Comparison of Cryptographic Algorithms GOST and RSA

R B N Achmad
Department of Master Information System, Universitas Komputer Indonesia, Jalan Dipatiukur No. 112-116, Bandung 40132, Indonesia

Email: rizal.75118005@mahasiswa.unikom.ac.id

Abstract. The GOST and RSA algorithms are one of the cryptographic algorithms. This journal has several objectives to compare the GOST and RSA algorithms, and determine which algorithms are good to be used. The method applied in this journal is the result of internationally indexed journal reviews and this journal helps in determining which algorithm is correct in the second variable. This research explains and concludes journals that have been published internationally. As conclusions that provide choices for readers, by giving the advantages and disadvantages of each algorithm. This research has the effect of making the reader choose which algorithm is suitable as the best recommendation from the available journals.

1. Introduction
The RSA algorithm is an algorithm that has been used since a long time, without realizing how many years ago helps data security on a system. Gost algorithm who currently popular is known as superior security with RSA by analyzing both algorithms. In this research, we discussed the Algorithms GOST and RSA in the confidentiality of the data and to find out the weaknesses and strengths of both algorithms. Things to note are the strengths and weaknesses of the second algorithm is obtained from the papers which have been published internationally.

Security and speed are important factors for comparison algorithms GOST and RSA. In the future some security concepts can be applied in RSA to provide more efficiency and safety [1]. However, RSA can be improved and faster received help with the appropriate approved methods [2] [3]. Unlike the algorithms GOST, GOST inhibits optimization of CPU on a system [4]. It is inhibits the CPU optimization, GOST have advantages of each round [5].

This study analyzed from several papers. Things that were analyzed are the strengths and weaknesses of both these algorithms. The variable in question is the level of security and rate of speed that is used by the reader. With the results obtained, the results of the analysis can be used as a reference for the selection of the algorithm you want to use the reader. But it is not necessary to use both algorithms. But another goal is expected to be a discussion with other readers.

The recommended methods are a number of papers related to this research. As a reference for the research, the methods used to discuss. Of the method of material, you will get the results of the analysis of advantages and disadvantages in both algorithms. Knowledge of strengths and weaknesses will give the values of the positive side of knowledge associated with both of these algorithms. If at any time the algorithm GOST and RSA is required, obtain an explanation of the advantages and disadvantages of both these algorithms.

2. Method
According to the Side-Channel journal R GOST Resistance Analysis of R 34.12-2015, the results of the placement by the two systems on Xilinx Spartan FPGA SLX45 6 shown in Table 1 below, there is an increasing number of FPGA resources are used because that part is responsible for the algorithms GOST R-2015 rising 34.12, the total amount of resources has grown less than doubled.
Table 1. Results of storing Gost and PRNG algorithms

| Schematic type                          | Without protection against attacks on secondary channels | With protection against attacks on secondary channels |
|-----------------------------------------|----------------------------------------------------------|-------------------------------------------------------|
| Resources                               |                                                          |                                                       |
| LUT                                     | 1,603                                                    | 2,878                                                 |
| FF                                      | 664                                                      | 906                                                   |
| Minimum Period. Ns                      | 10.921                                                   | 11.101                                                |

At the same time, the maximum frequency remains practically unchanged, because the reverse system operates parallel to the base [6]. In other journals Quality Manual for Medical Research Companies Actualization According to GOST R ISO 9001-2015. The GOST R ISO 9001-2015 following organisation, need to develop a process to identify potential sources of materials purchased to ensure the effectiveness and efficiency of the procurement process in General. In KPSSZ NII this process is under the control of service contracts, where the staff is guided by documented procedures currently. "to provide resources to the unit's" [7]. In this case, GOST has the potential as an effective and efficient algorithm for a quality research company.

According to the next paper entitled Methods for Implementation of Pseudo-Random Number Generators Based on GOST R 34.12-2015 on Hybrid CPU / GPU / FPGA High-Performance Systems. The findings presented in this article talks about the feasibility of using multidimensional stochastic conversion algorithm in high performance industrial GPGPU systems. Due to the high level of parallelism, algorithms Grasshopper offers high bandwidth capacity in the system multithreaded, highly relevant because of the massive reorientation of the main DPC equipment manufacturer that supports hybrid solutions. For special purpose systems that are used in the EUC (Equipment Under Control), a hardware approach to implement the Grasshopper GOST R 34.12 -2015 still is an efficient solution. [8].

Next is the other GOST algorithm entitled Motivation of Application, Analysis and Inconsistencies Standard GOST R 56002-2014 "Evaluation of Experience and Business Reputation of the Construction Organizations" Pavel. In the process, standard to evaluate other business entities, such as in the fields of production and services for agriculture, education and science, health and medicine. On the basis of GOST R 5602-2014 in addition to the national standards for assessment of architects, designers, engineers, surveyors, goodwill also approved a standard for API technical product manufacturers [9]. In the previous 2 journals both discussed related to production of the GOST system and both showed advantages in the GOST Algorithm.

The last is from the GOST algorithm with the title "Improving on the Integrated Diffie-Hellman-GOST. 94 key agreement protocol" Hoang. This journal provides general information about the DHKE Protocol and DSA. Some work related to develop key exchange protocols with Protocol DHKE is integrated into the DSA, i.e., Arazi, Ham, Phan and Liu Li and. Protocol has its own security weaknesses and needs to be improved. In this paper proposes two key exchange protocol NDH-GOSTI and NDH-new GOST2. This Protocol has all the security attributes of the known key authentication, advanced security, confidentiality is known-key key-share attack, the attack is not known, relay lock, key and the freshness of the disclosure of the status of the session. In addition, the Protocol of NDH-GOST2 have three advantages over other protocols, in particular, can produce more than one session key in a session, using a different hash function (H1, H2 and H3) and GOST standards. R94 that enhance security [10].

Next is an explanation of the RSA algorithm titled Virtual optical encryption using phase shifted digital holography and RSA algorithm. As a core, this journal has shown a novel image encryption
strategy using a phase shifting collimation phenomenon digital holography and RSA algorithm. Journal results are only digital methods, therefore, the requirements for expensive optical components are reduced. The overall technique is simple, fast, accurate, and very safe [11]. This explains that the RSA has no obstacles in the data security process.

In the Journal of Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm. In this paper, the method of combination of RSA and DSA 1024 512 has been done because the computing time is relatively fast. Time is obtained to make the locks is 33.5% slower than when creating separation of RSA and DSA. Computing time has 60% faster in the process of encryption and signing. And for decryption and verification, it has 23% faster than the separation of RSA and DSA. Not only does this combination method can encrypt a message, but also provides digital signatures for authentication that is secure and fast [3]. This paper explains more about security, which is supported by the fastest time when processing data.

In another journal Hybrid Security RSA Algorithm with Application of Web Service. This journal proposes new hybrid security encryption RSA, Hybrid, using more than two big primes in RSA-based cryptographic complexity to increase system cracking. The proposed hybrid security algorithm for RSA called HRSA has proven to be efficient. The key creation time, time of encryption, and decryption time is the main parameter measured for efficiency. It was found that the key creation time over ERSA and RSA public key or because both private key depends on the variable M that does not directly depend on the value of module: trace back the value of M that is hard, that leads to higher security. Thus, he is maintaining the confidentiality of the process of encryption and decryption. Sometimes (great for prime) might take a long time to manufacture keys, encryption and decryption. The model cannot be used in low-power devices. In future work, more theoretical basis will be provided to justify the proposed new encryption with a potentially significant modifications [12]. In this paper, it explains more about the complexity of system cracking with the RSA algorithm.

Other journals with the title Applying d-RSA with Login System to Speed Up Decryption Process in Client Side. The purpose of this paper is to propose a methodology is modified to log in the system. This system was derived from combining two different cryptographic algorithms, d-RSA and One Time Pad (OTP). The main concept is that, d-selected RSA key exchange for the OTP and OTP are used to protect the user’s password with encryption and decryption using the scheme of the OTP. In fact, the login system on previous studies originated from applications with RSA and OTP. However, in this study, the RSA was replaced by d-RSA because d-RSA decryption process can finish faster than RSA. Therefore, this implies that the proposed system can access the application faster than systems that implement RSA OTP and because of the time in the login system can be reduced. The results of the experiment about the access the application using the system log shows that the proposed method can be done faster when compared to systems that implement RSA and OTP. On the other side of the proposed method is slower than the system compared to the registration system. The reason is that it should take time to find the exact value of the new private key, dt, that is not the opposite of public key functions modulo Euler function. Fortunately, this process will only occur when the user first registered as new members [13]. In this case the process from RSA sometimes requires in the process of using RSA and OTP algorithms.

The final title for the explanation of the RSA algorithm is the Design of an Improved RSA Cryptosystem Based on Synchronization of Discrete Chaotic Systems. In this paper, the discrete sliding mode controller is the first proposed to achieve the master system in sync. Then by combining the RSA encryption algorithm synchronization, which is modified is presented. In this design, traditional RSA keys are traditionally are hidden and do not appear on the public channel so that the chances of being attacked can be removed. Therefore, RSA security features not only be maintained, but also can significantly promote the security of RSA Cryptography [14]. This paper explains more about the possibility of attacking the RSA public key.
3. Results and Discussion
   Based on the advantages and disadvantages of the GOST and RSA algorithms can be stated as follows:
   a. Strengths and Weaknesses about GOST
      The advantages of GOST:
      1. A new security algorithm will take a long time to examine the shortcomings of this algorithm.
      2. This algorithm has become a trusted standard for companies in the economic field.
      3. The GOST algorithm can be called an efficient algorithm.
      4. The GOST algorithm is most precisely used by large enterprise system security.
      The disadvantage of the GOST algorithm can be said that GOST is an algorithm that takes too much time because a lot of data will be encrypted with this algorithm. It can not be denied that more and more data require more time for data security.
   b. Strengths and Weaknesses about RSA
      The advantages of the RSA algorithm are as follows:
      1. This algorithm is said to be effective and efficient weighed by the GOST algorithm.
      2. This algorithm can still be developed by many parties in safer data security again.
      3. This algorithm uses a public key that can be adjusted to what it wants and thus can be flexible in the key he receives so the unique algorithm can be said to be very flexible [15] [16] [2].
      A very crucial disadvantage in this algorithm is about using a public key. The cracker will attack the public key even earlier with a cipher text or encryption results. In some journals described, it can be said that this is a crucial weakness in the RSA algorithm.

4. Conclusion
   The conclusion of several reviews of this journal is that all algorithms have advantages and disadvantages. If we want to use good data security, it is better to find out the needs of the system that will be used, it can be said the company or user who wants to use can maintain data security as desired and the other thing is not all data security is safe. Humans will always increase and good security will no longer the same in the future. If associated with these two algorithms, according to the authors, the GOST algorithm is better with the RSA algorithm, not because GOST is standard enterprise security, but because GOST has more than the RSA algorithm. The best point in GOST is having its own uniqueness weighed with the RSA algorithm. The repetitions several times from the results of the first encryption.

References
[1] M. R. Patidar, M. R. Bhartiya, and R. Bhartiya, “Implementation of Modified RSA Cryptosystem Based on Offline Storage and Prime Number,” *Int. J. Comput. Technol.*, 1(Issue 2), pp. 1–6, 2014.
[2] B. R. Ambedkar, A. Gupta, P. Gautam, and S. S. Bedi, “An efficient method to factorize the RSA public key encryption,” *Proc. - 2011 Int. Conf. Commun. Syst. Netw. Technol. CSNT 2011*, pp. 108–111, 2011.
[3] F. J. Aufa and A. S. Requirement, “Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm,” *2018 4th Int. Conf. Sci. Technol.*, 1, pp. 1–5, 2018.
[4] V. Korobitsin and S. Ilyin, “GOST-28147 encryption implementation on graphics processing units,” *ARES 2008 - 3rd Int. Conf. Availability, Secur. Reliab. Proc.*, pp. 967–974, 2008.
[5] X. Zhao et al., “Algebraic fault analysis on GOST for key recovery and reverse engineering,” *Proc. - 2014 Work. Fault Diagnosis Toler. Cryptogr. FDTC 2014*, pp. 29–39, 2014.
[6] M. I. Zvyagina, V. V. Skvortsov, and A. A. Skitev, “Side-channel analysis resistant implementation of GOST R 34.12-2015,” *Proc. 2018 IEEE Conf. Russ. Young Res. Electr. Electron. Eng. EIConRus 2018*, 2018–Janua, pp. 404–406, 2018.
[7] E. A. Batcina, G. V Artamonova, and M. F. Guskova, “Quality Manual for Medical Research Companies Actualization According to GOST R ISO 9001-2015,” 2018 IEEE Int. Conf. "Quality Manag. Transp. Inf. Secur. Inf. Technol.," pp. 583–586, 2018.

[8] A. A. Skitev, M. M. Rovnyagin, E. N. Martynova, M. I. Zvyagina, K. D. Shelopugin, and A. A. Chernova, “Methods for implementation of Pseudo-Random Number Generator based on GOST R 34.12-2015 in hybrid CPU/GPU/FPGA high-performance systems,” Proc. 2017 IEEE Russ. Sect. Young Res. Electr. Electron. Eng. Conf. ElConRus 2017, pp. 555–559, 2017.

[9] P. A. Lontsikh et al., “Motivation of application, analysis and inconsistencies standard GOST R 56002-2014 ‘evaluation of experience and business reputation of the construction organizations,’” 2016 IEEE Conf. Qual. Manag. Transp. Inf. Secur. Inf. Technol. IT MQ IS 2016, pp. 132–137, 2016.

[10] H. Van Viet, N. H. Minh, B. T. Truyen, and N. T. Nga, “Improving on the integrated Diffie-Hellman-GOST.R94 key agreement protocols,” 2013 3rd World Congr. Inf. Commun. Technol. WICT 2013, pp. 106–110, 2014.

[11] A. Chatterjee, J. Dhanotia, V. Bhatia, and S. Prakash, “Virtual optical encryption using phase shifted digital holography and RSA algorithm,” 2018 3rd Int. Conf. Microw. Photonics, ICMAP 2018, vol. 2018–Janua, no. Icmap, pp. 1–2, 2018.

[12] J. Gondaliya, S. Savani, V. S. Dhaduvai, and G. Hossain, “Hybrid security RSA algorithm in application of web service,” Proc. - 2018 1st Int. Conf. Data Intelli. Secur. ICDIS 2018, pp. 149–152, 2018.

[13] K. Somsuk and N. Thammawongsa, “Applying d-RSA with login system to speed up decryption process in client side,” 2017 IEEE 3rd Int. Conf. Eng. Technol. Soc. Sci. ICETSS 2017, 2018–Janua, pp. 1–5, 2018.

[14] F. Mo, Y. C. Hsu, H. H. Chang, S. C. Pan, J. J. Yan, and T. L. Liao, “Design of an improved RSA cryptosystem based on synchronization of discrete chaotic systems,” Proc. - 2016 Int. Conf. Inf. Syst. Artif. Intell. ISAI 2016, 1, pp. 9–13, 2017.

[15] T. C. Segar and R. Vijayaragavan, “Pell’s RSA key generation and its security analysis,” 2013 4th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2013, pp. 4–8, 2013.

[16] R. S. Dhukar, A. K. Gupta, and P. Sharma, “Modified RSA Encryption Algorithm (MREA),” Proc. - 2012 2nd Int. Conf. Adv. Comput. Commun. Technol. ACCT 2012, pp. 426–429, 2011.