Abstract

In recent years cyber-attacks are continuously developing. This means that hackers can find their way around the traditional cryptosystems. This calls for new and more secure cryptosystems to take their place. This paper outlines a new cryptosystem based on the dragon curve fractal. The security level of this scheme is based on multiple private keys, that are crucial for effective encryption and decryption of data. This paper discusses, how core concepts emerging from fractal geometry can be used as a trapdoor function for this cryptosystem.

References

1. Bhowmik, A., & Menon, U. (2018, May 9). Taming the Dragon. Retrieved from CodeFather - Quora: https://www.quora.com/q/rrqrllbcxwyhoqay/The-Dragon-Curve-Fractal-in-Python

2. Bhowmik, A., & Menon, U. (2020, 4 27). Dragon-Crypto. Retrieved from https://github.com/awnonbhowmik/Dragon-Crypto
3. Bhowmik, A., & Menon, U. (2020, April 30). Rainbow Dragon. Retrieved May 24, 2020, from https://github.com/awnonbhowmik/Dragon-Crypto/blob/master/RainbowDragon.py
4. Bourke, P. (1990, May). Macintosh IFS manual. Retrieved from Paul Bourke: http://paulbourke.net/fractals/ifs/
5. Bourke, P. (1991, July). L-System User Notes. Retrieved from Paul Bourke: http://paulbourke.net/fractals/lsys/
6. Brady, R., Davis, N., & Tracy, A. (2010, July). Encrypting with Elliptic Curve Cryptography. Retrieved from https://www.math.purdue.edu/~egoins/notes/Encrypting_Text_Messages_via_Elliptic_Curve_Cryptography.pdf
7. Geometry. (n.d.). In R. N. Aufmann, J. S. Lockwood, R. D. Nation, & D. K. Clegg, Mathematical Excursions (3rd ed., p. 463). CENGAGE Learning.
8. Silverman, J. H. (2006, June 19). The Discrete Logarithm Problem. An Introduction to the Theory of Elliptic Curves. Laramie, Wyoming, USA. Retrieved from https://www.math.brown.edu/~jhs/Presentations/WyomingEllipticCurve.pdf
9. Union of Equivalence Classes is Whole Set. (n.d.). Retrieved from ProofWiki: https://proofwiki.org/wiki/Union_of_Equivalence_Classes_is_Whole_Set

**Index Terms**

Computer Science  
Security

**Keywords**

Dragon curve, dragon fractal, dragon curve fractal, heighway dragon curve, heighway dragon fractal, cryptography, cryptosystem, crypto system, secure encryption, Iterative Function System, IFS, iteration, iteration, precision, trapdoor function.