5	50

According to the results, 5 rounds are enough to guarantee avalanche effect. Therefore, we chose number of rounds of the algorithm equal to 6.

This work was supported in part by the project UZB-Ind-2021-98 — “Research and development of stream encryption algorithm”. We are grateful to Timur Abdullaev for his help in the development of the new stream algorithm.

References

1. *Aleksander B. Vavrenyuk, Victor V. Makarov, Victor A. Shurygin.* Synchronous Stream Encryption Using an Additional Channel to Set the Key, Procedia Computer Science, Volume 190, 2021, Pages 797-802, ISSN 1877- 0509.

2. *Ronald L. Rivest, Jacob C. N. Schuldt.* Spritz — a spongy RC4-like stream cipher and hash function. IACR Cryptol. ePrint Arch. (2016): 856.

3. *Bo Qu, Dawu Gu, Zheng Guo, Junrong Liu.* Differential power analysis of stream ciphers with LFSRs. Computers & Mathematics with Applications. Volume 65, Issue 9, p. 1291-1299 (2013).

4. *Alisher Ikramov, MirsaidAripov, GayratJuraev.* SPONGE structure in the basis of a new stream cipher. Conference: Modern problems of applied mathematics and information technologies al-Khwarizmi 2021: abstracts of the international scientific conference (15-17 November, Fergana, Uzbekistan). FTY Fergana. 2021. p.188

5. *A. Chakraborti, N. Datta, A. Jha, C. Mancillas-Lypez, M. Nandi, Y. Sasaki.* Elastic-Tweak: A Framework for Short Tweak Tweakable Block Cipher. In: Adhikari, A., Kusters, R., Preneel, B. (eds) Progress in Cryptology INDOCRYPT 2021. INDOCRYPT 2021. Lecture Notes in Computer Science, vol 13143. Springer, Cham. https://doi.org/10.1007/978-3-030-92518-5_6.

6. *D. Chung, S. Lee, D. Choi, J. Lee.* Alternative Tower Field Construction for Quantum Implementation of the AES S-box. Cryptology ePrint Archive, Report 2020/941 (2020).

7. *A. Makalesi, et al.* A New Pseudo Random Number Generator Design with LFSR Based 32-Bit Floating Point with High-Speed FPGA. Int. J. Adv. Eng. Pure Sci. 2020, 32(3): 219-228.

8. *H. Kruppa, SUA Shahy.* Differential and Linear Cryptanalysis in Evaluating AES Candidate Algorithms. Technical report, National Institute of Standards and Technology. 1998.

9. *Juraev G.U., Marakhimov A.R.* Representation of the block data encryption algorithm in an analytical form for differential cryptanalysis. International Journal of Innovative Research in Information Security (IJIRIS). 2019, Issue 03, Volume VI, p.38-42. DOI: 10.26562/IJIRIS.2019. MRIS10081.

10. *Juraev G.U., Ikramov A.A., Marakhimov A.R.* About differential cryptanalysis algorithm of block encryption “Kuznyechik”. International Journal of Advanced Research in Science, Engineering and Technology (IJARSET). Vol. 6, Issue 2, Feb. 2019. P.8164-8169.

11. *Timur Abdullaev, and GayratJuraev.* Development of a method for generating substitution tables for binary and ternary number systems. AIP Conference Proceedings 2365, 040003 (2021); DOI: 10.1063/5.0056841 Published Online: 16 July 2021.

12. *Timur Abdullaev, and GayratJuraev.* Selection of the optimal type of the gamming function for symmetric encryption algorithms. AIP Conference Proceedings 2365, 040004 (2021); DOI: 10.1063/5.0056843 Published Online: 16 July 2021.

MAIN FEATURES OF THE PYTHON PROGRAMMING LANGUAGE

Seitimbetova A.B., Tohmetova K.M.

Karaganda Buketov University, Karaganda, Kazakhstan

Karaganda Technical University named after Abylkas Saginov,Karaganda, Kazakhstan

E-mail:s_b_aigerim@mail.ru, kuralay_tokhmetova@mail.ru

In connection with the currently observed rapid development of personal computing, there is a gradual change in the requirements for programming languages. Interpreted languages are beginning to play an increasingly important role, as the increasing power of personal computers begins to provide sufficient speed for the execution of interpreted programs. And the only significant advantage of compiled programming languages is the high-speed code they create. When the speed of program execution is not critical, the most appropriate choice is an interpreted language, as a simpler and more flexible programming tool.

In this regard, it is of particular interest to consider the relatively new programming language Python, which was created by its author Guido van Rossum in the early 90s. The author of the

programming language, Guido van Rossum, began creating the language in December 1989 at the Center for Mathematics and Computer Science in the Netherlands. Guido van Rossum is the main author of the language, he makes all responsible decisions on the modernization, improvement, and development of the Python language. In February 1991, Guido posted the source code to the alt.sources newsgroup. The name Python itself does not come from a type of snake. Guido van Rossum says he named the Python language after the 1970s English comedy show Monty Python's Flying Circus. Although the name of the language is still more often associated with the snake than with the transfer-file icons in KDE or Microsoft Windows and even the logo on the python.org website (before version 2.5) depict snake heads. For Guido van Rossum and the development team, it was and still is an important goal to make it fun to use.

Python is a stable and widespread language. It is used in many projects and various capacities: as the main programming language or for creating extensions and integrating applications. A large number of projects have been implemented in Python, and it is also actively used to create prototypes for future programs. Python is used by many large companies. Python with the NumPy, SciPy, and MatPlotLib packages is actively used as a universal environment for scientific calculations as a replacement for the common specialized commercial packages Matlab, IDL, and others. Professional 3D graphics programs such as Houdini and Nuke use Python to extend the standard features of the programs. Thus, Python is suitable for solving the lion's share of everyday tasks, whether it's backup, reading emails, or some kind of toy. The Python programming language is practically unlimited and can also be used in large projects. For example, Python is heavily used by IT giants such as Google and Yandex. In addition, the simplicity and versatility of Python make it one of the best programming languages. Python comes standard with the IDLE integrated development environment, in which editing programs will be much more convenient than in a simple text editor or terminal.

IDLE is written in Python using the Tkinter GUI toolkit, so it runs easily on any operating system for which a Python implementation exists. IDLE also has a built-in debugging system that allows you to run your program line by line, making it easier to find errors. But if for some reason IDLE does not suit you, then you can try other development environments and implementations. At the moment there are three known implementations of the Python runtime: CPython Jython, Python.NET. As the names suggest, the first environment is implemented in C, the second in Java, and the last in .NET. The CPython runtime is usually referred to simply as Python, and when people talk about Python, this implementation is often referred to. This implementation consists of an interpreter and extension modules written in C and can be used on any platform where a standard compiler is available. There are also pre-compiled versions for various operating systems, including various versions of OSWindows and various Linux distributions. The Jython runtime is a Python implementation for running the Java Virtual Machine (JVM). Any JVM version is supported, starting from version 1.2.2. To work with Jython, an installed Java machine (Java runtime) is required. It is not necessary to be able to write Java source code, but you will have to deal with JAR files and Java applets, as well as documentation in the JavaDOC.Python.NET format - this implementation does not compile Python code into MSL, but only provides an interpreter written in FROM#. Allows you to use .NET assemblies from Python code. The language is close to MATLAB and therefore good for programming mathematical calculations. In addition, Python can work with languages like C, C++, and Fortran, which are already widely used in scientific computing. In the IDLE integrated environment, it can be used as a calculator. Since Python is a general-purpose language, it can be used in any area of software development (client-server, Web applications).

Main features of Python:

In terms of functionality, Python can be called a hybrid. Its tools range between traditional scripting languages (such as Tcl, Scheme, and Perl) and software systems development languages (such as C, C++, and Java). Python provides the simplicity and ease of a scripting language, and the power usually found in compiled languages. Beyond the capabilities of other scripting languages,

this combination makes Python a convenient tool for developing large-scale projects. The following is a list of the main features that Python has in its arsenal:

Dynamic typing

Python itself keeps track of the types of objects used in the program, so you do not need to write long and complex declarations in the program code. Python has no concept of a type at all and no need to declare variables. Because Python code is not constrained by data types, it can automatically handle a range of objects.

Automatic memory management

Python automatically allocates memory for objects and frees it ("garbage collection") when the objects are no longer needed. Most objects can increase or decrease their memory footprint as needed.

Modular programming

To create large systems, Python provides features such as modules, classes, and exceptions. They allow you to decompose the system into components, use OOP to create reusable code, and gracefully handle events and errors that occur.

Built-in object types

Python exposes the most common data structures, such as lists, dictionaries, and strings, as features native to the programming language itself. These types are highly flexible and comfortable. For example, built-in objects can expand and contract as needed and can be combined with each other to represent data with a complex structure.

Built-in tools

To work with all these types of objects, Python has powerful and standard tools, including operations such as concatenation (joining collections), slicing (taking part in a collection), sorting, mapping, and more.

Utility Libraries

For more specific tasks, Python also includes a large collection of library tools that support just about everything you might need, from regular expression searching to networking. The Python library tools are where most of the work is done.

Third-Party Utilities

Python is an open-source software product and therefore developers can create their own precompiled tools to support tasks that cannot be solved internally.

References

1. Tutorial Python. D. Musin. 07.09.2015 version 02 - 136 p.
2. Workshop on algorithmization and programming in Python Khakhaev I.A. Moscow ed. Alt Linux 2011.
3. S. Shaposhnikova. Fundamentals of programming in Python. Textbook. Introductory course. - version 2. - 2011. - 44 p.
4. http://knowledge.allbest.ru/programming/2c0b65635b2bc79a5d53a89521316c27_0.html
5. http://www.ibm.com/developerworks/en/library/l-python_part_1/index.html

БІЛІМ БЕРУДЕГІ КОМПЬЮТЕРЛІК ТЕХНОЛОГИЯЛАР

Альжапарова А.Т., Турежанова М.Ж.
Академик Е. А. Бөкетов атындағы Қарағанды университеті, Қарағанды, Қазақстан
E-mail: asemgul.alzhaparova@bk.ru

Қоғамның қазіргі даму кезеңі оған компьютерлік технологиялардың күшті әсерімен сипатталады, олар адам қызметінің барлық салаларына еніп, қоғамда ақпараттық ағындардың таралуын қамтамасыз етеді, жаһандық ақпараттық кеңістікті құрайды. Бұл процестердің ажырамас және маңызды бөлігі білім беруді компьютерлендіру болып табылады. Компьютерлік технологиялар оқытудағы қосымша "қосымша" болуға арналмаған, бірақ оның тиімділігін едәуір арттыратын тұтас білім беру процесінің ажырамас бөлігі болып табылады.