Penerapan Pembangkit Bilangan Acak dalam Steganografi

Bayu Samudra - 13520128[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13520128@std.stei.itb.ac.id

***Abstrak*—Testing This document is a model and instructions for LaTeX. This and the IEEEtran.cls file define the components of your paper [title, text, heads, etc.]. *CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract.**

***Kata Kunci*—Keamanan, Steganografi, *Linear Congruetial Generator* (LCG)**

I. Pendahuluan

Dunia saat ini telah memasuki era yang penuh dengan data. Data setiap waktunya bertumbuh secara ekponensial. Data merupakan hal yang sangat penting bagi setiap orang. Data yang tersebar pada internet banyak jenisnya. Ada data yang merupakan data yang memang dibagikan untuk publik bahkan ada juga sata rahasia yang bersifat privat. Data yang bersifat privat ini haruslah dijaga kerahasiaannya. Sealh satu cara untuk menjaganya adalah dengan menggunakan kriptografi.

Kriptografi adalah ilmu yang mempelajari mengenai cara-cara untuk menjaga integritas dan keamanan dari suatu data. [1] Dalam menjaga data, kriptografi menggunakan cabang-cabang ilmu matematika terutama dalam teori bilangan. Kriptografi juga merupakan sebuah seni. Hal ini dikarenakan pada awal kemunculannya, setiap orang memiliki caranya tersendiri untuk mengamankan pesannya. Terdapat banyak kriptografi klasik seperti Caesar Cipher, Vigenere Cipher, Affine Cipher, dan lainnya.

Selain menggunakan kriptografi, terdapat sebuah teknik lain untuk mengamankan sebuah data. Teknik ini dikenal steganografi. Steganografi adalah sebuah ilmu yang mempelajari teknik-teknik bagaimana menyembunyikan sebuah data dalam sebuah media sehingga sulit untuk dikenali. [1] Steganografi ini sudah dikenal cukup lama sejak sejak bangsa Yunani. Steganografi yang pernah tercatat pada zaman itu adalah saat penguasa bernama Histaiaeus, seorang penguasa Yunani, mengirimkan pesan tersembunyi kepada Aristagoras untuk melawan Persia. Sang penguasa mengirimkan pesan tersebut dengan membotaki para budah dan rambutnya dibiarkan tumbuh, lalu dikirimkanlah kepada Aristagoras. Hal ini dapat dilihat pada buku yang telah ditulis oleh Herodatus, *Histories of Herodatus*.

Steganografi ini berbeda dengan Kriptografi. Pada kriptografi, data diubah menjadi sesuatu yang dapat tidak memiliki arti. Akan tetapi, data tersebut masih ada keberadaanya. Dalam Steganografi, data disembunyikan dalam sebuah medium sehingga tidak terlihat keberadaannya. Medium ini bisa apapun, baik itu gambar, video, file, atau bahkan teks. Data pada medium ini pada akhirnya harus bisa diekstraksi untuk diambil pesannya.

Steganografi ini memiliki kelebihan, yaitu data yang dikirimkan tidak menarik perhatian orang lain. Steganografi ini pun dapat diintegrasikan dengan Kriptografi untuk meningkatkan keamanan data yang disimpan.

II. Teori Dasar

A. Terminologi Dasar Steganografi

Dalam Steganografi, dikenal beberapa terminologi dasar. Berikut ini adalah beberapa terminologi dasar yang perlu diketahui: [1]

- Pesan tersembunyi adalah pesan yang disisipkan pada sebuah medium baik itu berupa video, image, audio, ataupun teks.
- Cover adalah media yang digunakan untuk menyisipkan pesan.
- *Stego-object* adalah media yang telah tersisipkan pesan tersembunyi di dalamnya.
- Steganalisis adalah cabang ilmu yang membahas mengenai pendeteksian pesan tersembunyi yang ada pada sebuah media. Terdapat beberapa jenis metode dalam steganalisis ini yang akan dijelaskan pada bagian selanjutnya.

B. Representasi Bilangan Bulat

Pada dasarnya, komputer menyimpan dan memproses informasi dalam bentuk sinyal duanilai. Setiap sinyal tersebut merepresentasikan angka dalam bentuk bit. Kumpulan dari berbagai bit dapat memberikan makna dari suatu data yang sedang diproses. Kumpulan dari berbagai bit ini dapat membantuk sebuah bilangan yang disebut dengan bilangan biner.

Dalam dunia keinformatikaan, terdapat dua jenis representasi bilangan bulat yang sering digunakan yaitu sebagai berikut:

- **Bilangan Biner**
  Bilangan biner yaitu bilangan dengan basis dua. Bilangan biner hanya terdapat dua simbol yang tersedia, yaitu 0 dan 1. Konversi bilangan biner ke bilangan desimal didefinisikan pada persamaan 1.

$$d = \sum_{i=0}^{n} b_i \cdot 2^i \tag{1}$$

Nilai b_i melambangkan digit biner ke-i dan d adalah bilangan desimal hasil konversi.

- **Bilangan Hexadesimal**
  Bilangan Hexadesimal adalah bilangan dengan basis 16. Dua digit dari bilangan ini merepresentasikan satu byte (8-bit). Bilangan Hexadesimal ini dapat meringkas penulisan biner dan juga memudahkan alam penganalisisan bilangan biner. Bilangan hexadesimal ini pada dasarnya terdiri dari simbol 0 sampai dengan 9 dilanjutkan dengan simbol A,B,C,D,E, dan F. Berikut ini adalah rumus konversi bilangan heksadesimal ke bilangan desimal.

$$d = \sum_{i=0}^{n} h_i \cdot 16^i \tag{2}$$

Nilai h_i menyatakan digit hexadesimal ke-i. Bila digit Hexadesimal bernilai A maka digantikan dengan nilai 10. Begitu pula dengan nilai B yang digantikan dengan nilai 11. Hal ini berlaku seterusnya hingga F.

C. Signifikansi Bit

Terdapat dua buah definisi yang perlu diperhatikan mengenai signifikansi bit.Misalkan terdapat sebuah bilangan bulat dengan w-digit dan urutan digitnya adalah $[b_{w-1}, b_{w-2}, \cdots, b_2, b_1, b_0]$. Digit b_{w-1} disebut sebagai *most significant bit* atau biasa disingkat sebagai MSB. Bit b_0 disebut sebagai *least significant bit* atau biasa disingkat sebagai LSB.

III. Pembahasan

Before you begin to format your paper, first write and save the content as a separate text file. Complete all content and organizational editing before formatting. Please note sections III-A–III-E below for more information on proofreading, spelling and grammar.

Keep your text and graphic files separate until after the text has been formatted and styled. Do not number text heads—LaTeX will do that for you.

A. Abbreviations and Acronyms

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, ac, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

B. Units

- Use either SI (MKS) or CGS as primary units. (SI units are encouraged.) English units may be used as secondary units (in parentheses). An exception would be the use of English units as identifiers in trade, such as “3.5-inch disk drive”.
- Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.
- Do not mix complete spellings and abbreviations of units: “Wb/m^2” or “webers per square meter”, not “webers/m^2”. Spell out units when they appear in text: “. . . a few henries”, not “. . . a few H”.
- Use a zero before decimal points: “0.25”, not “.25”. Use “cm^3”, not “cc”.)

C. Equations

Number equations consecutively. To make your equations more compact, you may use the solidus (/), the exp function, or appropriate exponents. Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign. Punctuate equations with commas or periods when they are part of a sentence, as in:

$$a + b = \gamma \tag{3}$$

Be sure that the symbols in your equation have been defined before or immediately following the equation. Use “(3)”, not “Eq. (3)” or “equation (3)”, except at the beginning of a sentence: “Equation (3) is . . .”

D. LaTeX-Specific Advice

Please use “soft” (e.g., `\eqref{Eq}`) cross references instead of “hard” references (e.g., `(1)`). That will make it possible to combine sections, add equations, or change the order of figures or citations without having to go through the file line by line.

Please don’t use the `{eqnarray}` equation environment. Use `{align}` or `{IEEEeqnarray}` instead. The `{eqnarray}` environment leaves unsightly spaces around relation symbols.

Please note that the `{subequations}` environment in LaTeX will increment the main equation counter even when there are no equation numbers displayed. If you forget that, you might write an article in which the equation numbers skip from (17) to (20), causing the copy editors to wonder if you’ve discovered a new method of counting.

BibTeX does not work by magic. It doesn’t get the bibliographic data from thin air but from .bib files. If you use BibTeX to produce a bibliography you must send the .bib files.

LaTeX can’t read your mind. If you assign the same label to a subsubsection and a table, you might find that Table I has been cross referenced as Table IV-B3.

LaTeX does not have precognitive abilities. If you put a `\label` command before the command that updates the counter it’s supposed to be using, the label will pick up the last counter to be cross referenced instead. In particular, a `\label` command should not go before the caption of a figure or a table.

Do not use `\nonumber` inside the `{array}` environment. It will not stop equation numbers inside `{array}` (there won't be any anyway) and it might stop a wanted equation number in the surrounding equation.

E. Some Common Mistakes

- The word "data" is plural, not singular.
- The subscript for the permeability of vacuum μ_0, and other common scientific constants, is zero with subscript formatting, not a lowercase letter "o".
- In American English, commas, semicolons, periods, question and exclamation marks are located within quotation marks only when a complete thought or name is cited, such as a title or full quotation. When quotation marks are used, instead of a bold or italic typeface, to highlight a word or phrase, punctuation should appear outside of the quotation marks. A parenthetical phrase or statement at the end of a sentence is punctuated outside of the closing parenthesis (like this). (A parenthetical sentence is punctuated within the parentheses.)
- A graph within a graph is an "inset", not an "insert". The word alternatively is preferred to the word "alternately" (unless you really mean something that alternates).
- Do not use the word "essentially" to mean "approximately" or "effectively".
- In your paper title, if the words "that uses" can accurately replace the word "using", capitalize the "u"; if not, keep using lower-cased.
- Be aware of the different meanings of the homophones "affect" and "effect", "complement" and "compliment", "discreet" and "discrete", "principal" and "principle".
- Do not confuse "imply" and "infer".
- The prefix "non" is not a word; it should be joined to the word it modifies, usually without a hyphen.
- There is no period after the "et" in the Latin abbreviation "et al.".
- The abbreviation "i.e." means "that is", and the abbreviation "e.g." means "for example".

An excellent style manual for science writers is [**?**].

F. Authors and Affiliations

The class file is designed for, but not limited to, six authors. A minimum of one author is required for all conference articles. Author names should be listed starting from left to right and then moving down to the next line. This is the author sequence that will be used in future citations and by indexing services. Names should not be listed in columns nor group by affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization).

G. Identify the Headings

Headings, or heads, are organizational devices that guide the reader through your paper. There are two types: component heads and text heads.

Component heads identify the different components of your paper and are not topically subordinate to each other. Examples include Acknowledgments and References and, for these, the correct style to use is "Heading 5". Use "figure caption" for your Figure captions, and "table head" for your table title. Run-in heads, such as "Abstract", will require you to apply a style (in this case, italic) in addition to the style provided by the drop down menu to differentiate the head from the text.

Text heads organize the topics on a relational, hierarchical basis. For example, the paper title is the primary text head because all subsequent material relates and elaborates on this one topic. If there are two or more sub-topics, the next level head (uppercase Roman numerals) should be used and, conversely, if there are not at least two sub-topics, then no subheads should be introduced.

H. Figures and Tables

a) Positioning Figures and Tables: Place figures and tables at the top and bottom of columns. Avoid placing them in the middle of columns. Large figures and tables may span across both columns. Figure captions should be below the figures; table heads should appear above the tables. Insert figures and tables after they are cited in the text. Use the abbreviation "Fig. 1", even at the beginning of a sentence.

TABLE I
TABLE TYPE STYLES

Table Head	**Table Column Head**		
	Table column subhead	***Subhead***	***Subhead***
copy	More table copy[a]		

[a]Sample of a Table footnote.

Fig. 1. Example of a figure caption.

Figure Labels: Use 8 point Times New Roman for Figure labels. Use words rather than symbols or abbreviations when writing Figure axis labels to avoid confusing the reader. As an example, write the quantity "Magnetization", or "Magnetization, M", not just "M". If including units in the label, present them within parentheses. Do not label axes only with units. In the example, write "Magnetization (A/m)" or "Magnetization {A[m(1)]}", not just "A/m". Do not label axes with a ratio of quantities and units. For example, write "Temperature (K)", not "Temperature/K".

ACKNOWLEDGMENT

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”. Avoid the stilted expression “one of us (R. B. G.) thanks . . .”. Instead, try “R. B. G. thanks. . .”. Put sponsor acknowledgments in the unnumbered footnote on the first page.

REFERENCES

Please number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in [3]—do not use “Ref. [3]” or “reference [3]” except at the beginning of a sentence: “Reference [3] was the first . . .”

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors’ names; do not use “et al.”. Papers that have not been published, even if they have been submitted for publication, should be cited as “unpublished” [**?**]. Papers that have been accepted for publication should be cited as “in press” [**?**]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [**?**].

DAFTAR PUSTAKA

[1] Munir, Rinaldi. 2019. *Kriptografi Edisi Kedua*. Bandung: Penerbit Informatika

[2] Munir, RInaldi. 2020. *Matematika Diskrit Revisi Ketujuh*. Bandung: Penerbit Informatika

[3] HIdayatullah, Priyanto. 2017. *Pengolahan Citra Digital Teori dan Aplikasi Nyata*. Bandung: Penerbit Informatika.

IEEE conference templates contain guidance text for composing and formatting conference papers. Please ensure that all template text is removed from your conference paper prior to submission to the conference. Failure to remove the template text from your paper may result in your paper not being published.