International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Running Linux - Based Random Number Statistical Test on Microsoft Windows

Sayed Mohammad Badiezadegan

CEO Dataman Co. funder, M.S. Cryptography (Applied Mathematics)
Email: *CEO[at]dataman.ca*

Abstract: ***In the realm of cryptography, the significance of high-quality random numbers cannot be overstated. These numbers, generated by well-defined algorithms with input sets known as seeds, depend on the entropy of the seed for their quality. Assessing the quality of random numbers has long been a challenge, but the National Institute of Standards and Technology NIST has provided a comprehensive solution in SP 800-22, a Statistical Test Suite for Random and Pseudorandom Number Generators designed for cryptographic applications. This suite encompasses a diverse array of statistical tests, including frequency tests, spectral tests, template matching tests, and more. In this article, we elucidate the process of compiling this suite on Microsoft Windows OS, leveraging the versatile Unix-like environment and command-line interface offered by Cygwin. Cygwin, originating from Cygnus Solutions and now a part of IBM, facilitates the execution of source-based Linux applications, provided the necessary tools and libraries are pre-installed. We present a step-by-step guide to configuring Cygwin, setting environment variables, and running the NIST STS, offering a practical resource for those seeking to evaluate and enhance the quality of random number generation in cryptographic applications.***

Keywords: NIST SP 800-22, Linux, Cygwin, random number quality, statistical test,

1. Introduction

In the world of cryptography, we cannot ignore the special place of high-quality ran- dom numbers. Indeed, random numbers created with known algorithms which re- quired an input set (technically called seed), and the higher the entropy of the seed, the more the algorithms are able to produce better-quality random numbers, but how can evaluate the quality of random numbers?

The National Institute of Standards and Technology (NIST) [https://www.nist.gov/] developed SP 800-22, A Statistical Test Suite for Random and Pseudorandom Number Generators[1] for Cryp- tographic Applications, specifies a set of statistical tests for randomness that included these standard test categories:

- Frequency (Monobits) Test
- Test For Frequency Within A Block
- Runs Test
- Test For The Longest Run Of Ones In A Block
- Random Binary Matrix Rank Test
- Discrete Fourier Transform (Spectral) Test
- Non-Overlapping (Aperiodic) Template Matching Test
- Overlapping (Periodic) Template Matching Test
- Maurer's Universal Statistical Test
- Linear Complexity Test
- Serial Test
- Approximate Entropy Test
- Cumulative Sum (Cusum) Test
- Random Excursions Test
- Random Excursions Variant Test

All of the mentioned tests are implemented in one tool called Statistical Test Suite (STS) and its final version is downloadable here [https://csrc.nist.gov/CSRC/media/Projects/Random-Bit-Generation/documents/sts-2 1 2.zip]. The downloaded zip file is contain the STS required source files and the main goal of this article is to show how to com- pile the STS on Microsoft Windows OS with an excellent Unix-like environment and command-line interface for Microsoft Windows called Cygwin that was founded by Cygnus Solutions, which was later acquired by Red Hat (now part of IBM) [2].

However, Cygwin is capable of running many source-based Linux applications if the application's prerequisite tools and libraries are already installed on the system.

Project Inception

This project commences by downloading Cygwin from its official website[2]. Open a browser on the Windows system and point it to the Cygwin website. Select the Install Cygwin by running the setup-x86 64.exe link to download the setup executable file. Then, run the executable file to begin the installation and click Next on the Cygwin Setup screen.

Follow the default selection to Install from the Internet and download the updated library as well as prerequisite files from the Cygwin repository.

Click Next to continue and then select where you want the Cygwin directory and all of its support files and binaries to be installed. The default folder to install is

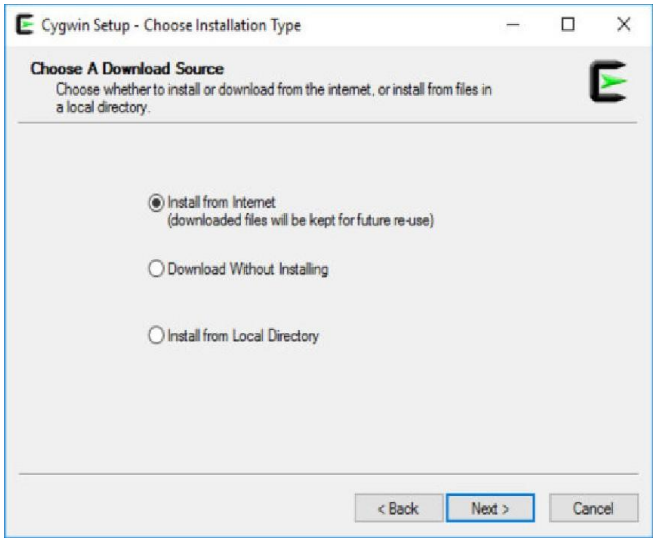

Figure 1: Cygwin installation type

C:\ cygwin64, but it can changed to C:\cygwin and also allow all users to have access to Cygwin.

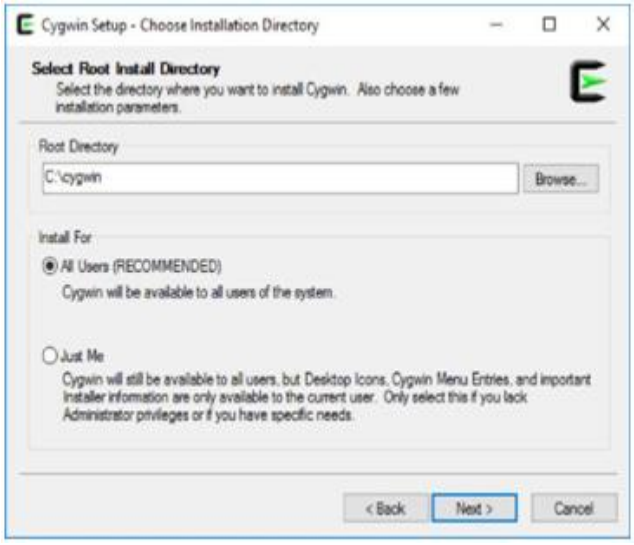

Figure 2: Cygwin installation folder

Click Next to continue and then enter the Cygwin directory name to download its files. It is recommended to use always C:\Temp. Also, if select a directory that doesn't exist, the installer prompts the user to create it.

Click Next to continue and then select Internet connection type. If there is some sort of proxy, should enter the setting here or leave it on direct connection.

Click Next to continue and then choose a download site on this screen from the list. Usually the default selection has better speed efficiency.

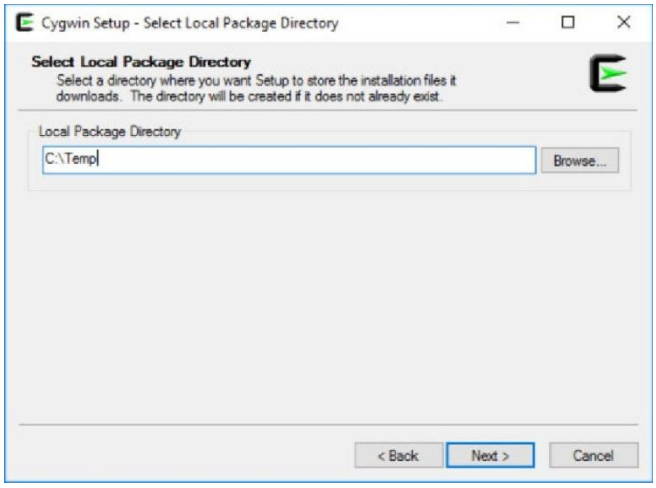

Figure 3: Cygwin local package directory

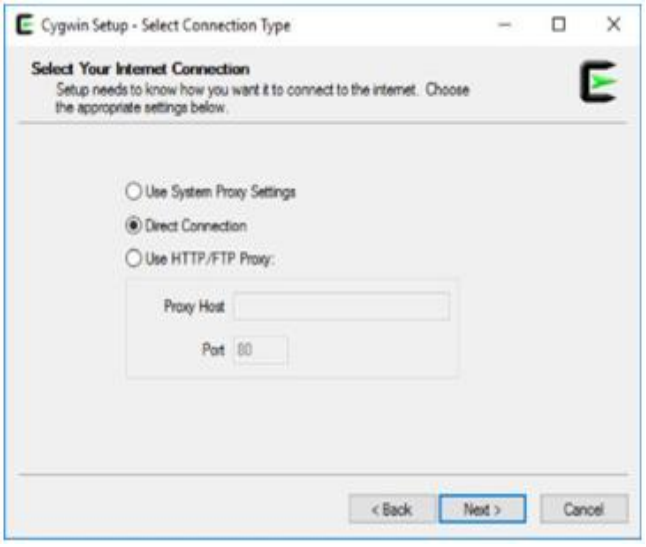

Figure 4: Connection type for installation process

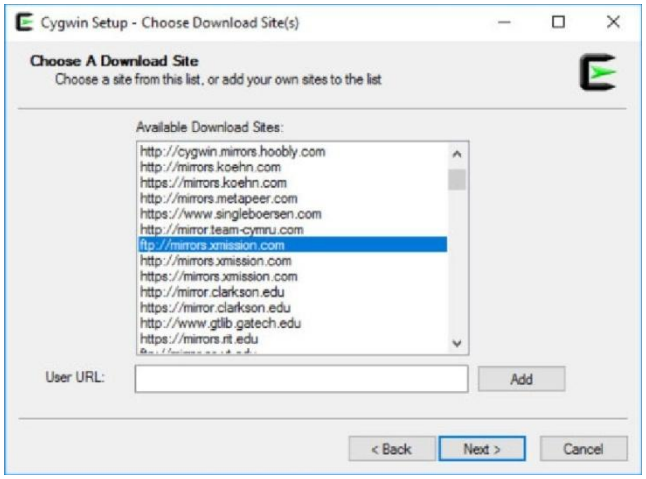

Figure 5: Download site mirror selections

After clicking next button, there is a package selection screen. If select nothing and continue with a default installation, Cygwin get a full complement of *nix commands in the C:\cygwin\bin directory. They're too numerous to list, but it's a list of standard commands.

It is highly suggest that peruse the different categories and make selections based on what project required to use on

Linux systems. For the most of Linux applications generally select OpenSSH, Bash, Bash-completion, Python, Tk/Tcl, but for NIST STS application should select ”gcc-core” and ”make” packages to install. Once made prefer selections, click Next to continue.

After Review and confirm selections, clicking Next to begin installation of selected packages.

The installation might take from a few minutes or some hours, depending on pack- age selections and internet speed.

The last screen notifies that the installation is complete and prompts user to create some handy icons. Now, Finish the installation process.

Setting the environment PATH variable

For the best results, Cygwin needs to add the C:\cygwin\bin directory to system PATH environment variable.

To set the System PATH to include\cygwin\bin directory, search for ”environment” and select the Control Panel option, Edit the system environment variables, when it appears. Select Environment Variables on the System Properties screen.

On the Environment Variables screen, select Path from the System Variables pane, and click Edit, then click New. Enter C:\cygwin\bin into the field and click OK when finished. Click OK on the other screens to save the entry and to close the System Properties window.

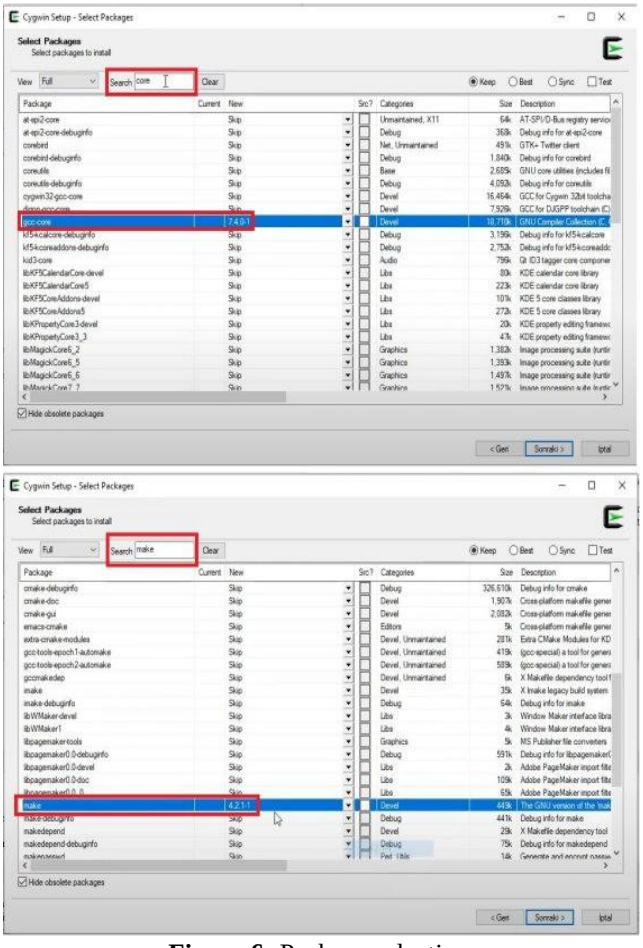

Figure 6: Package selection

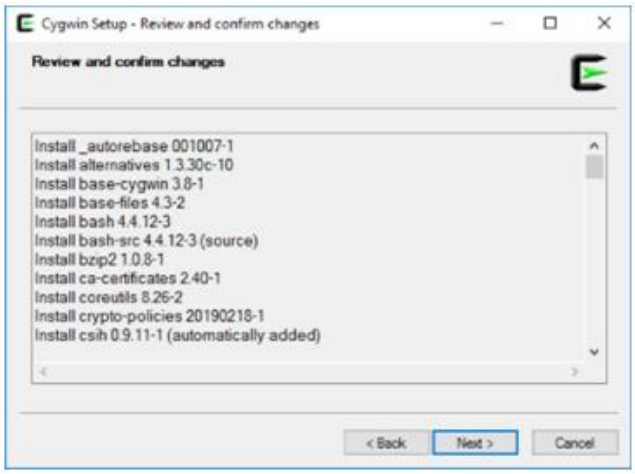

Figure 7: Cygwin installation starting

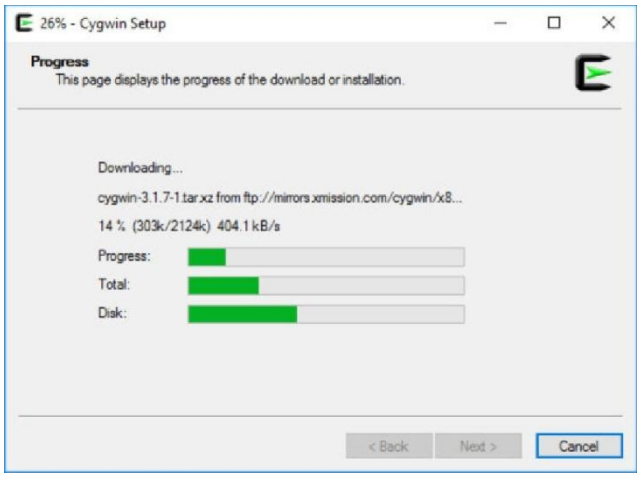

Figure 8: Cygwin installation process

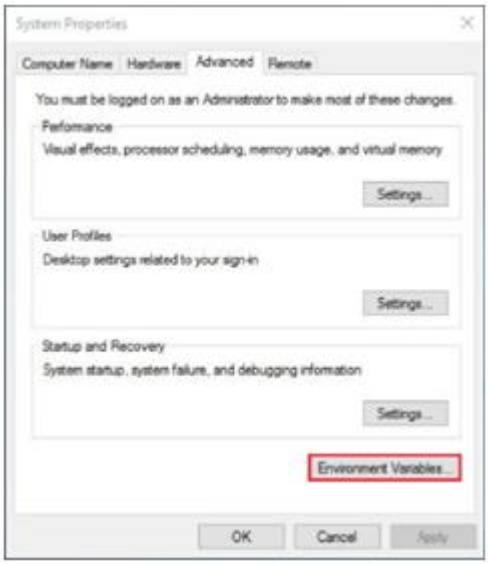

Figure 9: Environment PATH variable

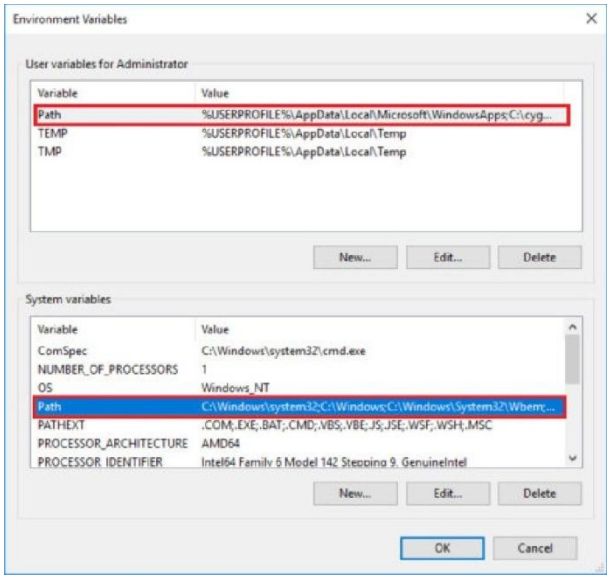

Figure 10: Environment PATH variable

Setting this system environment variable allows user to execute a Cygwin com- mand without providing the full path to the executable. This is handy for scripting too.

Test Cygwin with Running BASH

After installing the binaries in the system path, Bash can be invoked by opening a CMD window and type bash [ENTER]. Bash shell now works exactly like the installed Linux one does and it can run a few commands such as clear, ls, ls -la, pwd, and so on.

There are some differences that can be frustrating to new users if not aware of them. For example, In Bash, user will notice that the drives, C: and D:, are mounted as /cyg-drive/c and /cygdrive/d. Therefore, the C:\Temp directory is/cygdrive/c/temp in Cygwin Bash.

The Familiar directories such as /, /usr/bin, and /usr/lib exist under C:\cygwin with C:\cygwin directory as /.

Installing the NIST STS

After downloading the NIST Statistical Test Suite (STS) [https://csrc.nist.gov/CSRC/media/Projects/Random-Bit-Generation/documents/sts-2 1 2.zip] it's time to extract this com- pressed file with some file compressor tools like 7ZIP [https://www.7-zip.org/download.html] in the Windows Operating sys- tem Cygwin folder like Figure.

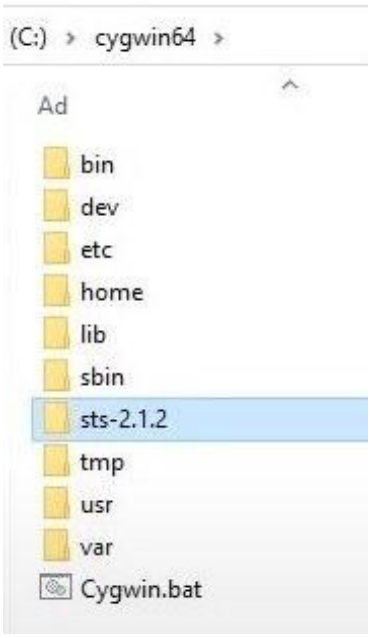

Figure 11: STS extracted folder in Cygwin folder

After successful STS uncompression, it's time to run Cygwin.bat in Windows Com- mand.

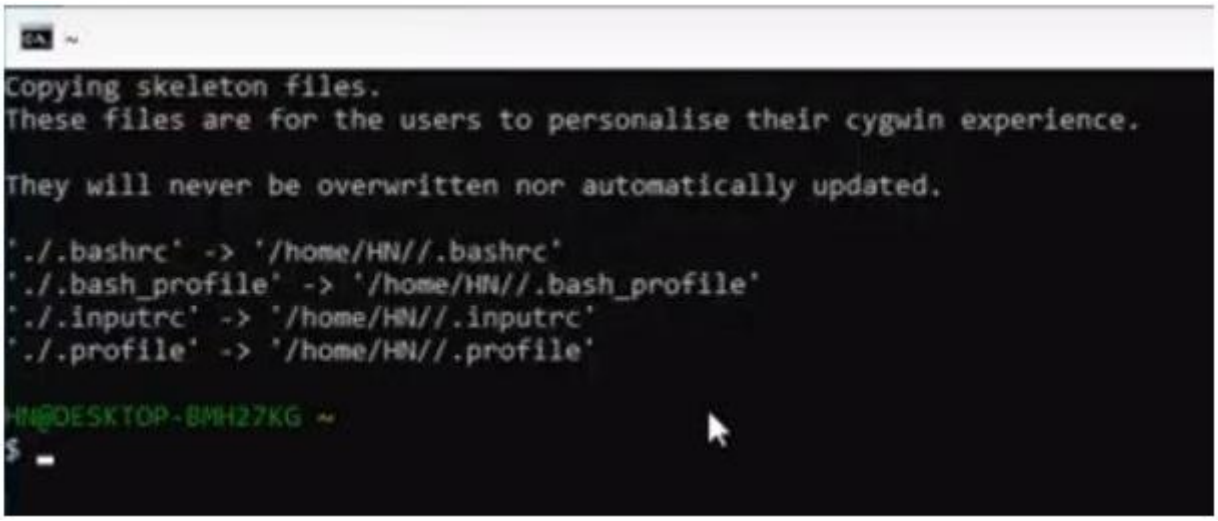

Figure 12: Running the Cygwin batch file

And then change directory (CD) to the STS extracted folder in Cygwin main folder,
Now, It's time to run make file for compiling the STS under Cygwin environment as be shown on the next page:

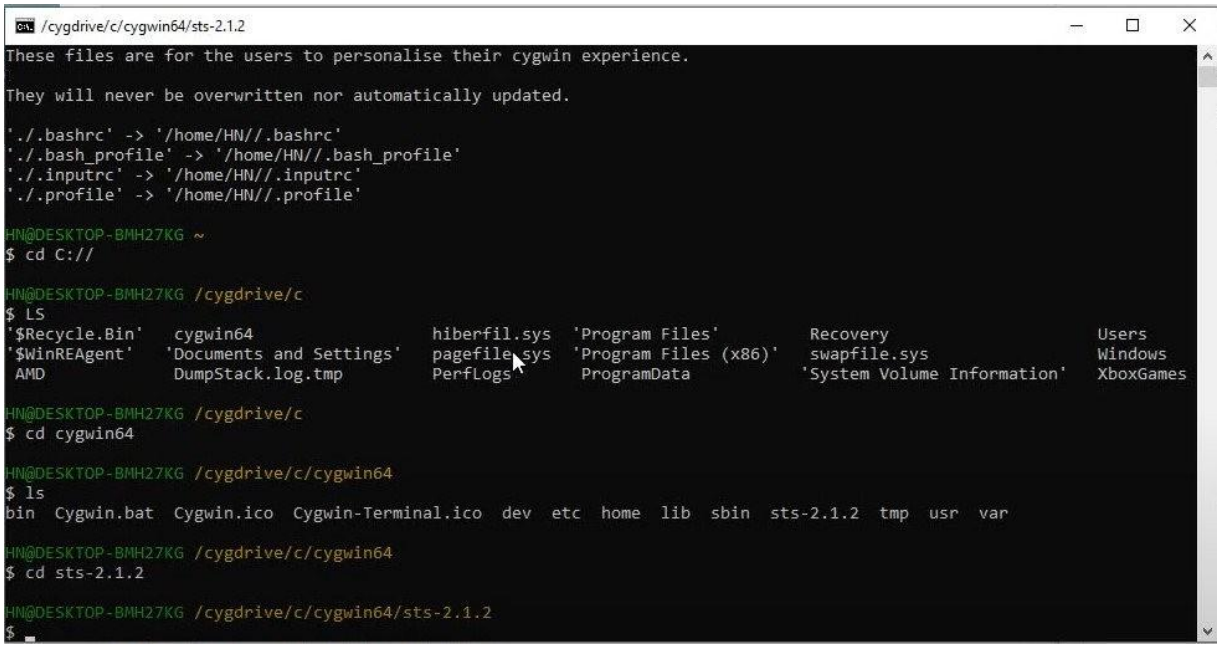

Figure 13: Change working Directory to STS folder

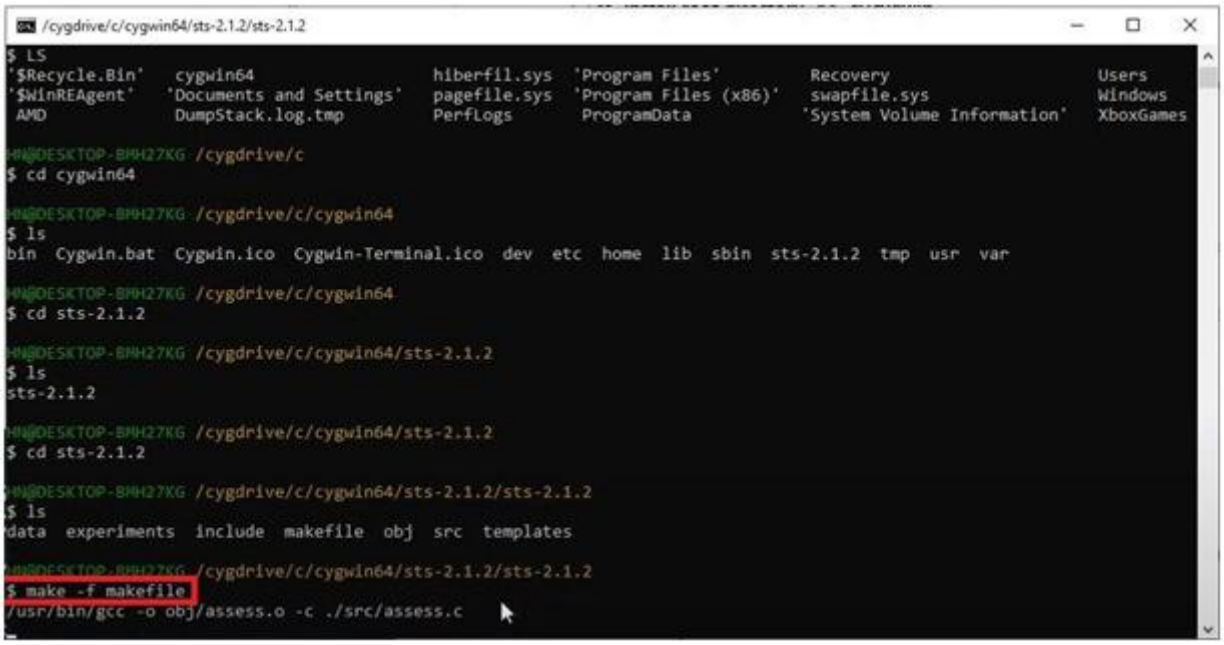

Figure 14: Change working Directory to STS folder

The following screen commands will be shown If the compiling process was fin- ished successfully:

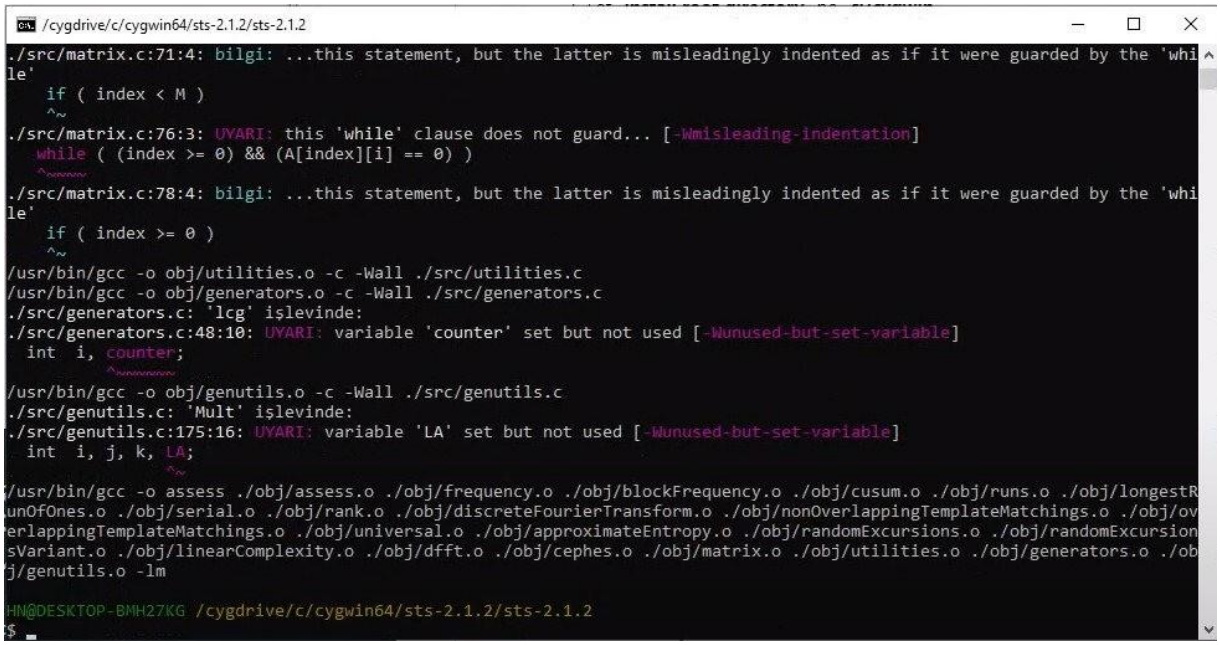

Figure 15: Successful Compiling with make

Also, the executive assess file should be generated in STS folder as be shown:

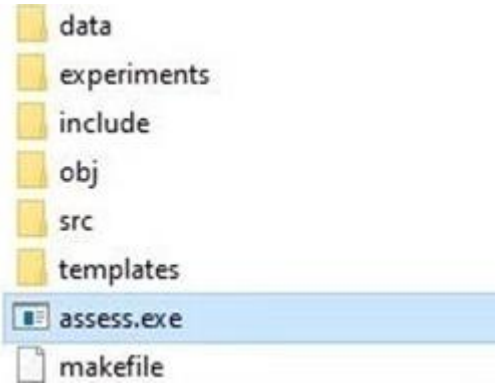

Figure 16: Assess file genarted

For running the assess file, it could be called with length of the individual bit stream, (for example: 100000)
Now, enter number [0] and enter an input file, for example, [data/data.pi] as be shown on the next page:

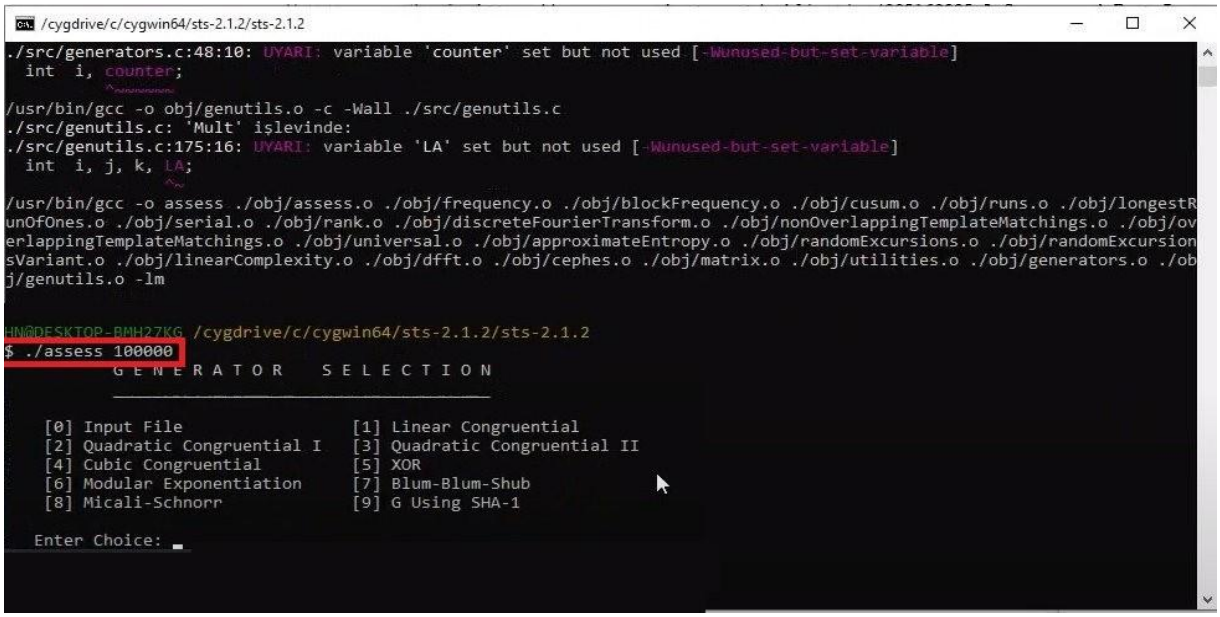

Figure 17: Assigned length of the individual bit stream

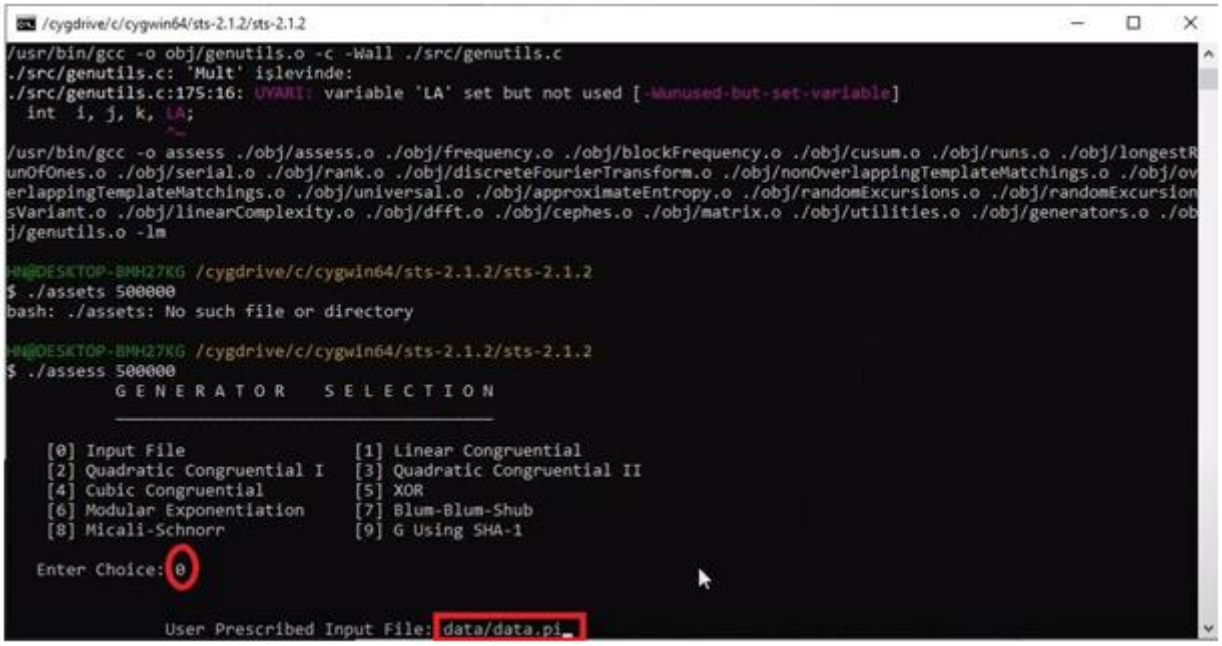

Figure 18: Assigning the data file

Now, It's time to deep inside with STS. For example, Select these options in order:

[1] ⇒[0] ⇒[10] ⇒[0]

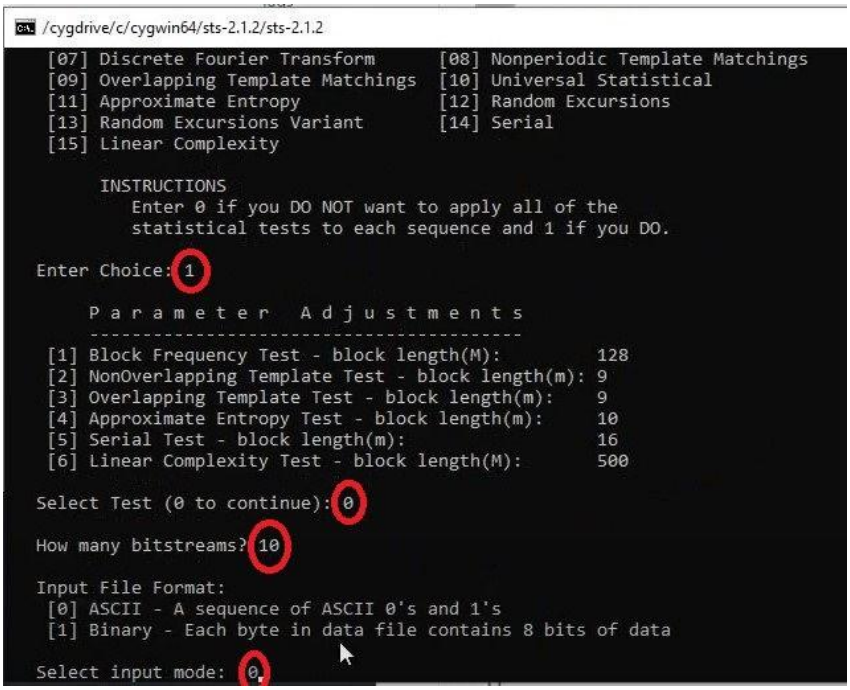

Figure 19: Select user options

If All tests done successfully, It should be finished with this screen:

In case of getting any errors about insufficient data in file, it should change the bit stream value [Figure 17] to the lower one and then start testing again.

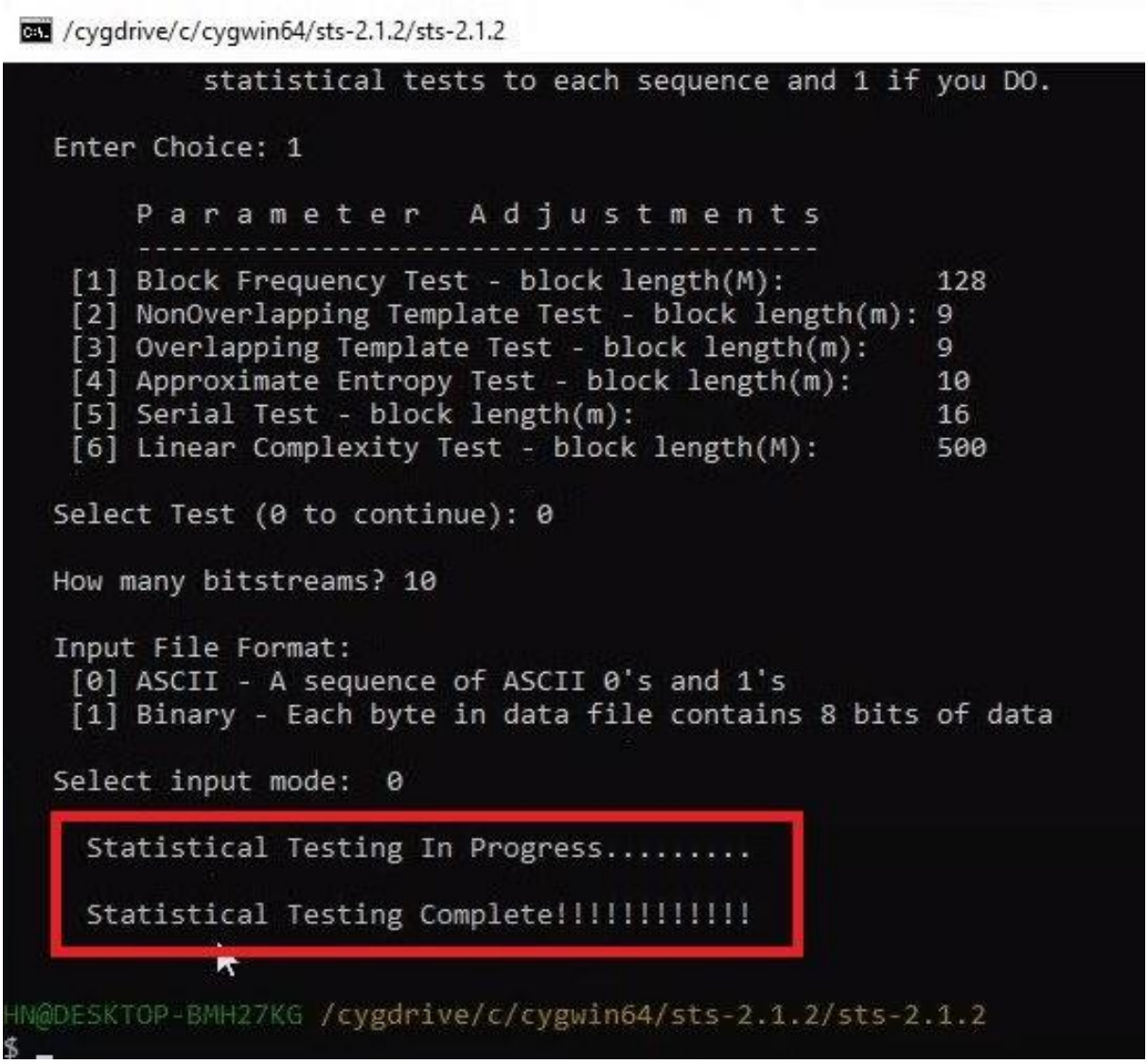

Figure 20: Test done!

Finally, There is a final testing result report is available at this text file: C:/cygwin/sts-2.1.2/experiments/AlgorithmTesting/finalAnalysisReport.txt

finalAnalysisReport.txt

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <data/data.pi>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
1	1	3	0	0	2	1	0	1	1	0.534146	10/10	Frequency
1	2	1	0	2	2	1	0	1	0	0.739918	10/10	BlockFrequency
1	1	1	2	1	0	0	2	1	1	0.911413	10/10	CumulativeSums
1	2	0	1	1	1	1	2	1	0	0.911413	10/10	CumulativeSums
0	4	1	1	0	2	0	1	0	1	0.122325	10/10	Runs
0	1	0	4	1	0	1	1	1	1	0.213309	10/10	LongestRun
1	1	0	1	1	1	2	1	0	2	0.911413	10/10	Rank
2	1	0	0	2	1	1	1	2	0	0.739918	10/10	FFT
1	2	1	0	2	2	1	1	0	0	0.739918	10/10	NonOverlappingTemplate
1	3	0	0	3	3	0	0	0	0	0.035174	10/10	NonOverlappingTemplate
3	1	1	0	0	1	0	3	0	1	0.213309	10/10	NonOverlappingTemplate
2	0	1	2	1	0	1	2	1	0	0.739918	10/10	NonOverlappingTemplate
0	2	1	1	0	2	1	1	2	0	0.739918	10/10	NonOverlappingTemplate
1	1	1	1	0	1	0	2	2	1	0.911413	10/10	NonOverlappingTemplate
0	2	1	1	1	2	1	0	1	1	0.911413	10/10	NonOverlappingTemplate
2	1	1	1	1	0	1	3	0	0	0.534146	10/10	NonOverlappingTemplate
1	0	1	1	1	2	1	0	2	1	0.911413	9/10	NonOverlappingTemplate
0	0	2	1	0	1	1	4	1	0	0.122325	10/10	NonOverlappingTemplate
0	2	0	2	0	1	2	1	1	1	0.739918	10/10	NonOverlappingTemplate
2	1	1	1	1	1	0	0	2	1	0.911413	10/10	NonOverlappingTemplate
1	1	3	1	0	1	1	1	1	0	0.739918	10/10	NonOverlappingTemplate
4	0	1	0	0	1	1	1	0	2	0.122325	9/10	NonOverlappingTemplate
1	2	1	0	1	2	1	0	0	2	0.739918	10/10	NonOverlappingTemplate
3	0	1	1	1	1	0	2	1	0	0.534146	10/10	NonOverlappingTemplate
2	1	0	0	2	1	1	2	0	1	0.739918	9/10	NonOverlappingTemplate
0	0	1	3	1	2	0	1	1	1	0.534146	10/10	NonOverlappingTemplate
0	1	1	1	1	0	0	2	3	1	0.534146	10/10	NonOverlappingTemplate

Figure 21: Report

References

[1] NIST Special Publication 800,22 - https://doi.org/10.6028/NIST.SP.800-22r1a, https://nvlpubs.nist.gov/nistpubs/legacy/sp/ nistspecialpublication800-22r1a.pdf
[2] A brief history of the Cygwin project by Cygnus solutions, https://cygwin. com/cygwin-ug-net/brief-history.html