***Implementasi Pembangkitan Bilangan Acak Untuk Menghasilkan Salt Menggunakan Hénon Map***

Fawwaz Anugrah Wiradhika Dharmasatya - 13520086

Program Studi Teknik Informatika

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Jalan Ganesha 10 Bandung

E-mail (gmail): 13520086@std.stei.itb.ac.id

*Abstract*—This electronic document is a “live” template and already defines the components of your paper [title, text, heads, etc.] in its style sheet. *\*CRITICAL: Do Not Use Symbols, Special Characters, or Math in Paper Title or Abstract*. (*Abstract*)

Keywords—component; formatting; style; styling; insert (key words)

# Pendahuluan

Pada penyimpanan data sensitif seperti *password*, umumnya *password* disimpan di basis data dalam bentuk *hash* dari *password* tersebut untuk mencegah penyalahgunaan *password* jika terjadi *data breach*. Namun, fungsi *hash* bersifat deterministik sehingga jika terdapat dua buat masukan yang sama, nilai *hash* dari kedua masukan akan sama. Hal ini memungkinkan penyerang membuat tabel berisi *password* dan nilai *hash* *password* tersebut. Penyerang dapat memanfaatkan tabel tersebut untuk mengakses akun lain yang memiliki nilai *hash* *password* yang sama. Hal ini akan mengancam keamanan pengguna.

Salah satu metode yang umum digunakan untuk mencegah serangan tersebut adalah menambahkan *salt* saat proses *hashing*. *Salt* adalah sebuah *string* yang dibangkitkan secara acak untuk ditambahkan ke *password* pada saat *hashing*. *Salt* bersifat unik untuk setiap *password* sehingga dua buah *password* yang sama akan memiliki nilai *hash* yang berbeda. Hal ini akan menyulitkan penyerang membuat tabel *hash* *password*.

Berdasarkan *guidelines* OWASP[1], *salt* harus *cryptographically strong*. *Cryptographically strong* didefinsiikan sebagai sistem kriptografi yang sangat tahan terhadap kriptoanalisis. Kriptoanalisis adalah upaya untuk men-*decipher* pola rahasia sebuah sistem. Untuk menghasilkan nilai yang *cryptographically strong*, umumnya digunakan *cryptographically secure pseudorandom number generator*(CSPRNG) atau mengumpulkan masukan acak dari sumber yang tidak bisa diamati, seperti API *Random Generator* di sistem operasi.

Dari kedua metode tersebut, membangkitkan nilai menggunakan API *Random Generator* dari sistem operasi, seperti **/dev/random** di Linux, menghasilkan nilai yang benar-benar acak. Hal ini dikarenakan API *Random Generator* mengumpulkan keacakan sistem untuk membangkitkan nilai acak. Namun, hal ini berarti bila keacakan sistem belum cukup untuk membangkitkan nilai, program harus menunggu sampai keacakan sistem sudah cukup untuk mendapatlan nilai acak. Hal ini dapat menyebabkan masalah *availability* jika terdapat banyak *request* dalam waktu singkat yang membutuhkan bilangan acak untuk membangkitkan *salt*. Oleh karena itu, pembangkitan *salt* menggunakan CSPRNG menjadi alternatif yang bagus untuk membangkitkan *salt* dalam jumlah banyak dan waktu yang singkat.

Salah satu metode untuk mengimpementasikan CSPRNG adalah menggunakan fungsi *chaos*. Fungsi *chaos* adalah fungsi yang peka pada nilai awal. Jika nilai awal berubah sedikit, maka nilai fungsi *chaos* yang dihasilkan bisa berbeda jauh. Salah satu contoh fungsi *chaos* adalah *hénon map*.

Pada makalah ini, penulis akan menjelaskan teori dasar *hénon map*, implementasi *hénon map* untuk membangkitkan *salt*, beserta eksperimen dan analisis eksperimen untuk menunjukkan efektifitas *hénon map* dalam membangkitkan *salt.*

# Dasar teori

## Salt

*Salt* adalah *string* unik yang dibangkitkan secara acak untuk ditambahkan ke setiap *password* pada saat *hashing*. Karena nilai *salt* unik untuk setiap *password*, penyerang harus memecahkan *hash* satu per satu menggunakan *salt* masing-masing *hash*. Hal ini membuat memecahkan *hash* dalam jumlah besar menjadi lebih sulit. Selain itu, *salt* juga melindungi *password* dari *rainbow attack*, yang menggunakan daftar *hash* yang sudah dikomputasi oleh penyerang.

## Bilangan Acak

Bilangan acak adalah bilangan yang tidak dapat diprediksi nilai dan kemunculannya. Bilangan acak bisa berupa *integer*, bilangan riil antara 0-1, atau *string* biner. Dalam dunia kriptografi, bilangan acak memegang peranan penting. Beberapa diantaranya adalah:

1. Pembangkitan nilai-nilai parameter kunci dalam algoritma kriptografi kunci publik.
2. Pembangkitan nilai acak k dalam algoritma enkripsi ElGamal.
3. Pembangkitan *initialization vector* (IV) dalam *block cipher.*
4. Pembangkitan *string* di dalam mekanisme *challenge and response* untuk otentikasi.
5. Pembangkitan kunci sesi oleh *client* di dalam SSL.

## Pembangkitan Bilangan Acak

Bilangan acak bisa dibangkitkan dengan dua cara, mengumpulkan masukan acak dari sumber yang tidak bisa diamati, seperti API *Random Generator* di sistem operasi, atau dibangkitkan menggunakan komputasi. Namun, tidak ada prosedur komputasi yang menghasilkan deret bilangan acak yang benar-benar sempurna (*true random*). Bilangan acak yang dihasilkan dengan prosedur komputasi adalah bilangan acak semu (*pseudo-random*), karena pembangkitan bilangannya dapat diulang kembali. Pembangkit deret bilangan acak semacam itu disebut *pseudo-random number generator* *(PRNG*). PRNG bersifat deterministik, artinya bilangan acak bisa diulang kembali pembangkitannya asalkan kunci (umpan) yang digunakan sama.

## CSPRNG

C*ryptographically secure pseudorandom number generator*(CSPRNG) adalah pembangkit bilangan acak yang aman secara kriptografi. Agar aman secara kriptografis, PRNG harus memenuhi beberapa syarat berikut:

1. Secara statistik lolos uji keacakan (*randomness test*).
2. Tahan terhadap serangan (*attack*) yang serius. Serangan ini bertujuan untuk memprediksi bilangan acak yang dihasilkan dari nilai-nilai sebelumnya.

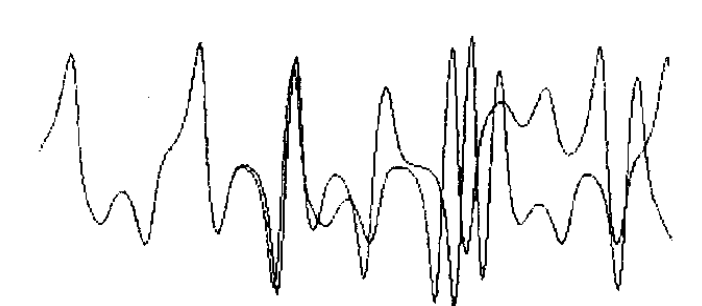
Beberapa persyaratan untuk memastikan bahwa syarat kedua terpenuhi antara lain:

1. Pembangkit bilang acak lulus pengujian *next-bit*. Sebuah pembangkit bit acak dikatakan lulus uji bit berikutnya (next-bit test) jika diberikan barisan k bit, maka tidak dapat diprediksi bit berikutnya 0 atau 1 dengan peluang lebih besar dari ½, sehingga dikatakan *unpredictable*.
2. Pembangkit bilangan acak harus tahan terhadap kompromi perluasan status (*state compromise extensions*). Maksudnya adalah jika penyerangan memperlajari sebagian atau seluruh status sekarang, tidak mungkin bagi penyerang untuk membentuk ulang aliran bilangan acak sebelumnya. Dalam praktiknya, ini berarti CSPRNG harus menggunakan fungsi banyak-ke-satu dalam prosesnya sehingga percobaan untuk membalikkan proses akan menaikkan jumlah kemungkinan aliran secara eksponensial dengan setiap langkah mundur. [5]

## Teori Chaos

Teori *chaos* menggambarkan perilaku sistem dinamis nonlanjar yang menunjukkan fenomena *chaos*. Berdasarkan Wolfram Mathworld [6], suatu sistem disebut menunjukkan fenomena *chaos* apabila memiliki karakterisitik berikut:

1. Memiliki sekumpulan titik yang tebal (*dense collections of points)* dengan orbit periodik.
2. Sensitif terhadap keadaan awal sistem. Jika nilai awal berubah sedikit saja, maka nilai *chaos* yang dihasilkan akan berbeda signifikan. Properti ini kadang-kadang disebut sebagai efek kupu-kupu (*butterfly* effect).
3. Memiliki topologi yang transitif.



**Gambar 1**. Ilustrasi Grafik Nilai Pada Sistem *Chaos*.

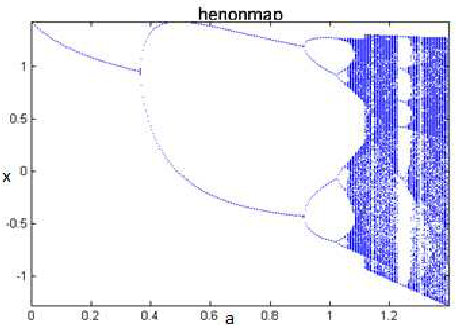
Sumber: <https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2023-2024/32-Pembangkit-bilangan-acak-2024.pdf>

## Henon Map

Henon map adalah pemetaan 2 dimesnsi untuk merepresentasikan perilaku *chaotic*, yang merupakan bentuk sederhana dari sistem Lorentz. Henon Map dapat diformulasikan dalam persamaan (1) dan (2).

Nilai xi dan yimerepresentasikan kordinat awal. Nilai xi+1 dan yi+1 merepresentasikan kordinat setelah transformasi. Nilai a dan b merepresentasikan nilai parameter *hénon map*. Jika persamaan Henon Map direduksi menjadi 1 dimensi, maka persamaan Henon Map akan menjadi seperti persamaan (3).

Persamaan Hanon yang kanon menggunakan nilai a=1,4 dan b=0,3.



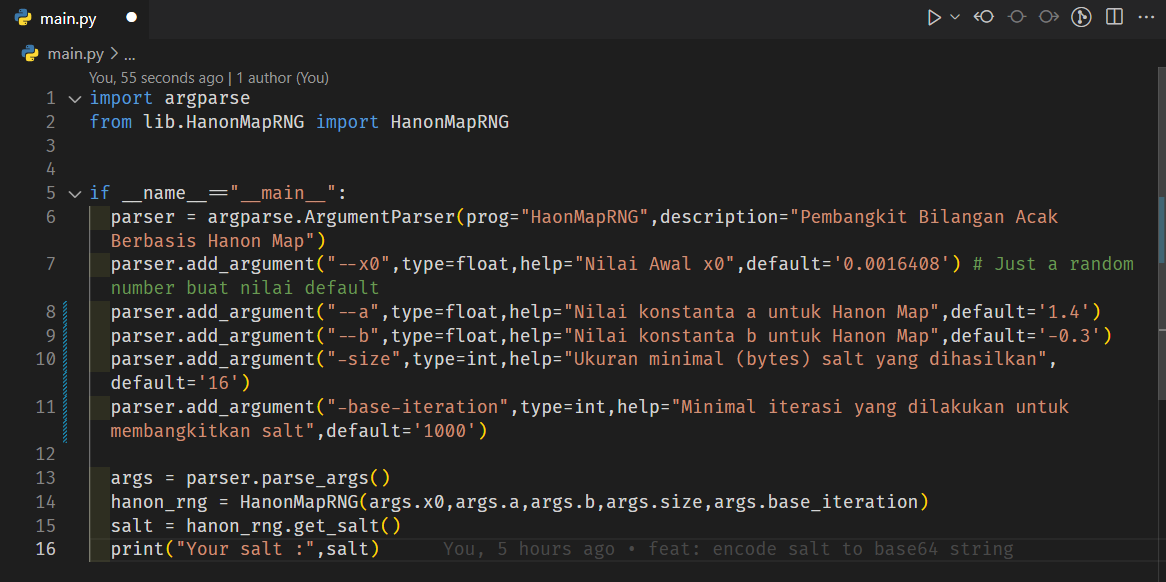
**Gambar 2**. *Bifurcation Diagram* Henon Map.

Sumber: <https://www.researchgate.net/figure/Bifurcation-diagram-for-Henon-map_fig1_224926941>

# Implementasi

Bagian ini menjelaskan tentang langkah-langkah untuk membangkitkan bilangan acak menggunakan *hénon map* serta pemanfaatan bilangan acak tersebut untuk membangkitkan *salt*. Implementasi dari penelitian ini berupa program untuk membangkitkan *salt* menggunakan *hénon map* dalam bahasa Python. Kode sumber program dapat dilihat pada tautan [ini](https://github.com/Wiradhika6051/Tugas-5-Kriptografi).

## Antarmuka Program



**Gambar 3**. Kode Sumber Antarmuka Program

Sumber: Dokumentasi Penulis

Pada tahap pertama, program membaca argumen yang dimasukkan pengguna ketika menjalankan program. Semua argumen bersifat opsional. Jika pengguna tidak memasukkan nilai untuk suatu argumen, program akan menggunakan nilai *default* argumen tersebut. Berikut contoh *command* untuk menjalankan program beserta argumen program.

|  |
| --- |
| $ python main.py --x0 0.00096204 --base-iteration 100 |

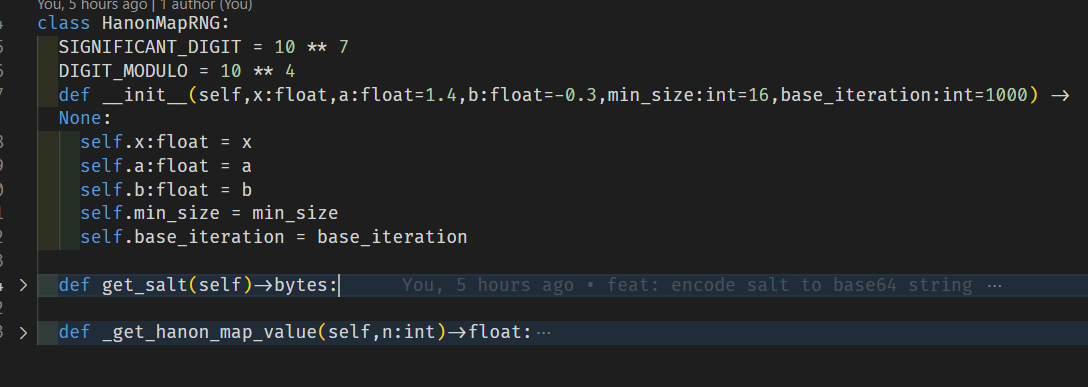
Keterangan mengenai setiap argumen pada program terdapat pada tabel **III.1**.

Tabel **III.1**: Daftar Argumen Program

|  |  |
| --- | --- |
| **Argumen** | **Keterangan** |
| x0 | Nilai awal *hénon map* |
| a | Konstanta a pada *hénon map* |
| b | Konstanta b pada *hénon map* |
| size | Ukuran **minimal** *salt* yang dihasilkan (dalam satuan *byte*) |
| base-iteration | Iterasi minimal untuk pembangkitan *salt* |

Setelah membaca argumen, program membuat objek dari kelas **HanonMapRNG** yang berfungsi untuk membangkitkan *salt*. Penjelasan lebih lengkap tentang isi kelas tersebut akan dibahas pada bagian berikutnya. Terakhir, program menampilkan *salt* yang sudah dibangkitkan.

## Kelas **HanonMapRNG**



**Gambar 4**. Kode Sumber Kelas **HanonMapRNG**

Sumber: Dokumentasi Penulis

Seluruh fungsionalitas untuk membangkitkan salt berada pada kelas **HanonMapRNG**. Kelas ini menerima argumen **x**, **a**, **b**, **min\_size**, dan **base\_iteration** yang masing-masing berkorespondensi dengan argumen masukan pengguna pada saat menjalankan program. Pustaka pembangkitan *salt* diimplementasikan dalam bentuk kelas dikarenakan nilai **x** terakhir *hénon map* pada pembangkitan *salt* sebelumnya akan dijadikan nilai awal *hénon map* untuk pembangkitan *salt* berikutnya.

## Pembangkitan Bilangan Acak

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, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

## Pembangkitan Salt

* 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/m2” or “webers per square meter,” not “webers/m2.” Spell units when they appear in text: “...a few henries,” not “...a few H.”

Identify applicable sponsor/s here. If no sponsors, delete this text box (*sponsors).*

* Use a zero before decimal points: “0.25,” not “.25.” Use “cm3,” not “cc.” (*bullet list*)

# Pengujian dan Analisis

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

## Authors and Affiliations

The template is designed so that author affiliations are not repeated each time for multiple authors of the same affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization). This template was designed for two affiliations.

### For author/s of only one affiliation (Heading 3): To change the default, adjust the template as follows.

#### Selection (Heading 4): Highlight all author and affiliation lines.

#### Change number of columns: Select the Columns icon from the MS Word Standard toolbar and then select “1 Column” from the selection palette.

#### Deletion: Delete the author and affiliation lines for the second affiliation.

### For author/s of more than two affiliations: To change the default, adjust the template as follows.

#### Selection: Highlight all author and affiliation lines.

#### Change number of columns: Select the “Columns” icon from the MS Word Standard toolbar and then select “1 Column” from the selection palette.

#### Highlight author and affiliation lines of affiliation 1 and copy this selection.

#### Formatting: Insert one hard return immediately after the last character of the last affiliation line. Then paste down the copy of affiliation 1. Repeat as necessary for each additional affiliation.

#### Reassign number of columns: Place your cursor to the right of the last character of the last affiliation line of an even numbered affiliation (e.g., if there are five affiliations, place your cursor at end of fourth affiliation). Drag the cursor up to highlight all of the above author and affiliation lines. Go to Column icon and select “2 Columns”. If you have an odd number of affiliations, the final affiliation will be centered on the page; all previous will be in two columns.

## 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. Styles named “Heading 1,” “Heading 2,” “Heading 3,” and “Heading 4” are prescribed.

## Figures and Tables

### 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.

1. Table Styles

| Table Head | Table Column Head | | |
| --- | --- | --- | --- |
| Table column subhead | Subhead | Subhead |
| copy | More table copya |  |  |

1. Sample of a Table footnote. *(Table footnote)*
2. Example of a figure caption. *(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.”

##### Video Link at Youtube *(Heading 5)*

Include link of your video on YouTube in this section.

# Kesimpulan dan saran

##### Ucapan terima kasih

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.

##### Referensi

The template will 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 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” [4]. Papers that have been accepted for publication should be cited as “in press” [5]. 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 [6].

1. OWASP. Methods for Enhancing Password Storage. Diakses pada 05 Juni 2024, dari <https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html#methods-for-enhancing-password-storage>
2. Arias, D. Adding Salt to Hashing: A Better Way to Store Passwords . Diakses pada 05 Juni 2024, dari <https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords>
3. Sargent, W. The Right Way to Use SecureRandom. Diakses pada 05 Juni 2024, dari <https://tersesystems.com/blog/2015/12/17/the-right-way-to-use-securerandom/>
4. Munir, R. (2024). *Pembangkit Bilangan Acak*. Diakses pada 05 Juni 2024
5. B. Williams, R. E. Hiromoto and A. Carlson, "A Design for a Cryptographically Secure Pseudo Random Number Generator," 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Metz, France, 2019, pp. 864-869, doi: 10.1109/IDAACS.2019.8924431.
6. Weisstein, Eric W. "Chaos." From MathWorld--A Wolfram Web Resource. <https://mathworld.wolfram.com/Chaos.html>**.** Diakses pada 09 Juni 2024.
7. Siswanto, A. , Katuk, N. , dan Ku-Mahamud, K. R. “Chaotic-Based Encryption Algorithm using Henon and Logistic Maps for Fingerprint Template Protection“. International Journal of Communication Networks and Information Security (IJCNIS), vol.12, no.1, 2020.
8. Text Steganography Using Lsb Insertion Method Along With Chaos Theory - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Bifurcation-diagram-for-Henon-map\_fig1\_224926941 [accessed 12 Jun, 2024]

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, 12 Juni 2024

Ttd

Nama dan NIM