalam kasus RSA, klaim keamanan disandarkan pada problem faktorisasi hasil perkalian dua bilangan prima yang besar. Klaim keamanan jenis ini harus membuktikan bahwa jika suatu cipher berhasil dipecahkan, maka problem lain yang berelasi dengannya juga terpecahkan. Di sini klaim keamanan juga tidak bersifat absolut karena bergantung pada problem lain yang telah dinyatakan sebagai *hard problem*.

## III. KARL POPPER DAN PRINSIP FALSIFIKASI

Prinsip falsifikasi sangat identik dengan Karl Popper. Menurut Bryan Magee dalam [3], Karl Popper merupakan salah satu

<sup>6</sup>*Hard problem* adalah permasalahan yang sulit dipecahkan atau yang memerlukan upaya sangat besar untuk memecahkannya

<sup>7</sup>*Brute force attack* adalah teknik serangan yang dilakukan dengan mencoba semua alternatif kunci yang mungkin

<sup>8</sup>Stream cipher merupakan jenis cipher simetrik yang mengenkripsi data karakter demi karakter. Yang termasuk dalam cipher simetrik selain *stream cipher* adalah *block cipher*. Cipher simetrik merupakan cipher dengan kunci enkripsi yang sama dengan kunci dekripsi.

<sup>9</sup>Cipher kunci publik atau cipher asimetris (*asymmetric cipher*) merupakan cipher dengan kunci enkripsi yang berbeda dengan kunci dekripsi

filosof terkemuka abad ke-20<sup>10</sup>. Popper berpandangan bahwa satu-satunya cara yang praktis untuk memperluas pengetahuan manusia adalah melalui proses kritik atau umpan balik yang tiada akhir.

Sekurang-kurangnya selama dua ratus tahun setelah Newton, ilmuwan Barat memandang bahwa sains baru itu adalah pengetahuan yang pasti, obyektif dan dapat diandalkan. Begitu suatu kenyataan atau hukum ilmiah yang baru ditemukan, hal itu tidak mungkin diubah lagi. Kepastian ini diyakini sebagai ciri khas sains. Pengetahuan ilmiah adalah pengetahuan yang paling dapat diandalkan di antara pengetahuan manusia dan dapat dianggap sebagai kebenaran yang tidak mungkin dikoreksi. Ilmu pengetahuan berkembang melalui cara menambahkan kepastian-kepastian yang baru ditemukan ke dalam khazanah kepastian yang sudah ada dan selalu bertambah.

Di sisi lain, Popper menyadari bahwa upaya pembuktian selama ratusan tahun ternyata tidak kunjung membuktikan kebenaran teori Newton. Popper juga menyatakan bahwa kebenaran suatu teori ilmiah memang selamanya tidak akan dapat dibuktikan. Hukum-hukum ilmiah hanyalah sekedar teori dan dengan demikian merupakan produk akal budi manusia. Bila teori-teori itu berjalan baik dalam penerapannya, maka berarti teori-teori tersebut mendekati kebenaran. Pencarian kepastian, yang menjadi obsesi filsuf-filsuf Barat dari Descartes sampai Russel harus ditinggalkan karena kepastian itu tidak ada. Tidaklah mungkin untuk membuktikan, pada akhirnya atau untuk selamanya, kebenaran teori ilmiah manapun.

Uraian di atas merupakan penjelasan prinsip falsifikasi yang diusung oleh Popper. Berdasarkan prinsip ini, tidak ada teori ilmiah yang dapat dibuktikan kebenarannya. Di sisi lain, teori ilmiah justru dapat dibuktikan kesalahannya atau di-falsifikasi. Masih menurut Popper, kemajuan ilmu pengetahuan hanya bergantung pada proses falsifikasi yang sistematis dan berkelanjutan.[4]. Teori falsifikasi juga menyatakan bahwa kekuatan suatu statement/teori itu bukan ditentukan dari tingkat validitas/kebenaran teori tsb namun ditentukan dari apakah teori tersebut dapat dibuktikan/diuji kesalahannya.

#### IV. FALSIFIKASI DAN KLAIM KEAMANAN

Bagian ini akan menjelaskan prinsip dasar dari klaim serta pembuktian keamanan cipher. Prinsip tersebut menyatakan bahwa suatu cipher hanya dapat dibuktikan aman relatif terhadap sejumlah teknik serangan yang sudah diketahui. Klaim keamanan tidak dapat menjamin bahwa cipher tersebut juga tahan terhadap semua kemungkinan teknik serangan lain. Berdasarkan prinsip ini, keamanan cipher tidak dapat dibuktikan. Di sisi lain, selalu terbuka peluang bagi para ahli untuk menemukan atau membuktikan kelemahan cipher.

Berikut ini kita akan mendefinisikan terlebih dahulu dua hal, yaitu mengenai keamanan dan ukuran keamanan cipher [6].

*Definisi 2 (Keamanan cipher):* Keamanan atau kekuatan cipher adalah: kemampuan cipher tersebut untuk menanggulangi berbagai serangan terhadapnya agar tujuan pengamanan

(misalnya: menjaga kerahasiaan/secretcy/confidentiality) dapat tercapai.

*Definisi 3 (Ukuran keamanan cipher):* Ukuran keamanan atau kekuatan cipher adalah: upaya dan sumber daya minimum yang diperlukan untuk mematahkan keamanan cipher tersebut.

Jadi, jika terdapat dua cipher, sebut saja  $A$  dan  $B$ , bagaimana cara kita menentukan cipher mana yg lebih aman/kuat? Dari definisi 3, kita harus menentukan cipher mana yg membutuhkan upaya atau sumber daya minimum yang paling besar untuk membongkarnya. Contoh: jika kita membutuhkan waktu minimum 5 tahun untuk membongkar cipher  $A$  dan minimal 3 tahun untuk membongkar cipher  $B$  dengan maka cipher  $A$  lebih kuat dari cipher  $B$ .

Jadi, bagaimana cara kita menentukan sumber daya minimum yang dibutuhkan untuk membongkar cipher  $A$ ? Karena kita akan menggunakan sumber daya minimum untuk menyerang cipher sebagai ukuran, maka, sebelumnya kita harus menemukan teknik atau cara serangan yang paling efisien, yaitu yang membutuhkan sumber daya minimum, diantara seluruh serangan yang mungkin dilakukan terhadap  $A$ . Kita sebut saja serangan paling efisien ini sebagai *Ult.Attack.A* (kependekan dari *ultimate attack* terhadap  $A$ ). Selanjutnya, kita tetapkan kebutuhan sumber untuk melakukan *Ult.Attack.A* tersebut sebagai ukuran kekuatan cipher  $A$ . Hal yg sama kita lakukan jg terhadap cipher  $B$  sehingga kita memperoleh sumber daya yang dibutuhkan untuk melakukan *Ult.Attack.B*. Selanjutnya kita dapat membandingkan kekuatan dua cipher tersebut berdasarkan perbandingan kebutuhan sumber daya tadi.

Untuk menemukan *Ult.Attack.A* dan *Ult.Attack.B* kita harus mengetahui semua teknik serangan yang mungkin dilakukan terhadap  $A$  dan  $B$ . Apakah hal ini mungkin? Dengan cara lain, mungkinkah kita membuktikan bahwa suatu teknik serangan terhadap  $A$  atau  $B$  ekuivalen dengan *Ult.Attack.A* atau *Ult.Attack.B*? Secara teoritis, hingga saat ini, jawaban untuk dua pertanyaan tersebut adalah negatif.

Jadi apa yang dapat kita lakukan untuk mengukur serta membandingkan keamanan cipher? Kegiatan atau upaya untuk mematahkan keamanan cipher disebut sebagai kriptanalisis. Sangat banyak teknik kriptanalisis yang telah dikembangkan oleh para ahli kriptanalisis. Kita ambil contoh, bahwa sekelompok ahli kriptanalisis telah menemukan  $n$  buah teknik serangan terhadap cipher  $A$ . Teknik serangan ini kita namakan *Attack.A<sub>1</sub>*, *Attack.A<sub>2</sub>*,..., dan *Attack.A<sub>n</sub>*. Berdasarkan informasi tersebut, kita hanya dapat menentukan serangan paling efisien terhadap  $A$  secara relatif dari  $n$  jenis serangan yang telah diketahui. Serangan ini kita beri nama *Ult<sub>relatif</sub>.Attack.A*. Untuk cipher  $B$ , jika terdapat  $m$  jenis serangan yang telah diketahui kita juga dapat menentukan *Ult<sub>relatif</sub>.Attack.B*.

Pertanyaan yang penting untuk kita ajukan saat ini adalah:

- Apakah tidak ada teknik serangan lain terhadap  $A$  yang lebih efisien dibandingkan  $n$  teknik serangan terhadap  $A$  yang telah diketahui?
- Apakah tidak ada teknik serangan lain terhadap  $B$  yang lebih efisien selain  $m$  teknik serangan terhadap  $B$  yang telah diketahui?

<sup>10</sup>Filosof terkemuka abad ke 20 yang lain menurut Bryan Magee adalah Bertrand Russel, Ludwig Wittgenstein dan Martin Heidegger

Berdasarkan penjelasan sebelumnya, pertanyaan-pertanyaan tersebut belum dapat dijawab. Singkatnya, para ahli hanya dapat mengatakan bahwa mereka telah menemukan  $n$  jenis serangan terhadap  $A$  dan  $m$  jenis serangan terhadap  $B$  dan berdasarkan hal itu mereka dapat menentukan batas bawah kebutuhan sumber daya untuk melakukan serangan terhadap  $A$  dan  $B$ . Jadi, Bukti formal yang diajukan para ahli untuk menyatakan bahwa cipher  $A$  lebih aman daripada cipher  $B$  (atau sebaliknya) hanya berlaku selama syarat tertentu dapat terpenuhi (*conditional*), yaitu belum ditemukannya serangan baru terhadap  $A$  (atau  $B$ ) yang membutuhkan sumber daya yang lebih kecil dibandingkan  $U_{relatif}.Attack.B$  (atau  $U_{relatif}.Attack.A$ ).

## V. DISKUSI

Berdasarkan penjelasan pada bagian sebelumnya kita menemukan keselarasan antara prinsip falsifikasi Karl Popper dengan prinsip pembuktian keamanan cipher. Sebagaimana dalam prinsip falsifikasi, para ahli kriptanalisis tidak dapat mengklaim keamanan absolut suatu cipher. Keamanan hanya dinyatakan secara relatif dan berlaku sepanjang belum ada teknik kriptanalisis baru yang menggugurkan klaim tersebut.

Sepanjang sejarah perkembangan kriptografi, terlihat bahwa kemajuan teknik desain cipher sangat tergantung pada penemuan teknik kriptanalisis baru. Algoritma cipher baru yang aman harus dapat menanggulangi seluruh teknik kriptanalisis hingga yang paling mutakhir. Hal ini tentu sejalan dengan pernyataan Karl Popper bahwa ilmu pengetahuan akan berkembang melalui proses falsifikasi dan perbaikan yang dilakukan secara berkelanjutan.

## VI. KESIMPULAN

Paper ini telah menjelaskan mengenai prinsip-prinsip pembuktian serta jenis-jenis klaim keamanan cipher. Keamanan cipher tidak dapat dinyatakan secara absolut, kecuali untuk kasus *one-time-pad* yang merupakan cipher ideal. Klaim keamanan cipher selalu dibuat berdasarkan asumsi-asumsi tertentu yang hampir semuanya masih terbuka untuk digugurkan. Relatifitas klaim keamanan ini justru merupakan salah satu permasalahan teoritis mendasar yang belum terpecahkan dalam disiplin kriptografi dan kriptanalisis.

Di bagian lain juga ditunjukkan bahwa prinsip-prinsip dalam pembuktian keamanan ini sangat sejalan dengan prinsip falsifikasi yang dikemukakan oleh Popper. Popper menyatakan bahwa kebenaran teori ilmiah mustahil untuk dibuktikan dan di sisi lain kesalahannya justru dapat dibuktikan.

Popper juga menyatakan bahwa kemajuan ilmu pengetahuan akan terjadi melalui proses falsifikasi yang dilakukan secara sistematis dan berkelanjutan. Sejarah perkembangan ilmu kriptografi dan kriptanalisis juga menunjukkan bahwa teknik-teknik baru dalam desain cipher yang lebih aman pada umumnya diajukan setelah muncul teknik serangan baru terhadap teknik desain atau cipher yang lama.

## REFERENCES

- [1] Johan Borst. *Block Ciphers: Design, Analysis and Side-Channel Analysis Kasteelpark Arenberg 1, B-3001 leuven-Haverlee (Belgium)*. PhD thesis, Katholieke Universiteit Leuven-Faculteit Toegepaste Wetenschappen, 2001.
- [2] Yusuf Kurniawan, Adang Suwandi A., M. Sukrisno Mardiyanto, Iping Supriana S., and Sarwono Sutikno. The new block cipher: Bc2. *International Journal of Network Security*, 8(1):16–24, January 2009.
- [3] Bryan Magee. *Confessions of a Philosopher: A Journey Through Western Philosophy*. Phoenix, 1997.
- [4] Bryan Magee. *The Story of Philosophy*. Dorling Kindersley Limited, London, 2001.
- [5] Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 1996.
- [6] Terry Ritter. Ritter's crypto glossary and dictionary of technical cryptography.
- [7] Claude Shannon. Communication theory of secrecy systems. 1949.
- [8] Jean-Jacques Slotine and Weiping Li. *Applied Nonlinear Control*. Prentice Hall, 1990.
- [9] Douglas R. Stinson. *Cryptography: Theory and Practice, Second Edition*. Chapman & Hall/CRC, February 2002.