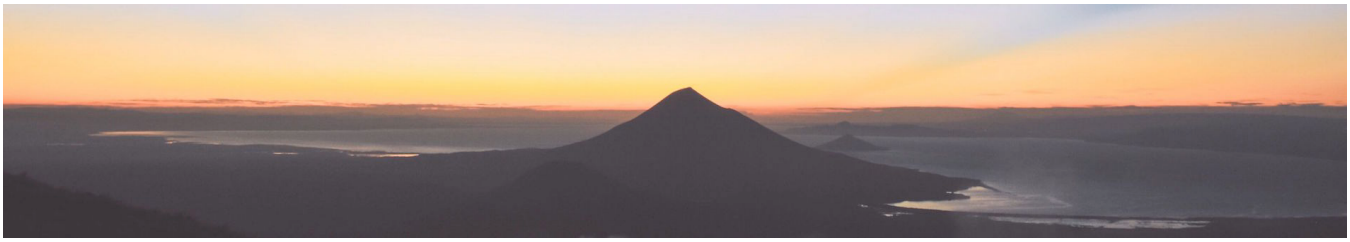
Random Number Generator

Welcome to your first space. Go ahead, edit and customize this home page any way you like. We've added some sample content to get you started.



Goal

Your space homepage should summarize what the space is for, and provide links to key resources for your team.

Core team

Harvey Honner-white
Team Lead

Alana Baczewski
Tech Lead

Sameer Farrell
Marketing

Mia Bednarczyk
Recruitment

Roadmap

You can edit this roadmap or create a new one by adding the Roadmap Planner macro from the Insert menu. Link your Confluence pages to each bar to add visibility, and find more tips by reading the Atlassian blog: Plan better in 2015 with the Roadmap Planner macro.

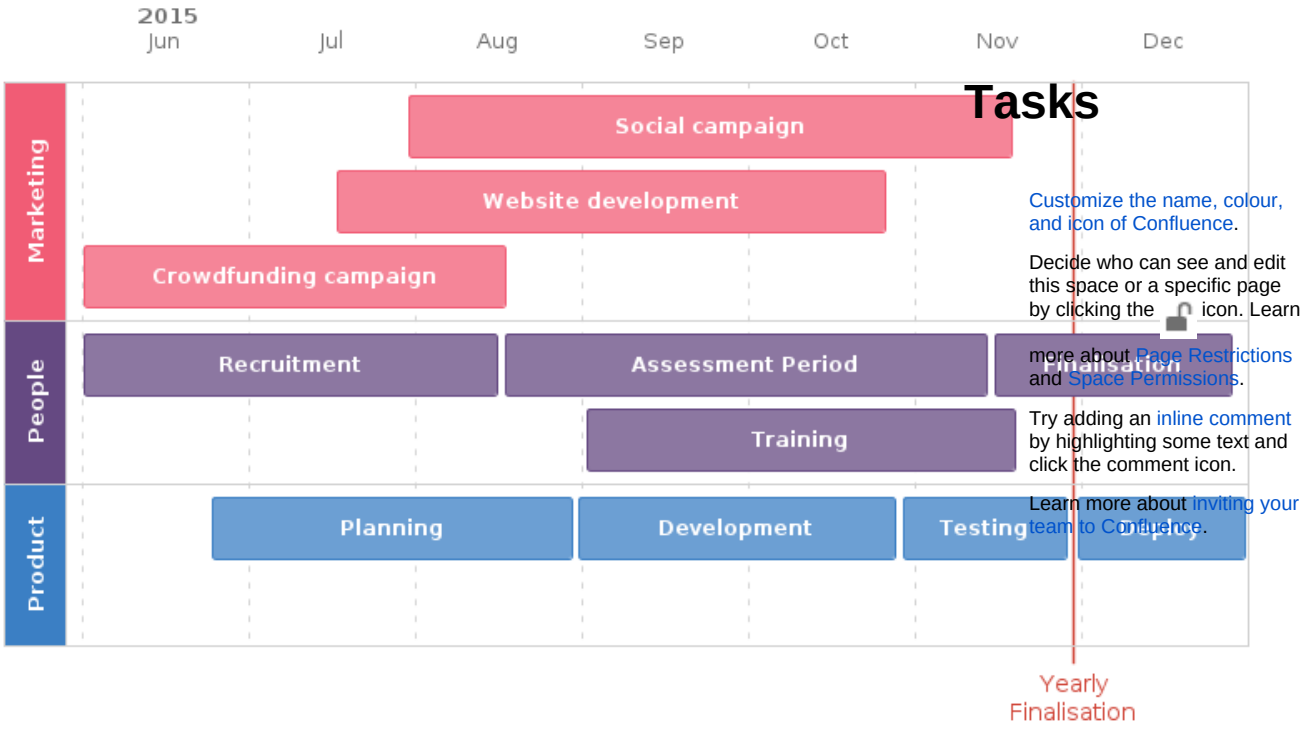
Quick navigation

When you create new pages in this space, they'll appear here automatically.

- Documentation of the random number generator

Useful links

Link	Description
Confluence 101: organize your work in spaces	Chances are, the information you need to do your job lives in multiple places. Word docs, Evernote files, email, PDFs, even Post-it notes. It's scattered among different systems. And to make matters worse, *the stuff your teammates need is equally siloed*. If information had feelings, it would be lonely. But with Confluence, you can bring all that information into one place.
Confluence 101: discuss work with your team	Getting a project outlined and adding the right content are just the first steps. Now it's time for your team to weigh in. Confluence makes it easy to discuss your work - with your team, your boss, or your entire company - in the same place where you organized and created it.
Confluence 101: create content with pages	Think of pages as a New Age "document." If Word docs were rotary phones, Confluence pages would be smart phones. A smart phone still makes calls (like their rotary counterparts), but it can do so much more than that



Know your spaces

Everything your team is working on - meeting notes and agendas, project plans and timelines, technical documentation and more - is located in a space; it's home base for your team.

A small team should plan to have a space for the team, and a space for each big project. If you'll be working in Confluence with several other teams and departments, we recommend a space for each team as well as a space for each major cross-team project. The key is to think of a space as the container that holds all the important stuff - like pages, files, and blog posts - a team, group, or project needs to work.

Know your pages

If you're working on something related to your team - project plans, product requirements, blog posts, internal communications, you name it - create and store it in a Confluence page. Confluence pages offer a lot of flexibility in creating and storing information, and there are a number of useful page templates included to get you started, like the meeting notes template. Your spaces should be filled with pages that document your business processes, outline your plans, contain your files, and report on your progress. The more you learn to do in Confluence (adding tables and graphs, or embedding video and links are great places to start), the more engaging and helpful your pages will become.

Learn more by reading Confluence 101: organize your work in spaces

---

Documentation of the random number generator

The document contains the concept of generating and applying random numbers and a hardware implementation. The problem of the lack of randomness in software solutions is undoubtedly important. Such numbers are widely used in cryptographic encryption, internet protocols, checksums, and in a great number of other applications. In the above work, the entire process of creating such a solution will be described, from the concept, through the selection of components, ending with tests, as well as the theory behind the problem.

Random numbers in computer science

At the very beginning we should describe the difference which is significant for this project. Mostly when it comes to random numbers in the IT environment it is really about pseudorandom numbers. Their name is not accidental, because in software solutions it is almost impossible to achieve true randomness. In this case, generating a random number is based on specifying a "seed", i.e. a number or a vector that initializes the generator. In many programming languages, the built-in mechanism treats as a seed the number of seconds since midnight on January 1, 1970. Naturally, this gives a great deal of unique grains, but they are still deterministic, so when someone finds the point in time at which pseudo-random numbers were generated, he is able to decode the sequence of these numbers and I will find dependencies among them.

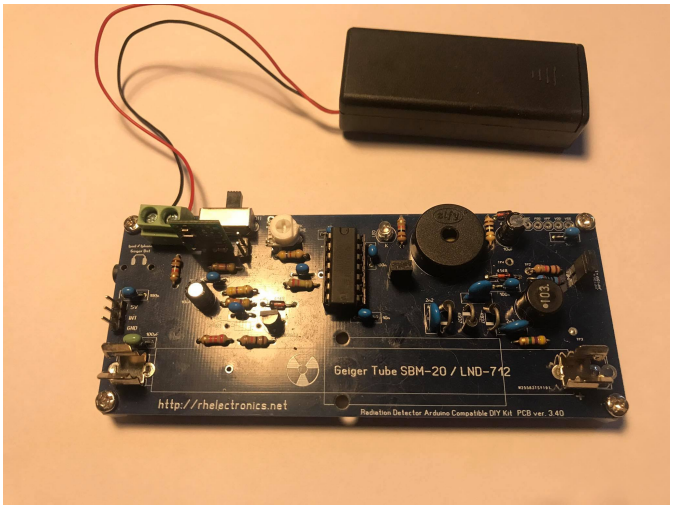
On the other hand, there are genuinely random number generators which rely on one or more sources of entropy. Entropy is characterized by the uncertainty that an event will occur at the next moment. Consequently, such generators are able to provide a given system with a non-deterministic sequence of bits, which is of great importance in many branches of computer science, especially in cryptography.

Selection of hardware components

In order to detect ionizing radiation events, a Geiger-Muller counter is needed, which in this project was powered by an Arduino microcontroller. Beads with a trace of uranium near the Geiger tube will detect radioactive decay. The 8-segment display with an expansion board will facilitate the reading of the number generated by the SPI protocol.

List of used elements:

- Geiger counter kit

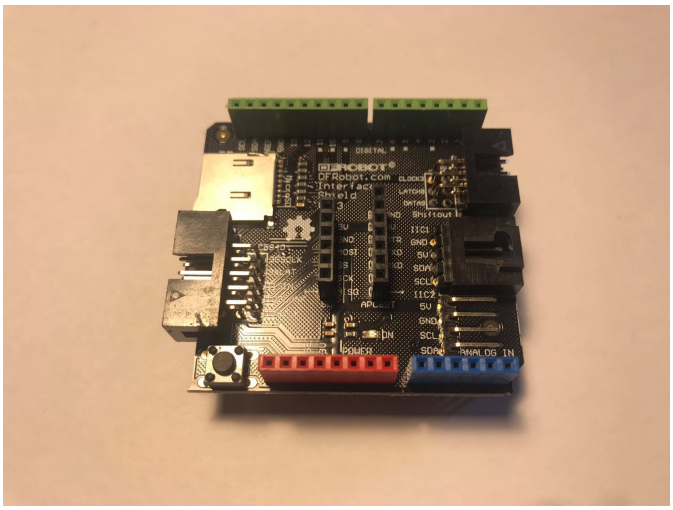


- Geiger tube

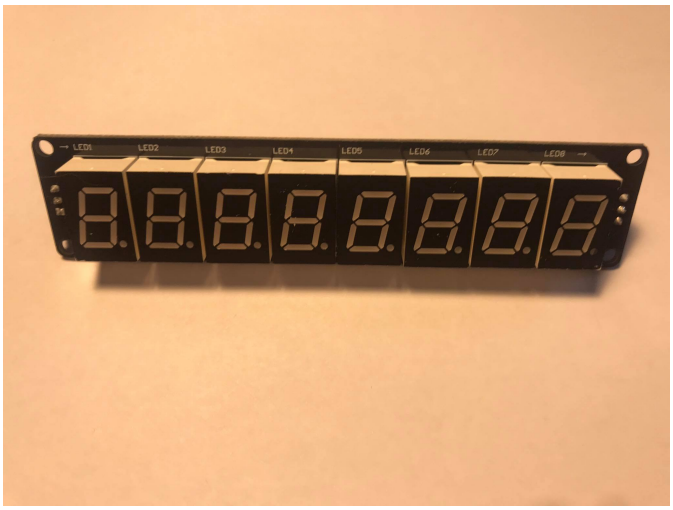
- Beads with traces of uranium

- Arduino Uno microcontroller

- Extension board for Arduino



- Tabolic module for 8-segment displays


LED1
LED2
LED3
LED4
LED5
LED6
LED7
LED8

Development environment

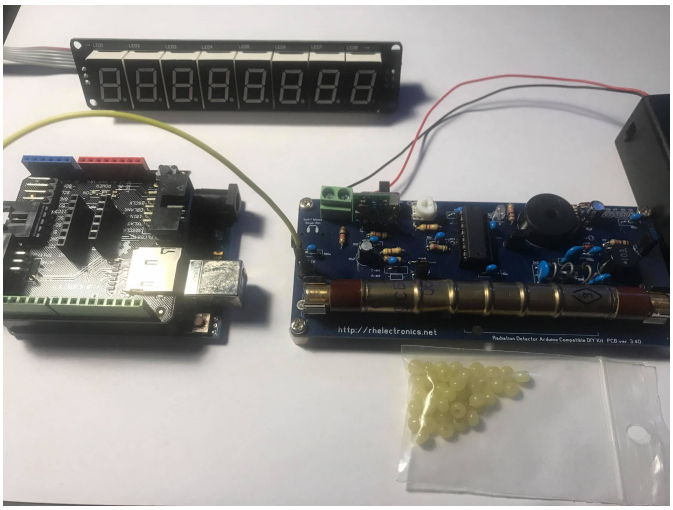
The project uses an Arduino microcontroller. In order to verify the code and update the firmware directly on the hardware, the development environment chosen is the Arduino IDE.

Estimate

Component name	Price (in z)
Arduino Uno	15
DFRobot Interface Shield	100
Geiger counter	135
Beads with traces of uranium	20
8-segment display	49
Geiger tube	80
Sum	400

The cost of the entire project was 400 z.

Implementation

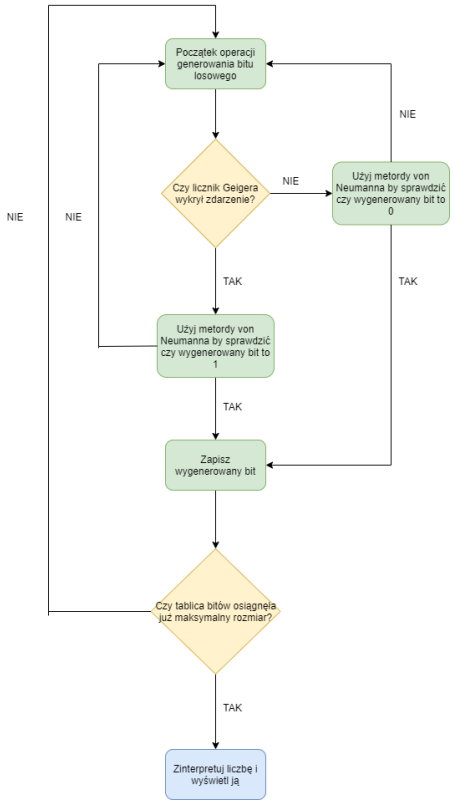


The kit is ready to run.

It is assumed that each bit will be generated every one millisecond. By default, a bit in time without a counter interrupt is translated to zero, and it is set to one when an event is received. To prevent the problem of the dominance of zeros, the von Neumann method was used, which consists in comparing two successive generated bits:

- If the bits have this value, they are discarded.
- If the bit sequence is 1.0, the generated bit is 1.
- If the bit sequence is 0, 1, the generated bit is 0.

By default, 8 bits are read, which gives the range of the generated number from 0 to 255. This string can be read through the microcontroller's serial port or shown on the display.



Block diagram of the algorithm.

Tests

Tests have been performed. Two test cases, TES-1 and TES-3, have been written. One error was identified during the test execution TES-2. While still testing, the bug was identified and fixed.

Summary

In summary, the implementation of the true random number generator was successful. Studying the subject of true randomness in the world of computer science allows you to understand the complexity of the problem in the field of data security and encryption. The solution itself caused several hardware problems, such as the selection of the microcontroller and the understanding of the interrupt technique. Also, the source of entropy changed during the project, due to limited knowledge in the field of image processing, so that the lava lamp as entropy did not work. One can conclude that even outside of business applications it is worth having access to real randomness, for example in home automation and remote access
to her via the Internet. It is also worth being aware of the mechanisms that operate in the systems that people use on a daily basis. Examples include banking or a multitude of applications that store and process sensitive personal data. Knowing that there is a possibility of maximum security by using nondeterministic keys or tokens, you can be more sure that our data will not be decrypted by people or institutions who could depend on them. It is increasingly said that personal information is the most valuable in these times, and that human preferences are used to feed complex machine learning algorithms.