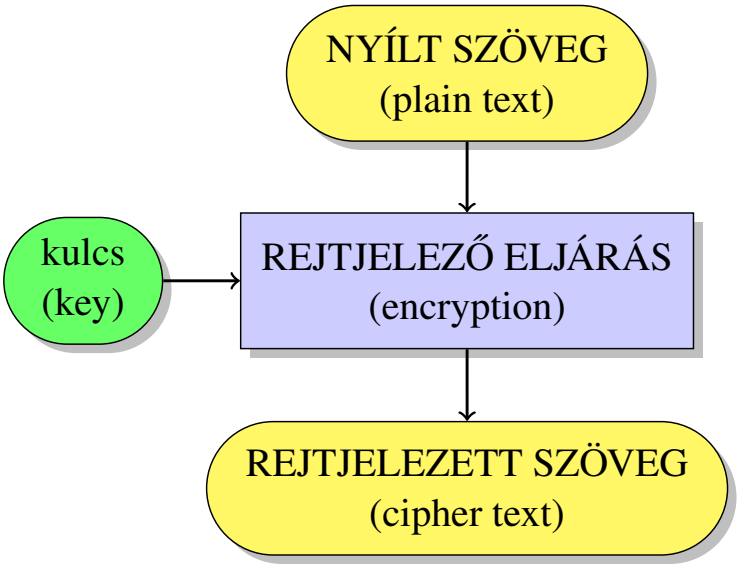
A kriptorendszer alapfogalmai: Rejtjelezés



REALENIGMASTORY

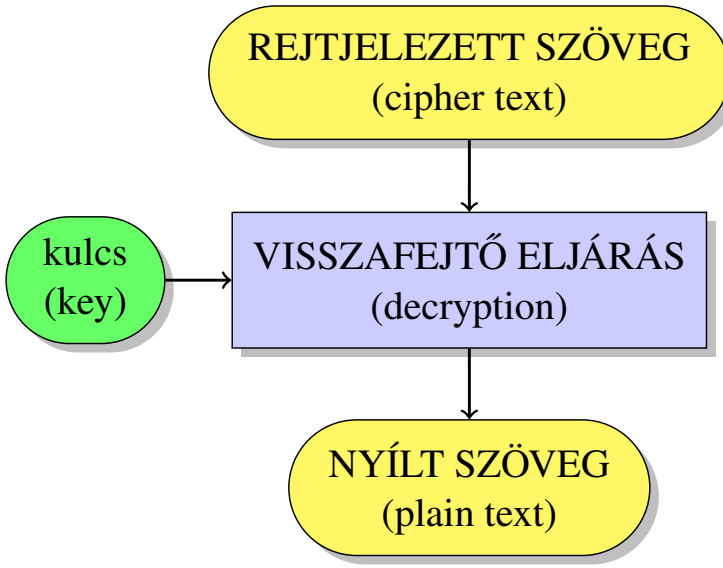
Ceasar-rejtjel
kulcs=7

YLHSLUPNTHZAVYF

A kriptorendszer kulcsterének fogalma

A kriptorendszer olyan kulcsainak halmaza, amik lényegesen különböző rejtjelezett szövegeket eredményeznek.

A kriptorendszer alapfogalmai: Visszafejtés



GQJYHMQJDUFWP

Ceasar-rejtjel
kulcs=-5

BLETCHLEYPARK

A Kerckhoff-féle alapelvek és a „katasztrófa-forgatókönyv”

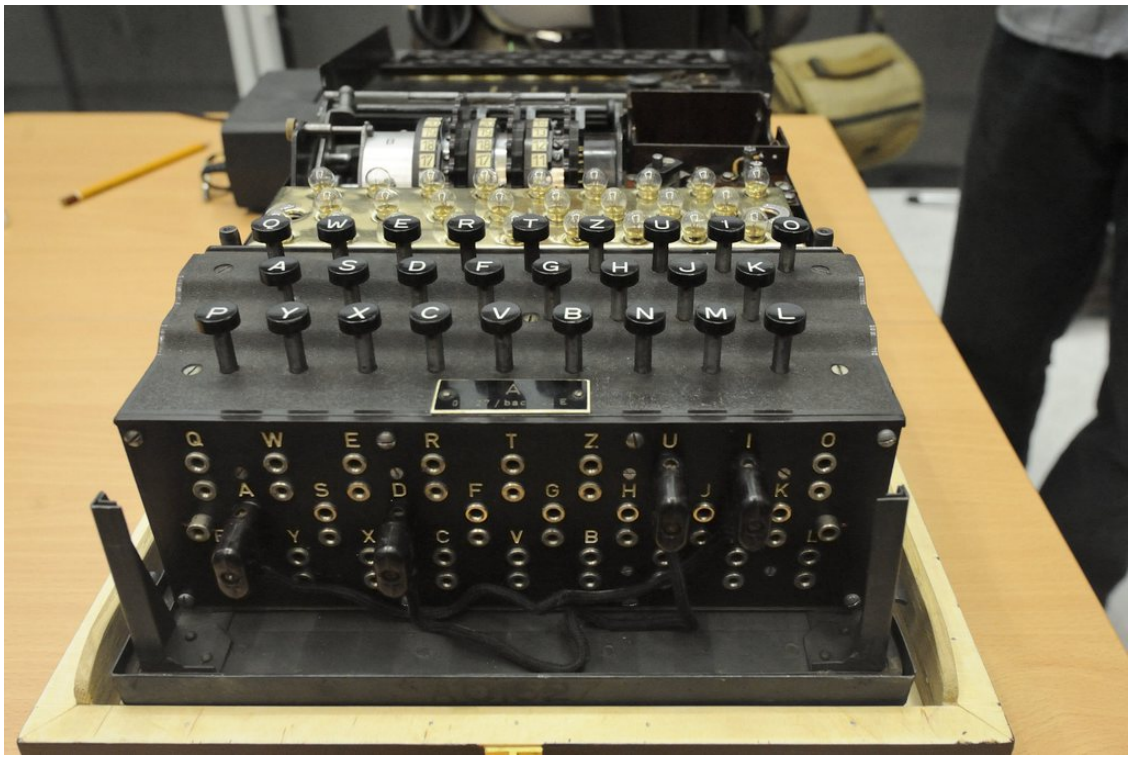
Auguste Kerckhoffs, *La Cryptographie Militaire*, 1883

1. A rendszernek gyakorlatilag, sőt lehetőleg matematikailag is **visszafejthetetlennek** kell lennie. A **rendszer maga nem lehet titkos,** nem jelenthet problémát, ha azt ismeri az ellenség.
2. A **kulcsnak rövidnek és könnyen továbbíthatónak** kell lenni, írott jegyzetek használata nélkül is.
3. A rendszer legyen használható a **Morse-távírós** kommunikációban.
4. A rendszernek **hordozhatónak** kell lennie, egy személy is tudja üzemelni.

A modern „katasztrófa-forgatókönyv” feltételezései

1. Az ellenfél teljesen ismeri a kriptorendszerünket.
2. Az ellenfél el tudja olvasni az összes rejtjelezett szövegünket.
3. Az ellenfél ismeri jelentős mennyiségű rejtjelezett szövegünkhöz tartozó nyílt szövegünket.

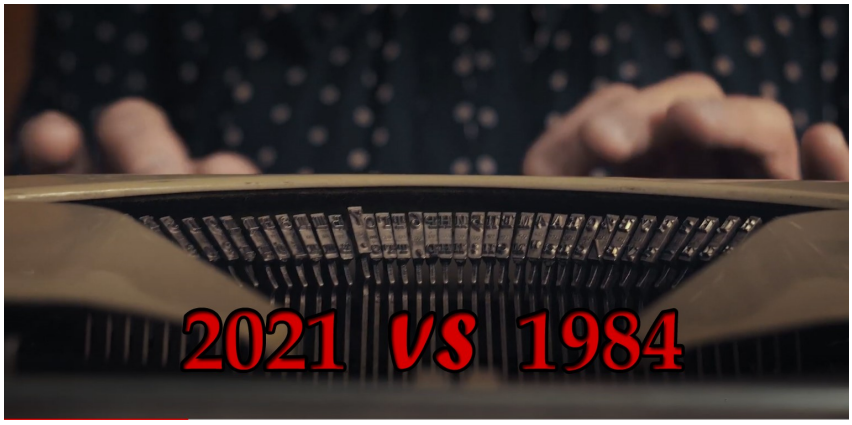
Az Enigma készülék



Problem 1. «2020»

A cipher machine `WINSTON` can transform a binary sequence in the following way. A sequence S is given, a cipher machine can add to S or remove from S any subsequence of the form 11, 101, 1001, 10...01. Also, it can add to S or remove from S any number of zeros.

When special agent Smith entered the room there were two identical `WINSTON` machines. He was curious to encrypt number 2020 and he tried to encrypt the number in it's binary form. The first cipher machine returned the binary form of number 1984, the second one returned the binary form of number 2021. Smith understood that one of the machines is broken. How did he know that?



NSUCRYPTO - 2021

the Eighth International Olympiad in Cryptography October 17-25

Dedicated to the 100th anniversary of the Cryptographic Service of Russian Federation

NSUCRYPTO is the unique cryptographic Olympiad containing scientific mathematical problems for school students, university students and professionals from any country. Its aim is to involve young researchers in solving curious and tough scientific problems of modern cryptography.

World-wide Olympiad for everybody! To become a participant you need to register on the website **nsucrypto.nsu.ru** and choose your category:

* **school student** * **university student** * **professional**

Registration and participation of the Olympiad are free of charge.

There will be **two independent the Internet rounds:**

The First round: October 17, 2021 at 16:00 NOVT (UTC +7)
(duration 4 hours 30 minutes; individual round; theoretical problems in math of crypto;
Section A - for school students, **Section B** - for university students and professionals)

The Second round: October 18-25, 2021
(duration - a week; team round (up to 3 members); hard research and programming problems)

Language of the Olympiad is English.

Organizers:
Novosibirsk State University
Sobolev Institute of Mathematics
KU Leuven
Belarusian State University
Tomsk State University

General sponsors:
Cryptographic Center (Novosibirsk)
Mathematical Center in Akademgorodok
Novosibirsk State University

Prizes are waiting for you!

We invite you to participate! Welcome!

Program Committee

S.Agievich (Belarusian State University, Belarus'), **L.Budaghyan** (University of Bergen, Norway), **A.Canteaut** (INRIA Paris, France), **C.Carlet** (University of Paris 8, France), **J.Daemen** (Radboud University, The Netherlands), **S.Gangopadhyay** (Indian Institute of Technology Roorkee, India), **E.Gorkunov** (Sobolev Institute of Mathematics, Russia), **A.Gorodilova** (Novosibirsk State University, Russia), **T.Helleseth** (University of Bergen, Norway), **X.Hou** (University of South Florida, USA), **V.Idrisova** (Sobolev Institute of Mathematics, Russia), **K.Kalgin** (Novosibirsk State University, Russia), **D.Kolegov** (Tomsk State University, Russia), **N.Kolomeec** (Sobolev Institute of Mathematics, Russia), **A.Kutsenko** (Novosibirsk State University, Russia), **N.Mouha** (Computer Security Division of NIST, USA), **S.Nikova** (KU Leuven, Belgium), **I.Pankratova** (Tomsk State University, Russia), **S.Picek** (Delft University of Technology, The Netherlands), **B.Preneel** (KU Leuven, Belgium), **M.Pudovkina** (Bauman Moscow State Technical University, Russia), **V.Rijmen** (KU Leuven, Belgium), **R.Rosie** (University of Luxembourg, Luxembourg), **A.Semenov** (Institute for System Dynamics and Control Theory, Russia), **F.Sica** (Nazarbayev University, Kazakhstan), **P.Stanica** (Naval Postgraduate School, USA), **N.Tokareva** (Novosibirsk State University, Russia), **M.Turan** (National Institute of Standards and Technology, USA), **A.Udovenko** (CryptoExperts, France), **A.Zubkov** (Steklov Mathematical Institute of RAS, Russia)

More details on nsucrypto.nsu.ru For all questions please contact nsucrypto@nsu.ru

MATHEMATICAL CENTER IN AKADEMGORODOK
Novosibirsk State University *THE REAL SCIENCE
Sobolev Institute of Mathematics
KU LEUVEN
BELARUSIAN STATE UNIVERSITY
National Research Tomsk State University