PAPER NAME

1. 2111 Indra Listiawan dkk-pg 1-10 .pdf

AUTHOR

Indra Listiawan

WORD COUNT

3895 Words

CHARACTER COUNT

22590 Characters

PAGE COUNT

10 Pages

FILE SIZE

1.5MB

SUBMISSION DATE

May 26, 2024 2:16 PM GMT+7

REPORT DATE

May 26, 2024 2:16 PM GMT+7

23% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 18% Internet database
- 18% Publications database
- Crossref database
- Crossref Posted Content database
- 13% Submitted Works database

COMPILER
Vol. 13, No. 1, May 2024, pp. 1~10
ISSN: 2252-2403 (Print), ISSN: 2549-2403 (Online)
Accredited Fourth Grade by Kemenristekdikti, Decree No:200/M/KPT/2020
DOI: 10.28989/compiler.v13i1.2111

Optimising Bcrypt Parameters: Finding the Optimal Number of Rounds for Enhanced Security and Performance

Indra Listiawan[1,*], Zaidir[2], Sugeng Winardi[3], Mohammad Diqi[4]
[1,2,] Department of Information Technology Diploma Program, Universitas Respati Yogyakarta
[3]Department of Information System, Universitas Respati Yogyakarta
[4]Department of Informatic Universitas Respati Yogyakarta

Article Info

Article history:

Received February 6, 2024
Accepted May 8, 2024
Published May 31, 2024

Keywords:

Security
Round
Optimal
BCrypt

ABSTRACT

Recent advancements in the field of information security have underscored the imperative to fine-tune Bcrypt parameters, particularly focusing on the optimal number of rounds as the objective of research. The methode of research is a Brute Force Search method to find the optimal value of bcrypt rounds. The primary focal point of optimization lies in the number of Bcrypt rounds due to its direct impact on security levels. Elevating the number of rounds serves to fortify the security of the Bcrypt algorithm, rendering it more resilient against brute-force attacks. The execution of the Bcrypt rounds in the experimental method mirrors real-world scenarios, specifically in the evaluation of Bcrypt parameters with a focus on entropy assessment of the hash. The selection of the number of rounds should consider the specific needs of the system, where security takes precedence or faster performance is a crucial factor.

Corresponding Author:

Indra Listiawan,
Department of Information Technology Diploma Program,
Universitas Respati Yogyakarta,
Email: *indra@respati.ac.id

1. INTRODUCTION

Recent advancements in information security have underscored the imperative to fine-tune Bcrypt parameters, particularly focusing on the optimal number of rounds. The selection of secure parameter configurations for cryptographic schemes necessitates a meticulous assessment of the attack cost required to compromise the scheme's integrity [1]. Numerous existing solutions geared towards enhancing data security rely on multi-round functions, resulting in prolonged execution times and heightened memory consumption [2]. However, a pioneering algorithm has been introduced, leveraging the reflective property inherent in balanced binary search tree data structure, thereby minimizing operational overhead while concurrently achieving a commendable level of security. Furthermore, a comprehensive evaluation of both the performance and security aspects of this algorithm has been conducted, comparing it with symmetric encryption algorithms like the Advanced Encryption Standard and Data Encryption Standard [3]. These recent breakthroughs underscore the criticality of optimizing parameters, particularly the number of rounds, to fortify data security across diverse applications.

The primary focal point of optimization lies in the number of Bcrypt rounds due to its direct impact on security levels. Elevating the number of rounds serves to fortify the security of the Bcrypt algorithm, rendering it more resilient against brute-force attacks. This is attributed to the fact that each round of Bcrypt involves multiple iterations of a key derivation function, consequently heightening the computational cost for any would-be attacker attempting to decipher the password. The augmentation in the number of rounds not only extends the time required for hash computation but also amplifies the complexity, thereby presenting a formidable challenge for an attacker in their pursuit to crack the password. Consequently, the optimization of the number of Bcrypt rounds emerges as a critical endeavour, essential for striking a delicate equilibrium between security and performance [4].

Elevating the number of Bcrypt rounds serves as a strategic enhancement to security, introducing formidable challenges for potential attackers engaging in brute force endeavours. The Bcrypt algorithm strategically incorporates random salts to thwart the creation of lookup tables, thereby intensifying the complexity of deciphering the original plaintext. However, the efficacy of the Bcrypt algorithm in ensuring security is not uniform across all character types. For instance, alphabetic characters comprising a total of 4 characters can be unravelled to their original plaintext within 4 days, whereas numeric characters, totalling 7 characters, pose a decryption challenge lasting a mere 10 hours. In contrast, a combination of mixed characters with a total of 7 characters proves impervious to decryption attempts within a 5-day timeframe. Consequently, while augmenting the number of Bcrypt rounds undeniably bolsters security, it introduces a nuanced dynamic wherein the overall system performance may be impacted, notably through a substantial increase in the decryption time required [5].

The optimization of Bcrypt parameters, especially the meticulous adjustment of the number of rounds, stands as a pivotal factor in the enhancement of system security. As the number of rounds increases, the computational cost of hashing passwords escalates, introducing formidable barriers for potential attackers attempting brute-force or dictionary attacks on passwords. The exponential growth in time required to compute the hash function with each additional round significantly impedes the attacker's progress. Furthermore, a higher number of rounds extends the temporal window available for the implementation of security patches and updates, consequently mitigating the risk of vulnerabilities being exploited. Thus, the strategic optimization of the number of rounds within Bcrypt parameters emerges as indispensable in fortifying system security and safeguarding user passwords [6].

The meticulous selection of secure parameter sets for cryptographic schemes is contingent upon the precise estimation of attack costs aimed at compromising these schemes [1]. In the ongoing NIST standardization process for post-quantum schemes, there is a heightened emphasis on the necessity for accurate estimation of attack costs, particularly as the selection of final candidates approaches. Recent assessments of code-based schemes have cast doubt on the proclaimed security of many proposals, underscoring the critical importance of precise estimations [7]. Furthermore, the incorporation of recent algorithmic advancements in decoding linear codes, such as information set decoding (ISD) in conjunction with nearest neighbour search, plays a pivotal role in ensuring accurate estimates of attack costs [8]. Practical formulas for attack costs have been formulated and are now accessible online, delivering classical and quantum estimates for the bit security of current code based NIST proposals.[9]

Contemporary data security solutions necessitate the implementation of multi-round functions to thwart differential and linear attacks. Nevertheless, this strategy entails prolonged execution times and increased memory consumption, rendering it less ideal for large datasets or systems sensitive to delays [2].

The recently introduced algorithm seeks to enhance Bcrypt parameters through the strategic utilization of the reflective features inherent in a balanced binary search tree data structure [2]. This algorithm effectively reduces overhead by harnessing the reflective property of a balanced binary search tree, leading to diminished execution times and lower memory consumption [10]. Notably, it incorporates a dynamic offset mechanism to achieve an elevated level of security [11]. In performance comparisons, the proposed algorithm surpasses symmetric encryption counterparts such as the Advanced Encryption Standard and Data Encryption Standard in terms of both running time and memory usage [12].

The recently introduced algorithm detailed in these papers represents a notable advancement in bolstering the security of symmetric encryption algorithms like AES and DES. Notably, the Improved DES algorithm exhibits heightened resilience against differential cryptanalysis compared to its predecessor DES [13]. The Optimized Advanced Encryption Standard (OAES) algorithm further elevates encryption and decryption complexity through the incorporation of random values, a random S-Box, and chaotic maps, fortifying resistance against attempts to decipher the original text [14]. Despite an increase in computational time, the fusion of AES and LUC algorithms within a hybrid scheme proves advantageous for enhancing data security [15]. Summing up the findings, review articles assert that refining the AES algorithm holds considerable promise for data encryption, particularly in response to the evolving landscape of computational power and the advent of quantum computers [16]. Another crypto algorithm introduced in one of the papers specifically aims to enhance cryptographic strength and withstand prevailing cryptanalysis methods [17].

This research adopts an experimental approach to optimize Bcrypt parameters, especially in determining the optimal number of rounds to improve security and system performance. This experimental design is designed to compare different Bcrypt spin configurations and analyze their impact on security and performance, with an emphasis on entropy assessment.

2. RESEARCH METHOD

The method of research is a Brute Force Search method to find the optimal value of bcrypt rounds. In this method, the program iteratively tests each round value in the list num_rounds_list and records the resulting hashing time and entropy for each round. Then, from all the resulting values, the program selects

the round that provides the fastest hashing time (min_time) and a reasonable entropy (above 0.5, under certain assumptions). That is the round that is considered optimal. In the context of searching for the optimal value of a bcrypt round, the entropy that is considered "reasonable" is above 0.5 because this value indicates a high level of randomness. If the entropy is too low, then the resulting hash may be more predictable and vulnerable to brute force attacks or other attacks. By choosing an entropy value above 0.5, we can ensure that the resulting hash has a higher level of security. However, determining this "reasonable" entropy value depends on the needs and security policies of the system in question [18]. The execution of the Bcrypt rounds in the experimental method mirrors real-world scenarios, specifically in the evaluation of Bcrypt parameters with a focus on entropy assessment of the hash. This method employs a combination of classical and contemporary cryptography/cryptanalysis algorithms and techniques to thoroughly examine the security aspects of Bcrypt. It's important to note that, as of now, quantum cryptography is not incorporated into this method [17].

A representative dataset fortifies the credibility of research outcomes by ensuring that the data employed for analysis faithfully mirrors the target population or input space [19]. In the realm of entropy assessment, the utilization of a representative dataset becomes paramount to evaluate the diversity and imbalance within the dataset, particularly when protected attributes lack clear labels [20]. By approximating the disparity of an unlabeled dataset concerning a protected attribute through a controlled set of labeled representative examples, researchers can proficiently scrutinize the dataset's diversity [21]. This method facilitates a cost-effective evaluation of dataset representativeness and empowers downstream applications to derive precise inferences from the data [22]. In this research, the dataset used is a combination of plaintext consisting of uppercase letters, lowercase letters, numbers, and characters. The variable is a change in the dataset, namely the combination that occurs in the plaintext.

The initial steps taken to establish the baseline for Bcrypt parameters are not explicitly outlined in the provided abstracts. Nevertheless, the security assessment does encompass an analysis of system entropy. One paper proposes an entropy weight-TOPSIS algorithm as a comprehensive evaluation method for enhancing security in power information systems [23]. Another paper delves into the application of entropy analysis to identify anomalies within an information system's event log, serving as an indicator of potential unauthorized activities [24]. Additionally, a differential entropy model is employed to scrutinize the functional processes of a clocked network synchronization system, emphasizing information security objectives [25]. While the specific procedures for measuring Bcrypt parameters remain undisclosed, the security evaluation process consistently integrates system entropy analysis across various contexts.

The research method was carried out in stages as follows. Research Design Phase. This study adopts an experimental approach to optimize Bcrypt parameters, especially in determining the optimal number of rounds to enhance system security and performance. This experimental design is crafted to compare various configurations of Bcrypt rounds and analyze their impacts on security and performance, with a focus on entropy assessment. The variables taken for this research are the dependent and independent variables.

a. Independent Variable: Number of Bcrypt rounds.
b. Dependent Variable:
   i. Security: Evaluate encryption strength by measuring system entropy.
   ii. Performance: Execution time

2. Implementation:

Implementation is carried out in a test environment that reflects real scenarios. Use of representative datasets to validate security and measure entropy levels. Experiment Procedure:

i. Initial Measurements:
   Selection of Bcrypt initial parameters as baseline.
   Security measurement with system entropy evaluation and performance analysis.
ii. Rounds Variations:
   Gradually adjusted the number of Bcrypt rounds.
   Involves various levels of rounds and recording of results.
iii. Outcome Measurement:
   1) Security evaluation: Calculate the entropy value and analyze the security distribution.
   2) Performance analysis: Records execution time for each configuration.

3. Analysis of Results:

To carry out analysis of research results, several things are done, namely:

a) Execution Time Comparison:
   The program measures the execution time for each round of Bcrypt. The execution time data is then printed in tabular form.
b) Entropy Calculation:
   For each Bcrypt hash, the program calculates the entropy of that hash. Entropy is a measure of the uncertainty or complexity of data. The higher the entropy, the more complex (random) the data is. Entropy data is printed in tabular form.

c) Optimal Rounds Selection:

The program searches for optimal Bcrypt rounds based on certain criteria. The criteria used here are minimal execution time and entropy that meets a certain threshold (here, the assumption is that entropy is more than 0.5). The optimal rounds along with execution time and entropy information are printed.

d) Performance Visualization:

The program creates a visual graph to show the relationship between the number of Bcrypt rounds and execution time. The graph helps to see the performance trend of Bcrypt with an increasing number of rounds.

3. RESULT DAN ANALYSIS

3.1. Result of research

This research uses 2 parameters, namely plaintext as a password and a round of computing the Bcrypt algorithm. The results are in the form of a table of computational results and a graph of processing time against the number of rounds.

Table 1. Computation Results with plaintext password123

Number of Rounds	Hashed Password	Elapsed Time	Entropy
4	$2b$04$JG9dprrb/bmRBT5V1KA/Q.R8Dtr8EObZVLSQx7rzAceteseqEyXn2	0.00299931	5.18173
5	$2b$05$URBTV1nOn5joYk8oy1HlNudxhJSeubmuRlX7q/alI9XiF4jiuCZtm	0.00614285	5.28173
6	$2b$06$61mD.FzPBUqLsMesi8RVpeKdKhGPLm6B3yXtpq.g1W8HGCK0zB1sK	0.0107515	5.01065
7	$2b$07$URgnow89MSNoSbUWHW9BXeo4XzcbUDSwLXUV1GINBT1e0Fiqu4MEq	0.0199661	5.01065
8	$2b$08$huMrspEx01HFwEaJwFk77elD3BbSKfHR5/vow3jjs616a0Dfq0fli	0.0396628	5.10248
9	$2b$09$gaoxUXdYKVbcLphIJIxbguQtGy11tWT1NHnbycv4Z5aXbve6ddPrq	0.0768716	5.22157
10	$2b$10$MydSX/CZ9zZhC6QsDwtrT.P0Yp8rbYmw7OV/kDW57PsAe5tMNETAa	0.157449	5.26098
11	$2b$11$AlCoTgqMYkxwQo08eMPIlupZcgo4xsleAmWpcqzo06cuXD64cW.pS	0.314404	5.00248
12	$2b$12$IclV5QdC7OSOaLXlANKwo.l7Xqovmgc8poQdj.zrBpvqTtgaoXlu2	0.625339	5.03581
13	$2b$13$UpuOcFD/yWR7NpomSzdgR.TDqEQ3Ih.mDK7NtROhvpDD.gUSZEox.	1.25438	4.97565
14	$2b$14$HFL/CjTNHIEvT4j4Y6aE6uzHJJ5GJZxeFb9eDOd1MXpkvjsUfUjyW	2.25886	5.15656
15	$2b$15$Tz.3mE4tOcUJnFVcqpA3IeyWgC6RqccBDGMitwb/Ch9uwcRmooLOq	4.35059	5.2549

```
The optimal round is 4 with elapsed time 0.0029993057250976562 seconds and entropy 5.181727678869736
```

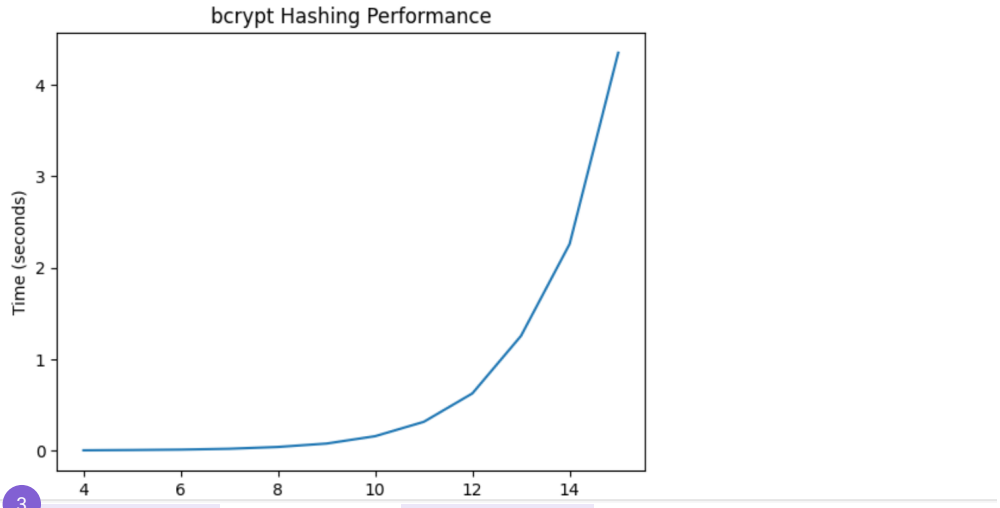

Figure 1. Graph of processing time against number of rounds with plaintext password123

Table 2 Computation Results with plaintext PassworD123

Number of Rounds	Hashed Password	Elapsed Time	Entropy
4	$2b$04$oBN/VGMlnc2p7dOPkTO/IetfQRqKhKRF0SAkgkfq0ScXQkePptAOW	0.00266337	5.06915
5	$2b$05$K6yjKl.jINJVAZZZ6ShcFOPMSvrma5hx6rKQH.HqQWcDwXtVmVIl6	0.00499368	5.05656
6	$2b$06$6WqA7nCgtYaOlSGCjo76ke/AAAImDs5kau0XFuIdPgN9nIom3rPfq	0.0096128	5.13581
7	$2b$07$/Ms3gH5kLCAsIczYQYhd1u0Atzq7Kj7qPIXOqJiT/BCu9d/.Gw4ei	0.0203941	5.25656
8	$2b$08$nk.nWU4ujq/W.qYi79.9Se1jKy5wDyMfEaiYjvybyzisxQ0sY93zm	0.0399351	5.06474
9	$2b$09$07y1AFndbmpg9Bcz3YI/OOw/C88BicOT3804.xcUQZigkKXY0RoVS	0.0784335	5.1899
10	$2b$10$ZBellWRIyXsmHO/Y71.xYO6f4278cR3.dS0ZYZLbf9dXEdzRxgHSm	0.152504	5.04398
11	$2b$11$/eb.psEjDSGqpCq9xQ51YON4Fk7AO2yYq7JJzahp.F1Wnn1ou5HqW	0.284311	5.0549
12	$2b$12$MzIuJMvIqOS5aGyf4/7PPu61PDm0MvkfJELFHM.70PGv3jyytgPUC	0.612239	5.04232
13	$2b$13$ZD2B5uO4R4Oc5ToNtDgRgeRq7AuCbsQWTR5dCrCoyWPWbrxvOYm22	1.26516	4.9314
14	$2b$14$F2JIBS6HQ8YwuN9OoAPR/u6izMhJJNhSAQKkILNPkvTwoHZDpk9o2	2.23119	5.06474
15	$2b$15$LibLjHK14GD9HMHwf8NPsu19ke/7Psho4oh9EYW8KB0kfhcHO3d9W	4.328	5.03581

```
The optimal round is 4 with elapsed time 0.0026633739471435547 seconds and entropy 5.069146220500345
```

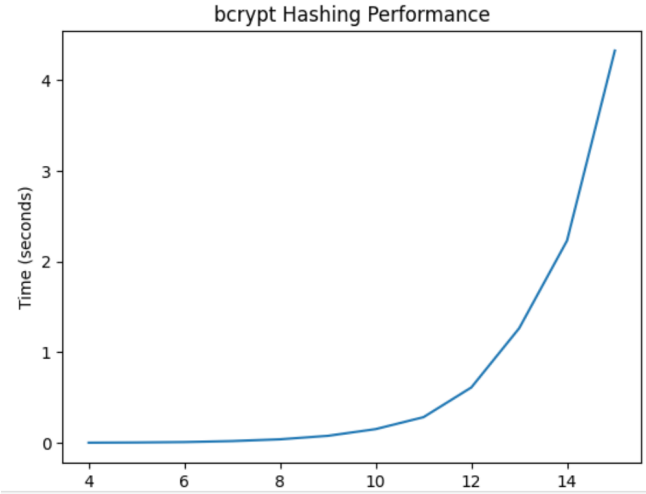

Figure 2. Graph of processing time against number of rounds with plaintext PassworD123

Table 3. Computation Results with plaintext P@sswo&D123

Number of Rounds	Hashed Password	Elapsed Time	Entropy
4	$2b$04$sAH2N7QflSt0e6evT21NKu5Go3JSb.7x0AJi.i0D0QJjKg5Vi0u.O	0.00354028	4.91882
5	$2b$05$Uz26tPAEW5Vjf2CUjyzkwOcBhq4IVAyppNn2WaCDtPlLO20AZpQsG	0.00590444	5.07565
6	$2b$06$vrO2Xm8m4gnnxuFpWRjyWuI1PFdc/RdsM/wB6j3dfk/ht35CjmiHG	0.0120656	5.24398
7	$2b$07$vQ67ARMzt9pEA6JRJD0h..HTF2ohb98v2cBITmOyKMz.q3qUF.XHu	0.0200562	5.08173
8	$2b$08$znTY2FfvTTQkauMK0e8DZ.VqyQimu0AoN5vJpsOTHMQJsad6zDp0y	0.0410914	5.08173
9	$2b$09$8TEZQPk0E.82cu7NwSsVhObzVxgiv1xiNjZKOt8kUReMjd9luRTK2	0.0759592	5.13581
10	$2b$10$gTW0ONTK3LggmoyQoTXoXucNczZtKrInr6jsks1ZuO.spPsO3H8xa	0.153852	5.04398
11	$2b$11$q.7RkUeXtBtzAOlPY10sF.9GJhVQBg7FcfXW2O6vNYQPcvUhv7mHi	0.310132	5.15656
12	$2b$12$OFPRStkVJqeWOm5.aVh6TeStiZup1TWFCKICJuScFR0rHD3VcSvhS	0.637124	5.04232
13	$2b$13$YiWDythrqRVvtCQB/c.qcOpD2l9RA5u8sXsMSKXATKX4cfAFxjT3G	1.2666	5.2899
14	$2b$14$emB3aPyXteXRo5qkWFaCEe2uzFdFdsxF79tGVlaziaW5k1EaLgeCm	2.28971	4.96748
15	$2b$15$FNMBGiSARlhOOu.oR/ZCGezsaaGJO9OVKi.Agx6TY/Vg1ltaEEW5i	4.40134	5.12323

The optimal round is 4 with elapsed time 0.0035402774810791016 seconds and entropy 4.91882038702278

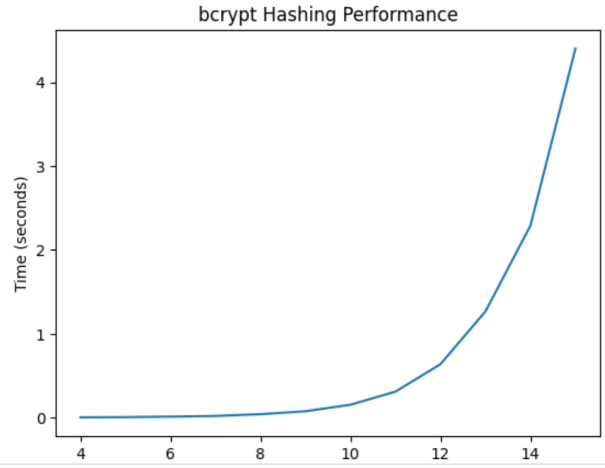

Figure 3. Graph of processing time against number of rounds with plaintext P@sswo&D123

3.2. Analysis

In the experiment above, research was carried out to optimize Bcrypt parameters by varying the number of rounds in the hashing process. Here are some key findings from the analysis of the trial results:

Password: password123

Time Growth and Entropy:

Hashing time tends to increase as the number of rounds increases.

Entropy tends to hover around a high value and is relatively stable throughout the spin variation.

Optimality:

The optimal number of rounds can be determined based on the fastest hashing time and still high enough entropy. In this case, round 4 may be considered optimal because they provide relatively fast hashing times and high levels of entropy.

3.1. Result of research

This research uses 2 parameters, namely plaintext as a password and a round of computing the Bcrypt algorithm. The results are in the form of a table of computational results and a graph of processing time against the number of rounds.

Table 1. Computation Results with plaintext password123

Number of Rounds	Hashed Password	Elapsed Time	Entropy
4	$2b$04$JG9dprrb/bmRBT5V1KA/Q.R8Dtr8EObZVLSQx7rzAceteseqEyXn2	0.00299931	5.18173
5	$2b$05$URBTV1nOn5joYk8oy1HlNudxhJSeubmuRlX7q/alI9XiF4jiuCZtm	0.00614285	5.28173
6	$2b$06$61mD.FzPBUqLsMesi8RVpeKdKhGPLm6B3yXtpq.g1W8HGCK0zB1sK	0.0107515	5.01065
7	$2b$07$URgnow89MSNoSbUWHW9BXeo4XzcbUDSwLXUV1GINBT1e0Fiqu4MEq	0.0199661	5.01065
8	$2b$08$huMrspEx01HFwEaJwFk77elD3BbSKfHR5/vow3jjs616a0Dfq0fli	0.0396628	5.10248
9	$2b$09$gaoxUXdYKVbcLphIJIxbguQtGy1ltWT1NHnbycv4Z5aXbve6ddPrq	0.0768716	5.22157
10	$2b$10$MydSX/CZ9zZhC6QsDwtrT.P0Yp8rbYmw7OV/kDW57PsAe5tMNETAa	0.157449	5.26098
11	$2b$11$AlCoTgqMYkxwQo08eMPIlupZcgo4xsleAmWpcqzo06cuXD64cW.pS	0.314404	5.00248
12	$2b$12$IclV5QdC7OSOaLXlANKwo.l7Xqovmgc8poQdj.zrBpvqTtgaoXlu2	0.625339	5.03581
13	$2b$13$UpuOcFD/yWR7NpomSzdgR.TDqEQ3Ih.mDK7NtROhvpDD.gUSZEox.	1.25438	4.97565
14	$2b$14$HFL/CjTNHIEvT4j4Y6aE6uzHJJ5GJZxeFb9eDOd1MXpkvjsUfUjyW	2.25886	5.15656
15	$2b$15$Tz.3mE4tOcUJnFVcqpA3IeyWgC6RqccBDGMitwb/Ch9uwcRmooLOq	4.35059	5.2549

The optimal round is 4 with elapsed time 0.0029993057250976562 seconds and entropy 5.181727678869736

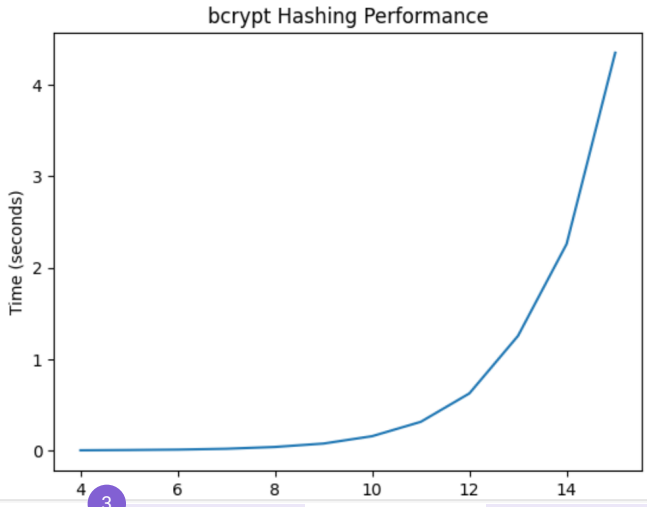

Figure 1. Graph of processing time against number of rounds with plaintext password123

Table 2. Computation Results with plaintext PasworD123

Number of Rounds	Hashed Password	Elapsed Time	Entropy
4	$2b$04$oBN/VGMlnc2p7dOPkTO/IetfQRqKhKRF0SAkgkfq0ScXQkePptAOW	0.00266337	5.06915
5	$2b$05$K6yjKl.jINJVAZZZ6ShcFOPMSvrma5hx6rKQH.HqQWcDwXtVmVIl6	0.00499368	5.05656
6	$2b$06$6WqA7nCgtYaOlSGCjo76ke/AAAImDs5kau0XFuIdPgN9nIom3rPfq	0.0096128	5.13581
7	$2b$07$/Ms3gH5kLCAsIczYQYhd1u0Atzq7Kj7qPIXOqJiT/BCu9d/.Gw4ei	0.0203941	5.25656
8	$2b$08$nk.nWU4ujq/W.qYi79.9Se1jKy5wDyMfEaiYjvybyzisxQ0sY93zm	0.0399351	5.06474
9	$2b$09$07y1AFndbmpg9Bcz3YI/OOw/C88BicOT3804.xcUQZigkKXY0RoVS	0.0784335	5.1899
10	$2b$10$ZBellWRIyXsmHO/Y71.xYO6f4278cR3.dS0ZYZLbf9dXEdzRxgHSm	0.152504	5.04398
11	$2b$11$/eb.psEjDSGqpCq9xQ51YON4Fk7AO2yYq7JJzahp.F1Wnn1ou5HqW	0.284311	5.0549
12	$2b$12$MzIuJMvIqOS5aGyf4/7PPu61PDm0MvkfJELFHM.70PGv3jyytgPUC	0.612239	5.04232
13	$2b$13$ZD2B5uO4R4Oc5ToNtDgRgeRq7AuCbsQWTR5dCrCoyWPWbrxvOYm22	1.26516	4.9314
14	$2b$14$F2JIBS6HQ8YwuN9OoAPR/u6izMhJJNhSAQKkILNPkvTwoHZDpk9o2	2.23119	5.06474
15	$2b$15$LibLjHK14GD9HMHwf8NPsu19ke/7Psho4oh9EYW8KB0kfhcHO3d9W	4.328	5.03581

The optimal round is 4 with elapsed time 0.0026633739471435547 seconds and entropy 5.069146220500345

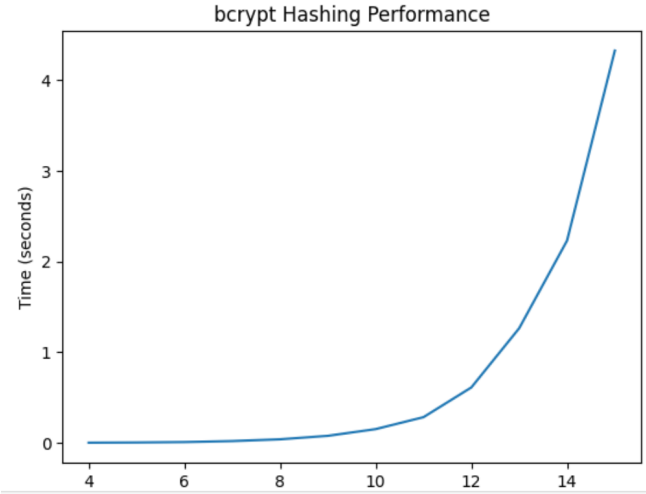

Figure 2. Graph of processing time against number of rounds with plaintext PasswordD123

Table 3. Computation Results with plaintext P@sswo&D123

Number of Rounds	Hashed Password	Elapsed Time	Entropy
4	$2b$04$sAH2N7QflSt0e6evT21NKu5Go3JSb.7x0AJi.i0D0QJjKg5Vi0u.O	0.00354028	4.91882
5	$2b$05$Uz26tPAEW5Vjf2CUjyzkwOcBhq4IVAyppNn2WaCDtPlLO20AZpQsG	0.00590444	5.07565
6	$2b$06$vrO2Xm8m4gnnxuFpWRjyWuI1PFdc/RdsM/wB6j3dfk/ht35CjmiHG	0.0120656	5.24398
7	$2b$07$vQ67ARMzt9pEA6JRJD0h..HTF2ohb98v2cBITmOyKMz.q3qUF.XHu	0.0200562	5.08173
8	$2b$08$znTY2FfvTTQkauMK0e8DZ.VqyQimu0AoN5vJpsOTHMQJsad6zDp0y	0.0410914	5.08173
9	$2b$09$8TEZQPk0E.82cu7NwSsVhObzVxgiv1xiNjZKOt8kUReMjd9luRTK2	0.0759592	5.13581
10	$2b$10$gTW0ONTK3LggmoyQoTXoXucNczZtKrInr6jsks1ZuO.spPsO3H8xa	0.153852	5.04398
11	$2b$11$q.7RkUeXtBtzAOlPY10sF.9GJhVQBg7FcfXW2O6vNYQPcvUhv7mHi	0.310132	5.15656
12	$2b$12$OFPRStkVJqeWOm5.aVh6TeStiZup1TWFCKICJuScFR0rHD3VcSvhS	0.637124	5.04232
13	$2b$13$YiWDythrqRVvtCQB/c.qcOpD2l9RA5u8sXsMSKXATKX4cfAFxjT3G	1.2666	5.2899
14	$2b$14$emB3aPyXteXRo5qkWFaCEe2uzFdFdsxF79tGVlaziaW5k1EaLgeCm	2.28971	4.96748
15	$2b$15$FNMBGiSARlhOOu.oR/ZCGezsaaGJO9OVKi.Agx6TY/Vg1ltaEEW5i	4.40134	5.12323

The optimal round is 4 with elapsed time 0.0035402774810791016 seconds and entropy 4.91882038702278

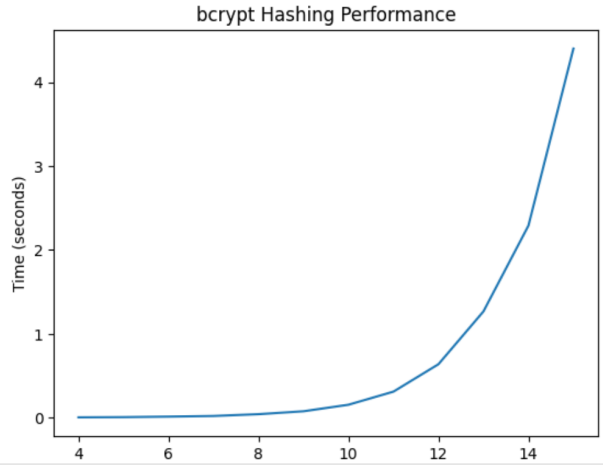

Figure 3. Graph of processing time against number of rounds with plaintext P@sswo&D123

3.2. Analysis

In the experiment above, research was carried out to optimize Bcrypt parameters by varying the number of rounds in the hashing process. Here are some key findings from the analysis of the trial results:

1. Password: password123

   Time Growth and Entropy:
   Hashing time tends to increase as the number of rounds increases.
   Entropy tends to hover around a high value and is relatively stable throughout the spin variation.
   Optimality:
   The optimal number of rounds can be determined based on the fastest hashing time and still high enough entropy. In this case, rounds 4 may be considered optimal because they provide relatively fast hashing times and high levels of entropy.

b. Password: PasswordD123

Time Growth and Entropy:
Just as before, hashing time tends to increase with increasing rounds.
Entropy is generally high, and spin variations do not have a dramatic impact on entropy.
Optimality:
Round 4 may be considered the optimal choice as it provides fast hashing times and a remaining high entropy level.

c. Password: P@sswo&D123

Time Growth and Entropy:
Just as before, hashing time tends to increase with increasing rounds.
Entropy is generally high, and spin variations do not have a dramatic impact on entropy.
Optimality:
Round 4 may be considered the optimal choice as it provides fast hashing times and a remaining high entropy level.

d. Password: PasswordD123

Time Growth and Entropy:
The hashing time again increases as the rounds increase.
Entropy remains high and stable over a certain range of values.
Optimality:
Rounds 4 can be considered optimal choices as they provide a combination of fast hashing times and high levels of entropy.

4. CONCLUSION

Based on the findings obtained from the tests carried out, it can be concluded, among other things:

1. Security and Performance Trade-off: It was found that there was a trade-off between the level of security (entropy) and performance (hahing time). The selection of the number of rounds should take into account the specific needs of the system, where security takes precedence or faster performance is a crucial factor.
2. Entropy Threshold Value: In this analysis, the entropy threshold value that is considered reasonable is 0.5. This value can be adjusted based on the security policy in place.
3. Customization Based on Use Case: The optimal choice of rounds can vary depending on the characteristics of the password used and the priority between security and performance.
4. The results of this analysis provide a basis for selecting optimal Bcrypt parameters in a given scenario.

REFERENCE

[1] A. Esser and E. Bellini, "Syndrome Decoding Estimator," in *Public-Key Cryptography – PKC 2022*, vol. 13177, G. Hanaoka, J. Shikata, and Y. Watanabe, Eds., Cham: Springer International Publishing, 2022, pp. 112–141. doi: 10.1007/978-3-030-97121-2_5.

[2] B. Alabdullah, N. Beloff, and M. White, "E-ART: A New Encryption Algorithm Based on the Reflection of Binary Search Tree," *Cryptography*, vol. 5, no. 1, 2021, doi: 10.3390/cryptography5010004.

[3] M. Curty, K. Azuma, and H.-K. Lo, "A quantum leap in security," *Phys Today*, vol. 74, no. 3, pp. 36–41, Mar. 2021, doi: 10.1063/PT.3.4699.

[4] I. Hwang, S. Kim, and C. Rebman, "Impact of regulatory focus on security technostress and organizational outcomes: the moderating effect of security technostress inhibitors," *Information Technology & People*, vol. 35, no. 7, pp. 2043–2074, Jan. 2022, doi: 10.1108/ITP-05-2019-0239.

[5] T. P. Batubara, S. Efendi, and E. B. Nababan, "Analysis Performance BCRYPT Algorithm to Improve Password Security from Brute Force," *J Phys Conf Ser*, vol. 1811, no. 1, pp. 1 – 7, Mar. 2021, doi: 10.1088/1742-6596/1811/1/012129.

[6] C. Carlet, "Parameterization of Boolean functions by vectorial functions and associated constructions," *Advances in Mathematics of Communications*, pp. 624–650, 2022, doi: 10.3934/amc.2022013.

[7] A. Shafique, J. Ahmed, W. Boulila, H. Ghandorh, J. Ahmad, and M. U. Rehman, "Detecting the Security Level of Various Cryptosystems Using Machine Learning Models," *IEEE Access*, vol. 9, pp. 9383–9393, 2021, doi: 10.1109/ACCESS.2020.3046528.

[8] G. Wu, F. Guo, and W. Susilo, "Generalized public-key cryptography with tight security," *Inf Sci (N Y)*, vol. 504, pp. 561–577, Dec. 2019, doi: 10.1016/j.ins.2019.07.041.

[9] B. R. Curtis and R. Player, "On the Feasibility and Impact of Standardising Sparse-secret LWE Parameter Sets for Homomorphic Encryption," in *Proceedings of the 7th ACM Workshop on*

Encrypted Computing & Applied Homomorphic Cryptography, London United Kingdom: ACM, Nov. 2019, pp. 1–10. doi: 10.1145/3338469.3358940.

[10] A. Ben Ammar and A. A. Minalla, "An Algorithm Based on Self-balancing Binary Search Tree to Generate Balanced, Intra-homogeneous and Inter-homogeneous Learning Groups," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 6, pp. 190–197, 2023, doi: 10.14569/IJACSA.2023.0140622.

[11] Z. Yang, Y. Chang, and Y. Yang, "An Improved Algorithm of Binary Balanced Tree with Super Large-scale Data Set".

[12] S. Ibrahim and A. M. Abbas, "A Novel Optimization Method for Constructing Cryptographically Strong Dynamic S-Boxes," *IEEE Access*, vol. 8, pp. 225004–225017, 2020, doi: 10.1109/ACCESS.2020.3045260.

[13] Ph.D (Pursuing) Department of Computer Science Madurai Kamraj University Madurai (Tamil Nadu) India *et al.*, "Improved Data Encryption Standard Algorithm using Zigzag Scan for Secured Data Transmission," *International Journal of Innovative Technology and Exploring Engineering*, vol. 12, no. 6, pp. 26–37, May 2023, doi: 10.35940/ijitee.F9516.0512623.

[14] T. Alemami, M. A. Mohamed, and S. Atiewi, "Advanced approach for encryption using advanced encryption standard with chaotic map," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 2, p. 1708, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1708-1723.

[15] W. Ady Putra, S. Suyanto, and M. Zarlis, "Performance Analysis Of The Combination Of Advanced Encryption Standard Cryptography Algorithms With Luc For Text Security," *SinkrOn*, vol. 8, no. 2, pp. 890–897, Apr. 2023, doi: 10.33395/sinkron.v8i2.12202.

[16] J. Khudair, K. Abd Ghan, and M. Rizuan Bin Baharon, "Comparative Study in Enhancing AES Algorithm: Data Encryption," *Wasit Journal for Pure sciences*, vol. 2, no. 2, pp. 316–339, Jun. 2023, doi: 10.31185/wjps.100.

[17] D. Shatokhin, "New Encryption Algorithm with Improved Security," *Global Journal of Research in Engineering*, pp. 33–40, Feb. 2023, doi: 10.34257/GJREJVOL23IS1PG33.

[18] I. Nuraeni, Y. H. Agustin, D. Kurniadi, and I. D. Ariyanti, "Implementasi Skema QR-Code dan Digital Signature menggunakan Kombinasi Algoritma RSA dan AES untuk Pengamanan Data Sertifikat Elektronik," pp. 43–52, 2020.

[19] L. H. Clemmensen and R. D. Kjærsgaard, "Data Representativity for Machine Learning and AI Systems." arXiv, Feb. 2023. [Online]. Available: http://arxiv.org/abs/2203.04706

[20] V. Keswani and L. E. Celis, "Auditing for Diversity using Representative Examples." arXiv, Jul. 2021. [Online]. Available: http://arxiv.org/abs/2107.07393

[21] G. Blanc, "Subsampling Suffices for Adaptive Data Analysis." arXiv, Sep. 2023. [Online]. Available: http://arxiv.org/abs/2302.08661

[22] A. Katsenou, F. Zhang, M. Afonso, G. Dimitrov, and D. R. Bull, "BVI-CC: A Dataset for Research on Video Compression and Quality Assessment," *Frontiers in Signal Processing*, vol. 2, p. 874200, Apr. 2022, doi: 10.3389/frsip.2022.874200.

[23] Shen Yang, Yi Lu, Mingshuang Gao, Ce Wang, Junnan Wang, and Yunfeng Guo, "Comprehensive evaluation of power information system security protection based on entropy weight-TOPSIS algorithm," Dec. 2022, p. 1247404. doi: 10.1117/12.2653831.

[24] M. Panchenko, A. Bigdan, T. Babenko, and D. Tymofieiev, "DETECTING THE INFORMATION SECURITY ANOMALIES BASED ON AN ENTROPY ANALYSIS OF THE INFORMATION SYSTEM," *Energy and automation*, vol. 59, no. 1, 2022, doi: 10.31548/energiya2022.01.072.

[25] A. K. Kanaev, E. V Oparin, and E. V Oparina, "Ensuring Information Security for Clocked Network Synchronization System based on the System Entropy Analysis," *Proceedings of Petersburg Transport University*, vol. 19, no. 3, pp. 505–514, 2022.

23% Overall Similarity

Top sources found in the following databases:

- 18% Internet database
- Crossref database
- 13% Submitted Works database
- 18% Publications database
- Crossref Posted Content database

TOP SOURCES

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	ejournals.itda.ac.id Internet	2%
2	eprint.iacr.org Internet	2%
3	University of Birmingham on 2020-01-13 Submitted works	1%
4	shmpublisher.com Internet	1%
5	thesai.org Internet	1%
6	Ahmet Samil Demirkol, Muhammet Emin Sahin, Baris Karakaya, Hasan ... Crossref	<1%
7	Macquarie University on 2024-05-21 Submitted works	<1%
8	sro.sussex.ac.uk Internet	<1%

9	mdpi.com Internet	<1%
10	Andre Esser, Emanuele Bellini. "Chapter 5 Syndrome Decoding Estimat... Crossref	<1%
11	koreascience.kr Internet	<1%
12	zenodo.org Internet	<1%
13	arxiv.org Internet	<1%
14	journal.unnes.ac.id Internet	<1%
15	repository.uksw.edu Internet	<1%
16	ijitee.org Internet	<1%
17	Toras Pangidoan Batubara, Syahril Efendi, Erna Budhiarti Nababan. "An... Crossref	<1%
18	wjps.uowasit.edu.iq Internet	<1%
19	Xiaotong Sun, Ying Qu, Lianru Gao, Xu Sun, Hairong Qi, Bing Zhang, Tin... Crossref	<1%
20	polgan.ac.id Internet	<1%

21	University of Hull on 2022-12-15 Submitted works	<1%
22	dblp.uni-trier.de Internet	<1%
23	Yahia Alemami, Mohamad Afendee Mohamed, Saleh Atiewi. "Advance... Crossref	<1%
24	Takayuki Kushida. "Chapter 15 Distributed Logging Service with Distrib... Crossref	<1%
25	Bayan Alabdullah, Natalia Beloff, Martin White. "E-ART: A New Encrypti... Crossref	<1%
26	Muhammad Remzy Syah Ramazhan, Alhadi Bustamam, Rinaldi Anwar. ... Crossref	<1%
27	Claude Carlet. "A Wide Class of Boolean Functions Generalizing the Hi... Crossref	<1%
28	e3s-conferences.org Internet	<1%
29	joiv.org Internet	<1%
30	Glyndwr University on 2023-12-20 Submitted works	<1%
31	Akshay Aggarwal, Ram Kumar Dhurkari. "Association Between Stress a... Crossref	<1%
32	Middlesex University on 2023-07-02 Submitted works	<1%

33	hitskancheepuram on 2024-04-23 Submitted works	<1%
34	we.umg.edu.pl Internet	<1%
35	arxiv-vanity.com Internet	<1%