**Generate Dynamic Key On Asymmetric Key Cryptography Infrastructure**

N. Yuvaraj, M.E1 , D. Manikandan, M.E,(Ph.D)2 , Dr. V. Parthasarathy3

The report gives an outline of another strategy for creating solid secret word keys, especially for use out in the open key cryptography like the RSA calculation. It talks about the dangers of secret word split the difference through on the web and disconnected assaults, the idea of public key cryptography, and the current RSA calculation. The principal center is around the presentation of dynamic keys for RSA, stressing the utilization of progressively created indivisible numbers to improve security. It likewise frames an indivisible number age calculation for making irregular primes inside a predetermined stretch and examines the advantages of the proposed strategy, featuring improved and decreased time necessities. At long last, it addresses the counteraction of disavowal of administration assaults and proposes another strategy for relieving such dangers.

**Morse Code Security**

Gaurav Gawade , Gulam M.Khan , Indrajeet Gurav , Lonkar Kiran Rajendra , Prof. Mrs. Vanita Gadekar

The report is revolved around a spearheading strategy pointed toward sustaining information security inside distributed computing by incorporating DNA successions with Morse code and crisscross examples for powerful encryption. It gives understanding into the authentic effect of Morse code and highlights the developing meaning of distributed computing, especially in tending to related security challenges. The proposed framework includes encoded record capacity, client access worked with through Morse code keys, and critical key age processes. Underscoring elevated safety efforts, the utilization of the framework stretches out to offering secure transmission and capacity of delicate information, taking special care of basic areas including the military, aeronautics, naval force, and radio correspondences. This imaginative methodology presents a promising road for supporting information security inside current figuring standards.

**Symmetric Key Cryptography using Dynamic Key and Linear Congruential Generator (LCG)**

**Authors:**

[**Zeenat Mahmood**](https://www.researchgate.net/scientific-contributions/Zeenat-Mahmood-2053508833?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19)

[**J. L. Rana**](https://www.researchgate.net/scientific-contributions/J-L-Rana-2037036396)

[**Ashish Khare**](https://www.researchgate.net/profile/Ashish-Khare-9)

The paper presents another symmetric key cryptographic technique using dynamic key age to address the rising interest for vigorous electronic information security. Direct Congruential Generator (LCG) is utilized for key age, comprising a block figure procedure. The strategy's eminent benefit lies in the age of another unique key for every encryption and unscrambling activity, essentially confusing expected breaks. Not at all like customary strategies depending on long haul shared keys helpless against cryptanalysis, this approach renders design recognition for cryptanalysis on the powerful key for all intents and purposes incomprehensible. The idea of dynamic key with symmetric cryptography is likened to a one-time cushion, offering improved security. The proposed cryptography framework in the paper includes four rounds of encryption and unscrambling, with various sections of the powerful key used in each round to brace versatility against cryptanalysis assaults.

**A Hybrid Cryptographic Algorithm Combining Stream and Block Ciphers for Secure Image Encryption**

by M.A. Khan, M. Khurram, and M.A. Malik (2022)

This paper presents a clever half and half methodology for upgrading picture security on the web by joining encryption and steganography. The proposed technique includes encoding the picture with a high level form of the AES calculation, trailed by disguising it inside a cover picture utilizing steganography. The trial results and examination displayed in the paper highlight the adequacy of this half breed approach, showing its capacity to give elevated protection from different assaults.

**Data Encryption Using Morse Code**

* [Aditya Pathak](https://www.researchgate.net/scientific-contributions/Aditya-Pathak-2227553325?_sg%5B0%5D=LLVNf2N1G2EMPT-1d0ufH0y6Ox_2WztqxVilaBlkxcZgd5wY1kOxuT84ycJkEFGkO6g_8_U.ezIv96Ps_rjfZD_hFaLvcfOYLEPVIPp4O4tQPKWevwryChcEDSsBgDf8TD19zTMcHEa4udpmrlgPyyac8CZfcg&_sg%5B1%5D=UvLiDCEI9gQuqmq_GFigDX3GlSYt-UlbB7s9u4qDFnMnLcHIrbDDlNvj0dujEaTfDUSCGj0.QW5f9ILDXsJjZoFVugW9ulBOdHgN7l6r3BqJrvFaaKmm3PuOq_Lx5RWDXR16fkOhZ78r3xkFOShSgYqF8kcWeA&_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InNpZ251cCIsInBhZ2UiOiJwdWJsaWNhdGlvbiIsInBvc2l0aW9uIjoicGFnZUhlYWRlciJ9fQ)
* [Anmol Kaur](https://www.researchgate.net/scientific-contributions/Anmol-Kaur-2242860369?_sg%5B0%5D=LLVNf2N1G2EMPT-1d0ufH0y6Ox_2WztqxVilaBlkxcZgd5wY1kOxuT84ycJkEFGkO6g_8_U.ezIv96Ps_rjfZD_hFaLvcfOYLEPVIPp4O4tQPKWevwryChcEDSsBgDf8TD19zTMcHEa4udpmrlgPyyac8CZfcg&_sg%5B1%5D=UvLiDCEI9gQuqmq_GFigDX3GlSYt-UlbB7s9u4qDFnMnLcHIrbDDlNvj0dujEaTfDUSCGj0.QW5f9ILDXsJjZoFVugW9ulBOdHgN7l6r3BqJrvFaaKmm3PuOq_Lx5RWDXR16fkOhZ78r3xkFOShSgYqF8kcWeA&_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InNpZ251cCIsInBhZ2UiOiJwdWJsaWNhdGlvbiIsInBvc2l0aW9uIjoicGFnZUhlYWRlciJ9fQ)
* [Sagar](https://www.researchgate.net/scientific-contributions/Sagar-2227573777?_sg%5B0%5D=LLVNf2N1G2EMPT-1d0ufH0y6Ox_2WztqxVilaBlkxcZgd5wY1kOxuT84ycJkEFGkO6g_8_U.ezIv96Ps_rjfZD_hFaLvcfOYLEPVIPp4O4tQPKWevwryChcEDSsBgDf8TD19zTMcHEa4udpmrlgPyyac8CZfcg&_sg%5B1%5D=UvLiDCEI9gQuqmq_GFigDX3GlSYt-UlbB7s9u4qDFnMnLcHIrbDDlNvj0dujEaTfDUSCGj0.QW5f9ILDXsJjZoFVugW9ulBOdHgN7l6r3BqJrvFaaKmm3PuOq_Lx5RWDXR16fkOhZ78r3xkFOShSgYqF8kcWeA&_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InNpZ251cCIsInBhZ2UiOiJwdWJsaWNhdGlvbiIsInBvc2l0aW9uIjoicGFnZUhlYWRlciJ9fQ)

The rising dependence on the web has highlighted the basic requirement for guaranteeing the security of information. Cryptography assumes a fundamental part in defending information by encoding it in a way that renders it unintelligible to unapproved clients. Morse code, with its utilization of dabs and runs to address letters and numbers, presents an expected strategy for information encryption. Nonetheless, to support security further, the scrambled information might require re-encryption utilizing extra calculations to alleviate potential unscrambling dangers. Past information security, protecting the respectability of the encryption calculation is fundamental to forestall unapproved unscrambling endeavors. Python's Cryptography module offers an answer as Fernet, which works with the encryption of both the calculation and information records, guaranteeing they stay secure. By utilizing the Python Cryptography module's symmetric encryption strategy, which utilizes a solitary key for both encryption and decoding, this paper means to show the joined utilization of Morse code, time, and Python's Cryptography module to boost information security.

**Dynamic Key Cryptography and Applications**

Huy Hoang Ngo, Xianping Wu, Phu Dung Le, Campbell Wilson, and Balasubramaniam Srinivasan

The paper "Dynamic Key Cryptography and Applications" handles the crucial job of cryptography in protecting information uprightness and privacy inside current security models. It acquaints a powerful key hypothesis with address cryptography's defencelessness to cryptanalysis assaults, underlining the capability of dynamic keys as one-time symmetric cryptographic keys to improve framework security outstandingly. The proposed group of dynamic key age capabilities means to adjust security and execution, especially in remote organization correspondence. The paper basically audits forerunner plans and leads exhaustive examinations to highlight the benefits and capability of dynamic keys to sustain cryptographic frameworks. The top to bottom investigation of dynamic keys offers guarantee in reinforcing information security in different basic areas.