Modern titkosírások és a matematika

Az Enigma feltörése

Nagy Gábor Péter

Szegedi Tudományegyetem
Bolyai Intézet, Geometria Tanszék

Kutatók Éjszakája
2015. szeptember 25.

Tagolás

1. A titkosírások elméleti alapelvei
2. Az Enigma
3. Napjaink kriptorendszerei

Titkosírások tudományos alapja

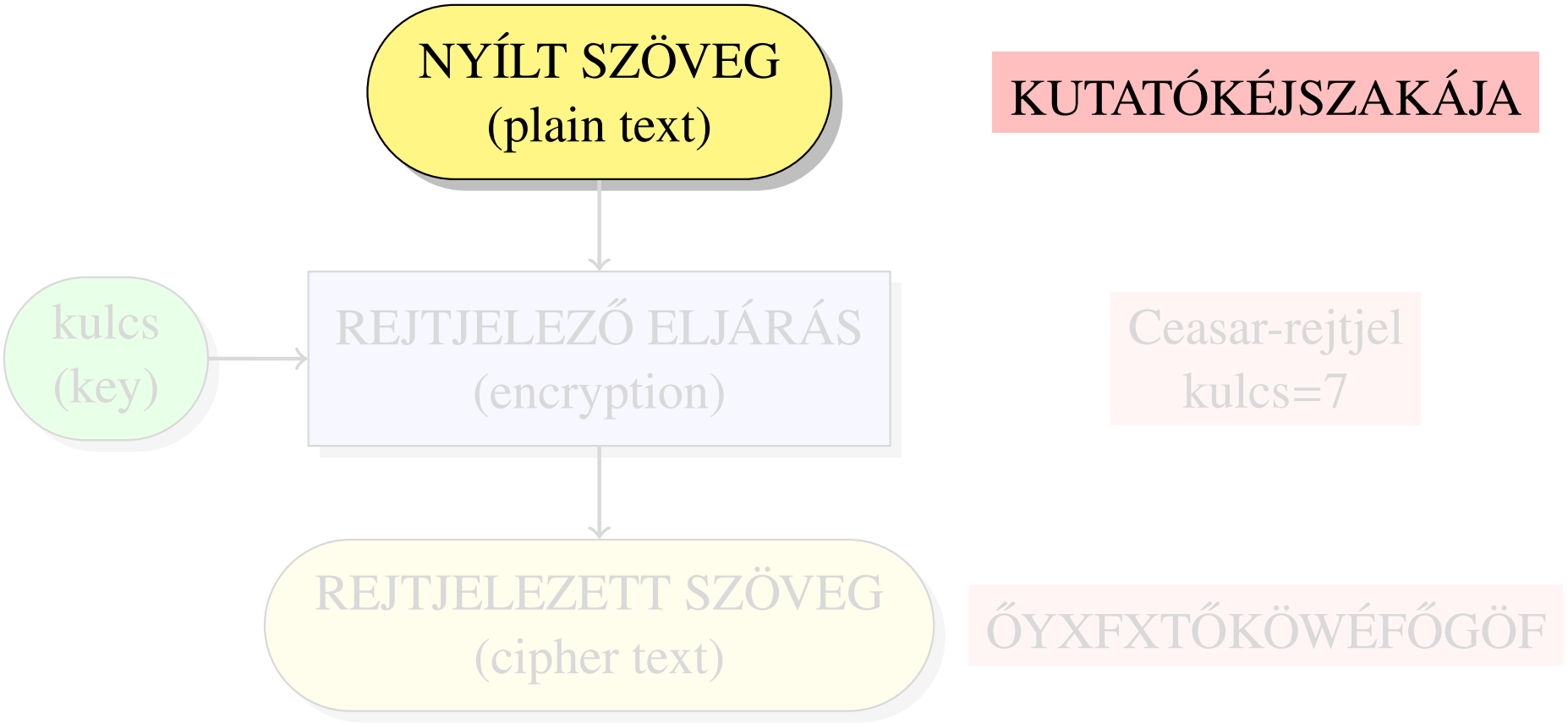
A történeti háttér:

- A titkosírások modern módszerei a 19. század elejétől terjedtek el.
- Ezeket a mai napig elsősorban katonai vagy üzleti célokra használják.
- Ekkortól próbálják a titkosítási technikákat tudományos alapokra helyezni

A KRIPTOANALÍZIS tudományos módszerei:

- Hagyományos: Nyelvészet, matematikai statisztika
- Modern: Absztrakt algebra, bonyolultságelmélet, számítástudomány

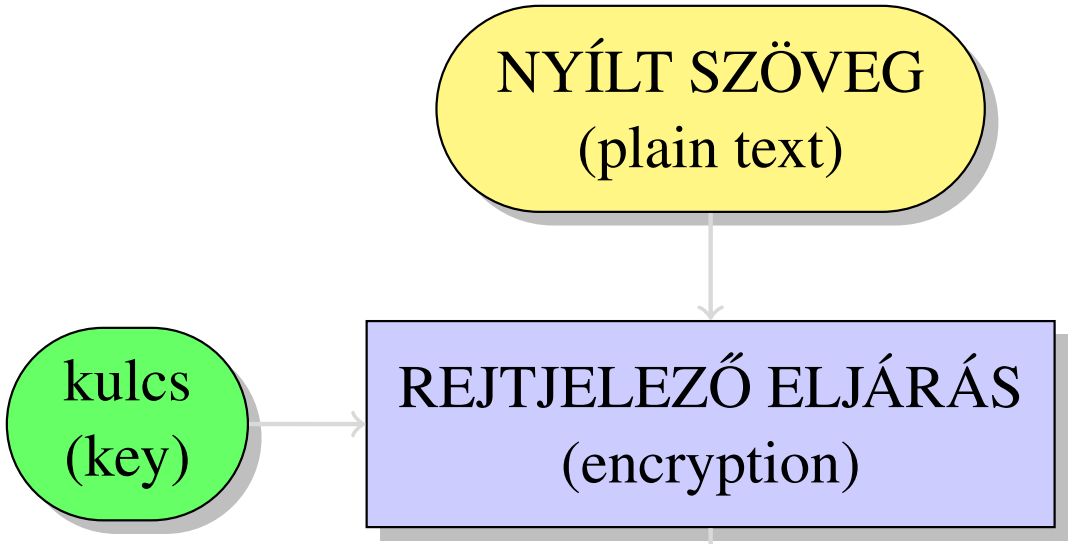
A kriptorendszer alapfogalmai: Rejtjelezés



A kriptorendszer kulcsterének fogalma

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

A kriptorendszer alapfogalmai: Rejtjelezés



KUTATÓKÉJSZAKÁJA

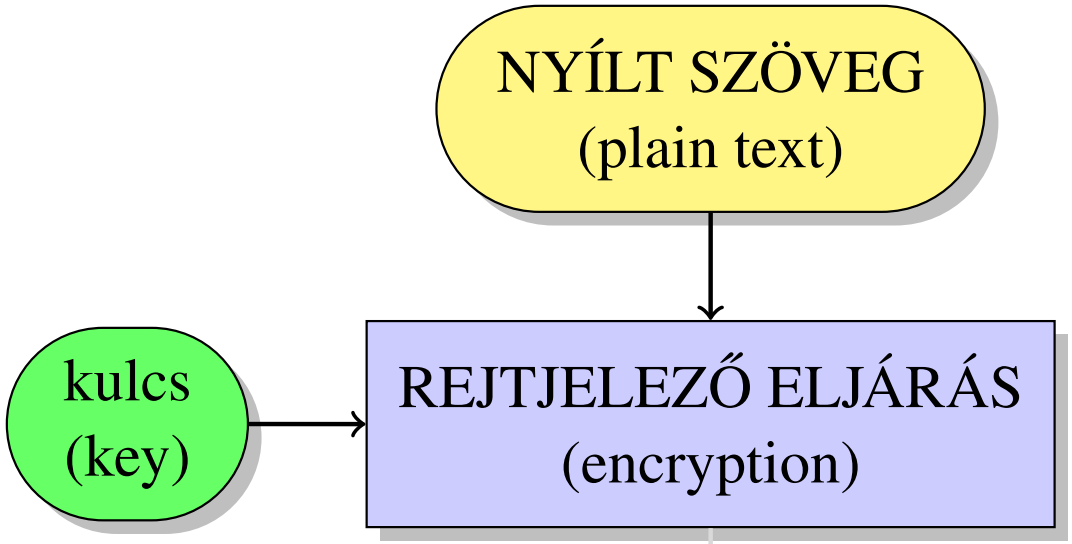
Ceasar-rejtjel
kulcs=7

ŐYXFXTŐKÖWÉFŐGÖF

A kriptorendszer kulcsterének fogalma

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

A kriptorendszer alapfogalmai: Rejtjelezés



KUTATÓKÉJSZAKÁJA

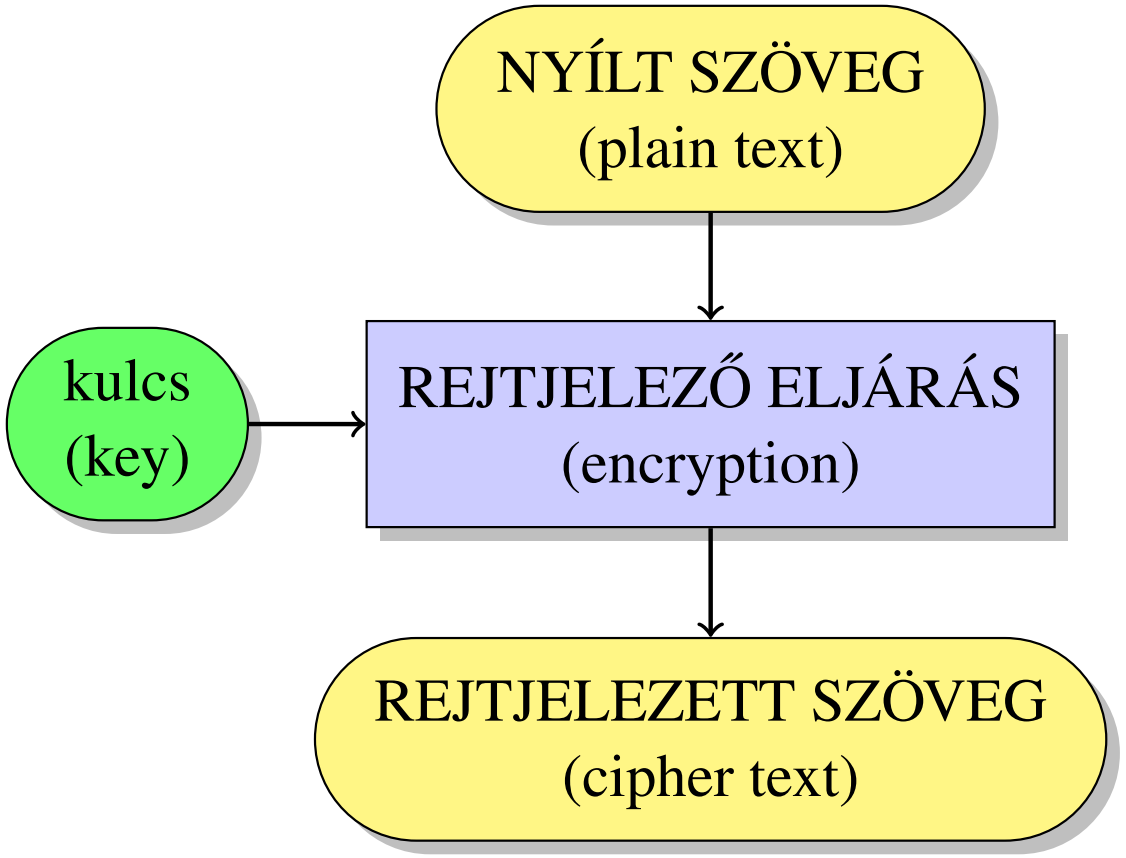
Ceasar-rejtjel
kulcs=7

ŐYXFXTŐKÖWÉFŐGÖF

A kriptorendszer kulcsterének fogalma

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

A kriptorendszer alapfogalmai: Rejtjelezés



KUTATÓKÉJSZAKÁJA

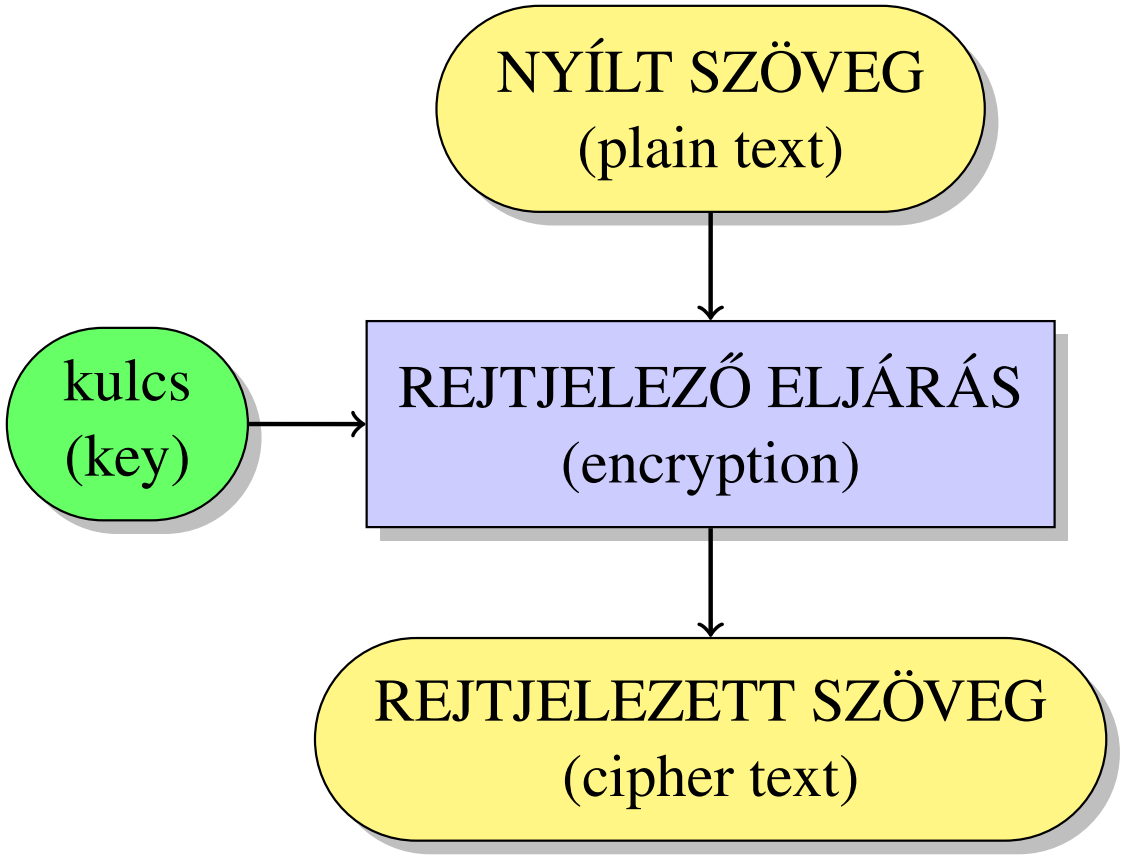
Ceasar-rejtjel
kulcs=7

ŐYXFXTŐKÖWÉFŐGÖF

A kriptorendszer kulcsterének fogalma

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

A kriptorendszer alapfogalmai: Rejtjelezés



KUTATÓKÉJSZAKÁJA

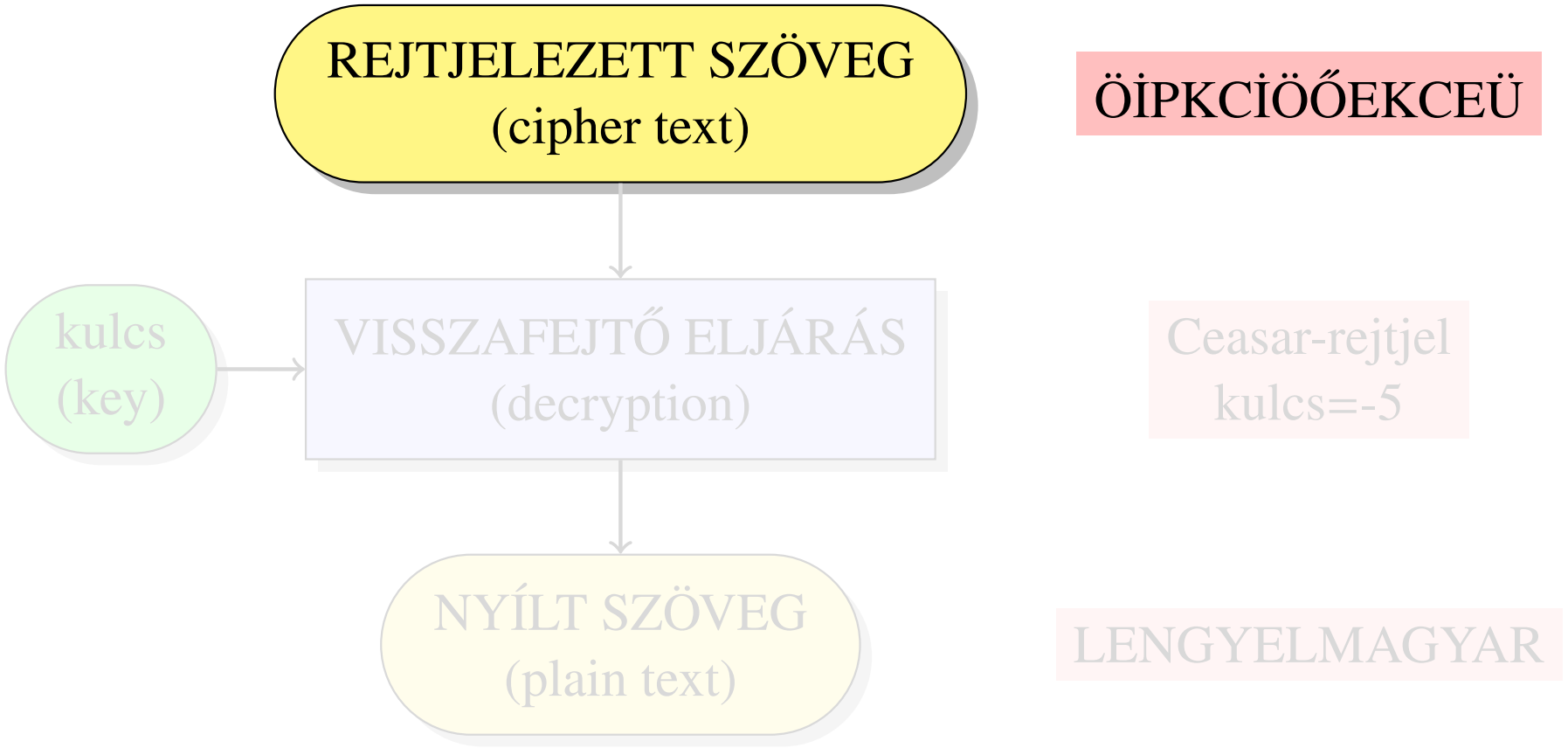
Ceasar-rejtjel
kulcs=7

ŐYXFXTŐKÖWÉFŐGÖF

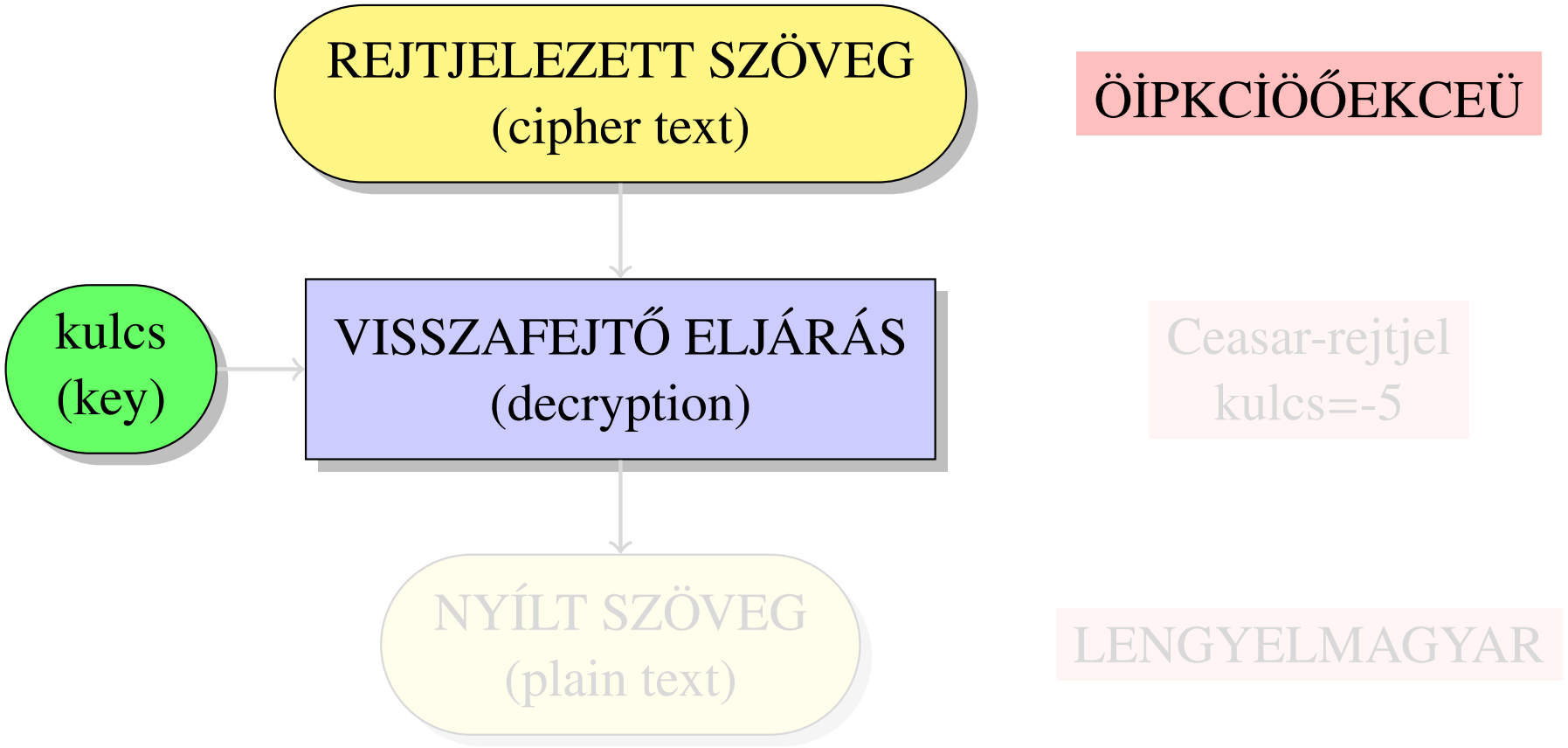
A kriptorendszer kulcsterének fogalma

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

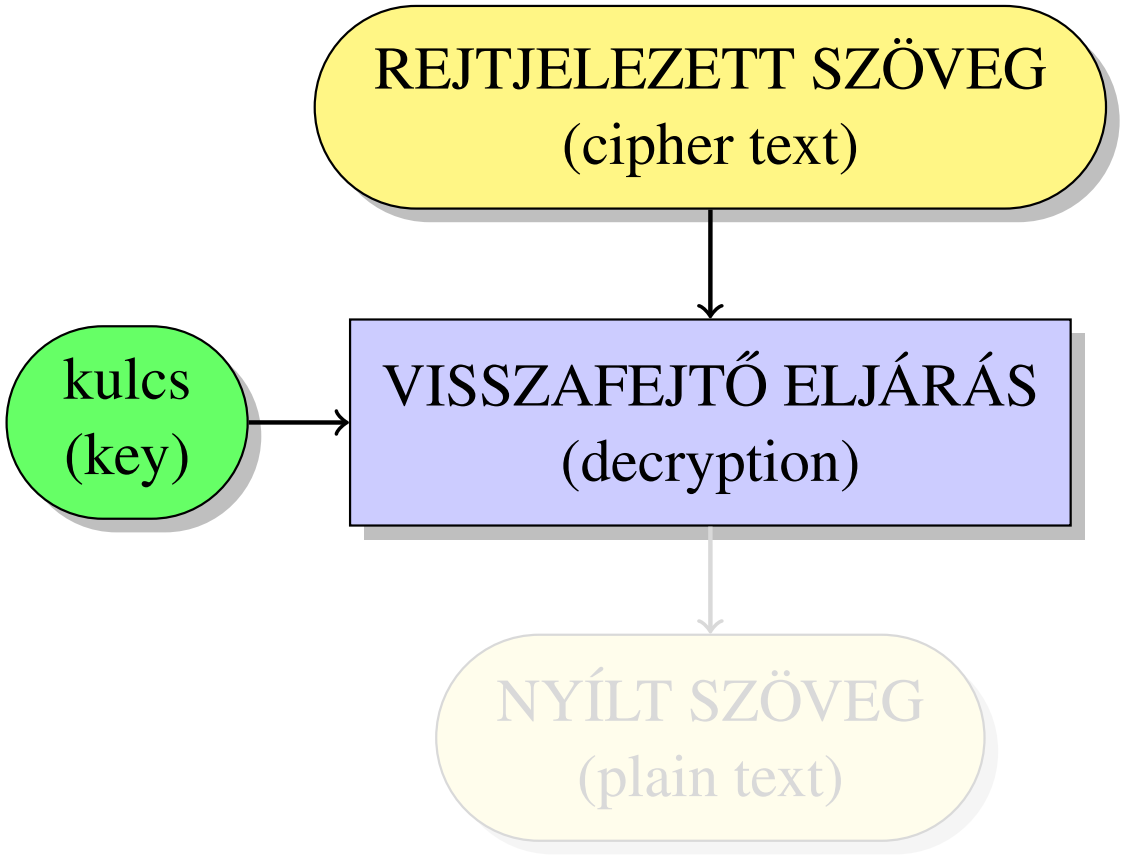
A kriptorendszer alapfogalmai: Visszafejtés



A kriptorendszer alapfogalmai: Visszafejtés



A kriptorendszer alapfogalmai: Visszafejtés

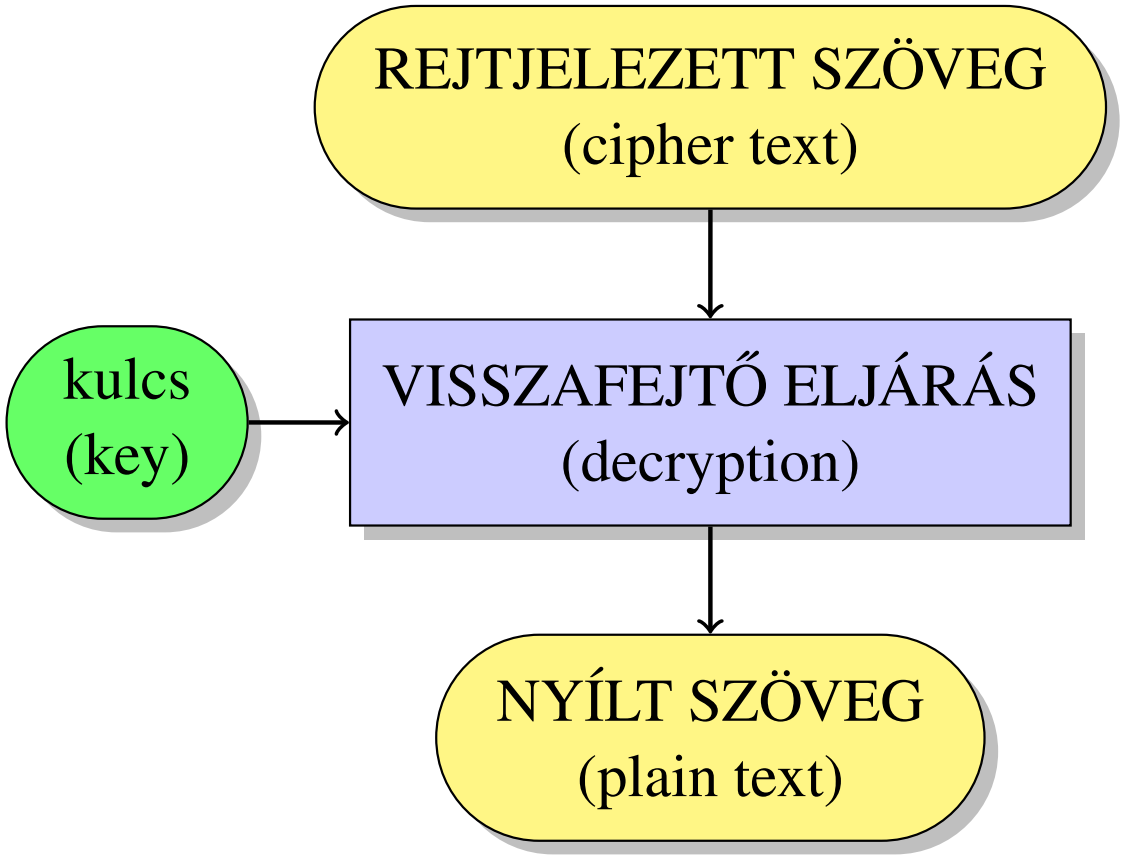


ÖİPKCİÖŐEKCEÜ

Ceasar-rejtjel
kulcs=-5

LENGYELMAGYAR

A kriptorendszer alapfogalmai: Visszafejtés



ÖİPKCİÖŐEKCEÜ

Ceasar-rejtjel
kulcs=-5

LENGYELMAGYAR

A Ceasar-féle titkosírás rendszer

- Tegyük fel, hogy a 35 betűs magyar ábécét használjuk.
- Kulcsként válasszunk egy számot 1 és 34 között.
- Ebben a példában legyen a kulcs a 7-es.
- A nyílt szöveg minden betűjét helyettesítsük azzal a betűvel, ami az ábécében 7-el utána van: A $\mapsto$ F, Á $\mapsto$ G, stb.

1	2	3	4	5	6	7	8	9	10	$\cdots$	33	34	35
A	Á	B	C	D	E	É	F	G	H	$\cdots$	X	Y	Z
F	G	H	I	Í	J	K	L	M	N	$\cdots$	D	E	É

Sebezhetőségek

- A kulcstér csak 34 elemű.
- Ha ismerjük egyetlen betű megfejtését, akkor ismerjük a kulcsot.

A Ceasar-féle titkosírás rendszer

- Tegyük fel, hogy a 35 betűs magyar ábécét használjuk.
- Kulcsként válasszunk egy számot 1 és 34 között.
- Ebben a példában legyen a kulcs a 7-es.
- A nyílt szöveg minden betűjét helyettesítsük azzal a betűvel, ami az ábécében 7-el utána van: $A \mapsto F$, $Á \mapsto G$, stb.

1	2	3	4	5	6	7	8	9	10	$\cdots$	33	34	35
A	Á	B	C	D	E	É	F	G	H	$\cdots$	X	Y	Z
F	G	H	I	Í	J	K	L	M	N	$\cdots$	D	E	É

Sebezhetőségek

- A kulcstér csak 34 elemű.
- Ha ismerjük egyetlen betű megfejtését, akkor ismerjük a kulcsot.

A Ceasar-rendszer „javításai”

A klasszikus monoalfabetikus rendszer

- Az ábécé ciklikus eltolásai helyett a betűk tetszőleges összecserélése.
- A kapott kulcstér mérete angol ábécé esetén

$$26! = 403\,291\,461\,126\,605\,635\,584\,000\,000 \approx 4 \cdot 10^{26}$$

- A ma legjobb szuperszámítógép kb. 370 év alatt végez ennyi műveletet.
- **Sebezhetőség:** A természetes nyelvekben a betűk a gyakoriságuk alapján beazonosíthatók.

Vigenère-rejtjel: A klasszikus polialfabetikus rendszer

- A Ceasar-kulcs értéke függ a betű helyétől.
- **Sebezhetőség:** Fejlett *statisztikai módszerek*, illetve *ismert szövegrészek*.

Ajánlott irodalom

- Edgar Allan Poe: Az aranybogár (1843)
- Verne Gyula: Nyolcszáz mérföld az Amazonason (1881)

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 típusok

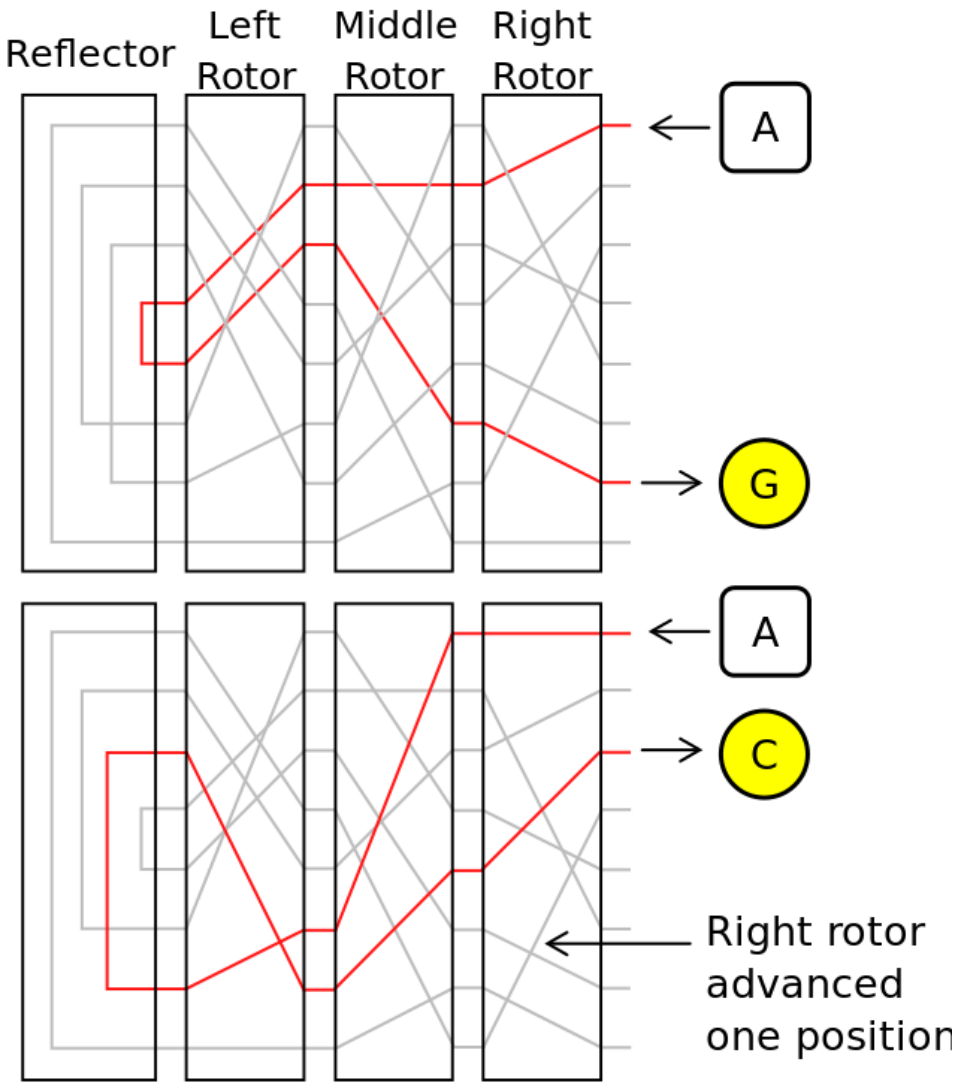
- A német hadsereg 1930-tól használt Enigma típusú gépeket rejtjelezésre.
- A hadsereg különböző része (szárazföldi erők, haditengerészet, légierő, titkosszolgálatok) különböző típusokat használtak.
- Az évek során a típusokat fejlesztették is, igyekeztek növelni a titkosítás erősségét.
- Ezen a képen GUDERIAN páncélos tábornok látható 1940-ben az Enigma használata közben.

Az Enigma típusok közös működési alapelvei

- Polialfabetikus rendszer 26 ékezet nélküli latin betűs ábécével.
- Elektromos működés egy billentyűzet és egy lámpamező segítségével.
- A **kulcs** két részből tevődik össze

(1) 3-4 cserélhető forgótárcsa és egy visszafordító tárcsa *(Walzen)*

(2) Kapocstábla 10 pár csatlakozó dugóval *(Steckerbrett)*



Enigma demó programok

- Böngészőben futó Adobe Flash program, beállításokkal, működési elvet is bemutatja:

  `http://enigmaco.de/enigma/enigma.html`

- Windows program, grafikus demó beállításokkal:

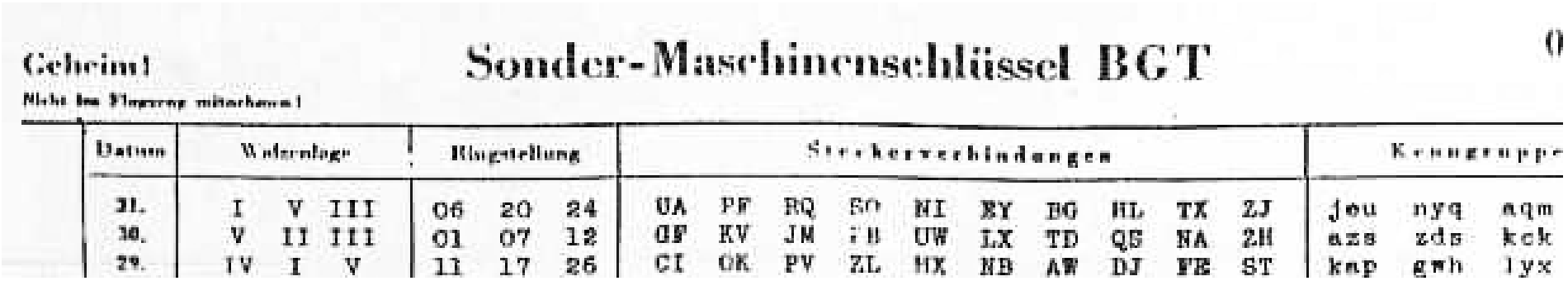
  `http://pc1cipher.pagesperso-orange.fr/enigma-en/`

- Android program tabletre és okostelefonra, grafikus demó beállításokkal:

  `Enigma Simulator Franklin Heath Ltd`

Az Enigma használata

- Minden napra volt egy előre meghatározott napi kulcs, ami tartalmazta a tárcsák és a kapocstábla kezdeti beállításait.
- A napi kulcsokat havonta előre kiadták egy szigorúan titkos kiadványban. (A tengeralattjárókon *vízben oldható* papírral-tintával.)

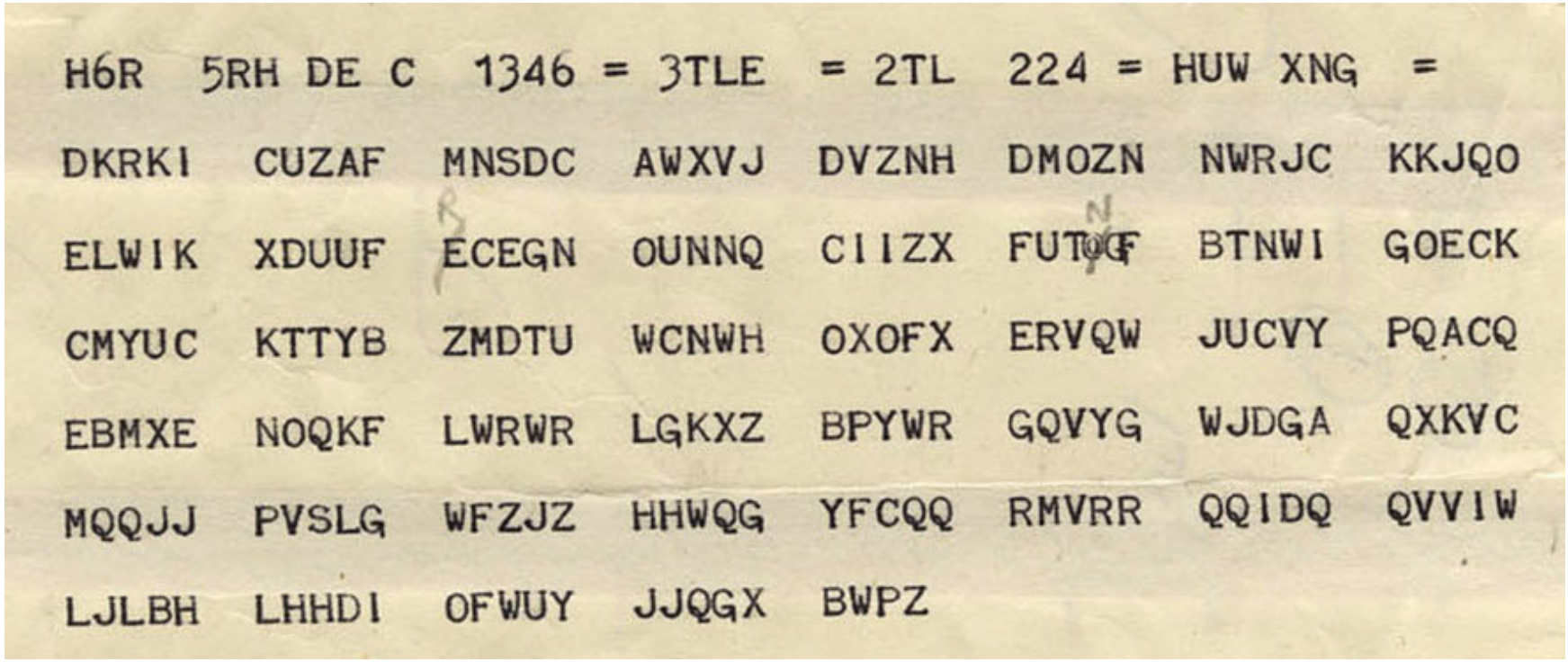


Geheim! Sonder-Maschinenschlüssel BGT

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppe
31.	I V III	06 20 24	UA PF RQ SO NI EY BG HL TX ZJ	jeu nyq aqm
30.	V II III	01 07 12	GF KV JM IB UW LX TD QS NA ZH	azs zds kck
29.	IV I V	11 17 26	CI OK PV ZL HX NB AW DJ FE ST	kap gwh lyx

- Egy üzenet maximum 250 karakterből állhatott.
- **Minden üzenetnek külön kulcsa** volt, egyéni tárcsabeállítással; a napi kapocstábla beállítást nem változtatták.
- Az üzenet fejlécében közölték az egyéni tárcsabeállítást.
- Az üzenteket Morse-jelekkel rádión továbbították.

Példa: Egy eredeti rejtjelezett Enigma-üzenet



H6R 5RH DE C 1346 = 3TLE = 2TL 224 = HUW XNG =

DKRKI CUZAF MNSDC AWXVJ DVZNH DMOZN NWRJC KKJQO

ELWIK XDUUF ECEGN OUNNQ CIIZX FUTQF BTNWI GOECK

CMYUC KTTYB ZMDTU WCNWH OXOFX ERVQW JUCVY PQACQ

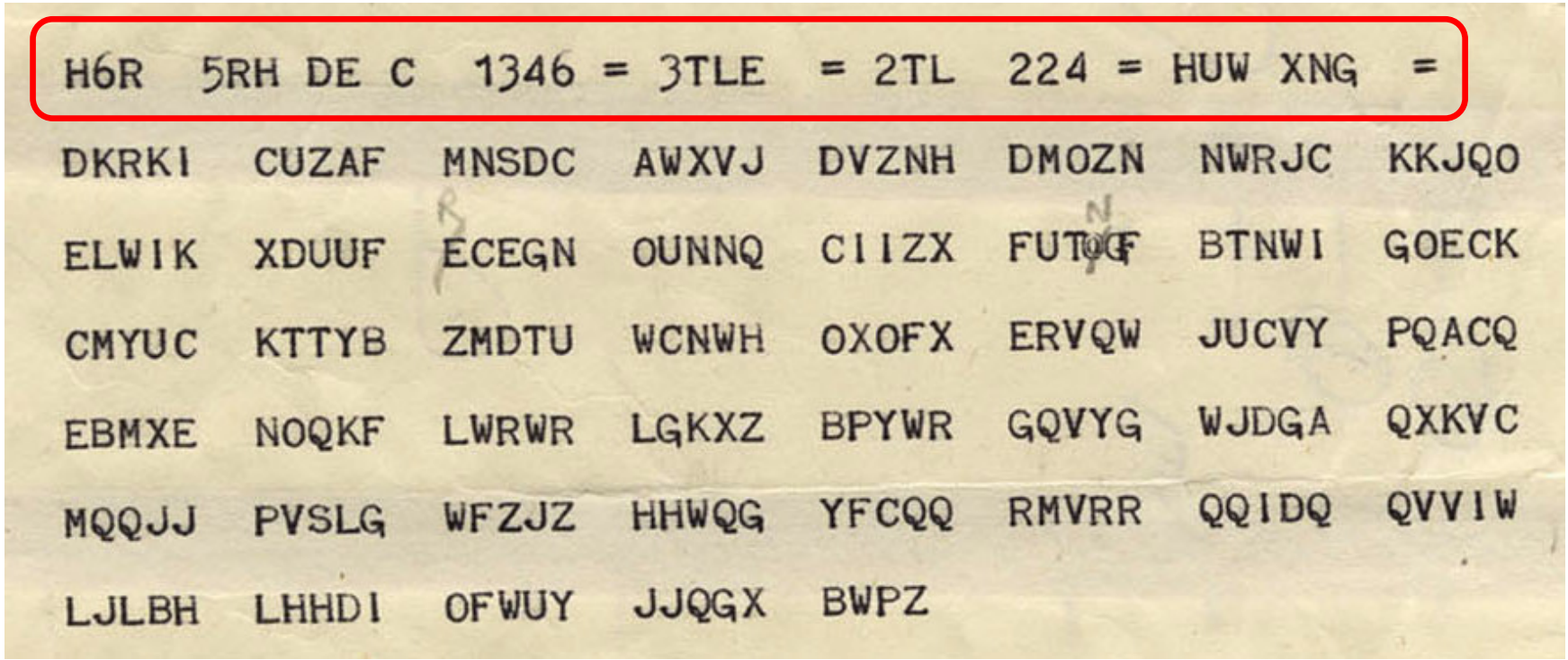
EBMXE NOQKF LWRWR LGKXZ BPYWR GQVYG WJDGA QXKVC

MQQJJ PVSLG WFZJZ HHWQG YFCQQ RMVRR QQIDQ QVVIW

LJLBH LHHDI OFWUY JJQGX BWPZ

Példa: Egy eredeti rejtjelezett Enigma-üzenet

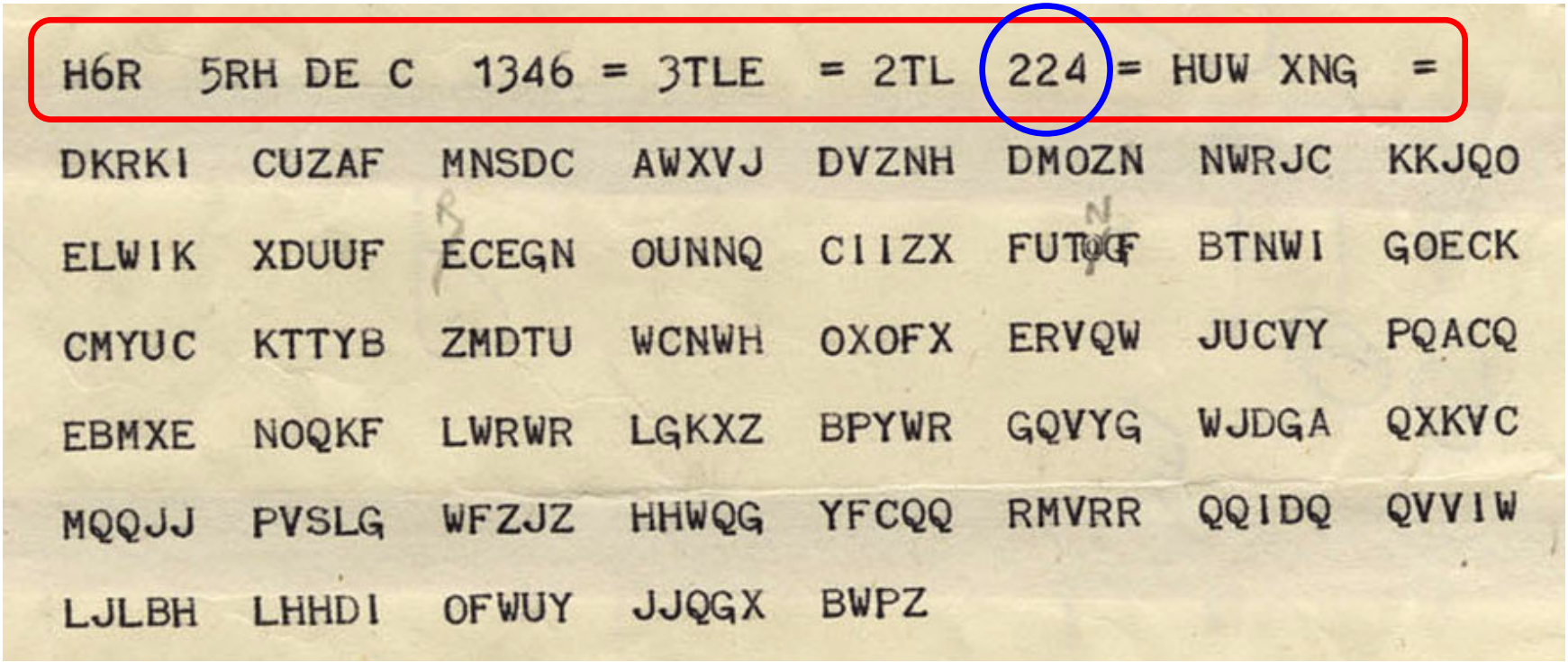
fejléc



Példa: Egy eredeti rejtjelezett Enigma-üzenet

fejléc

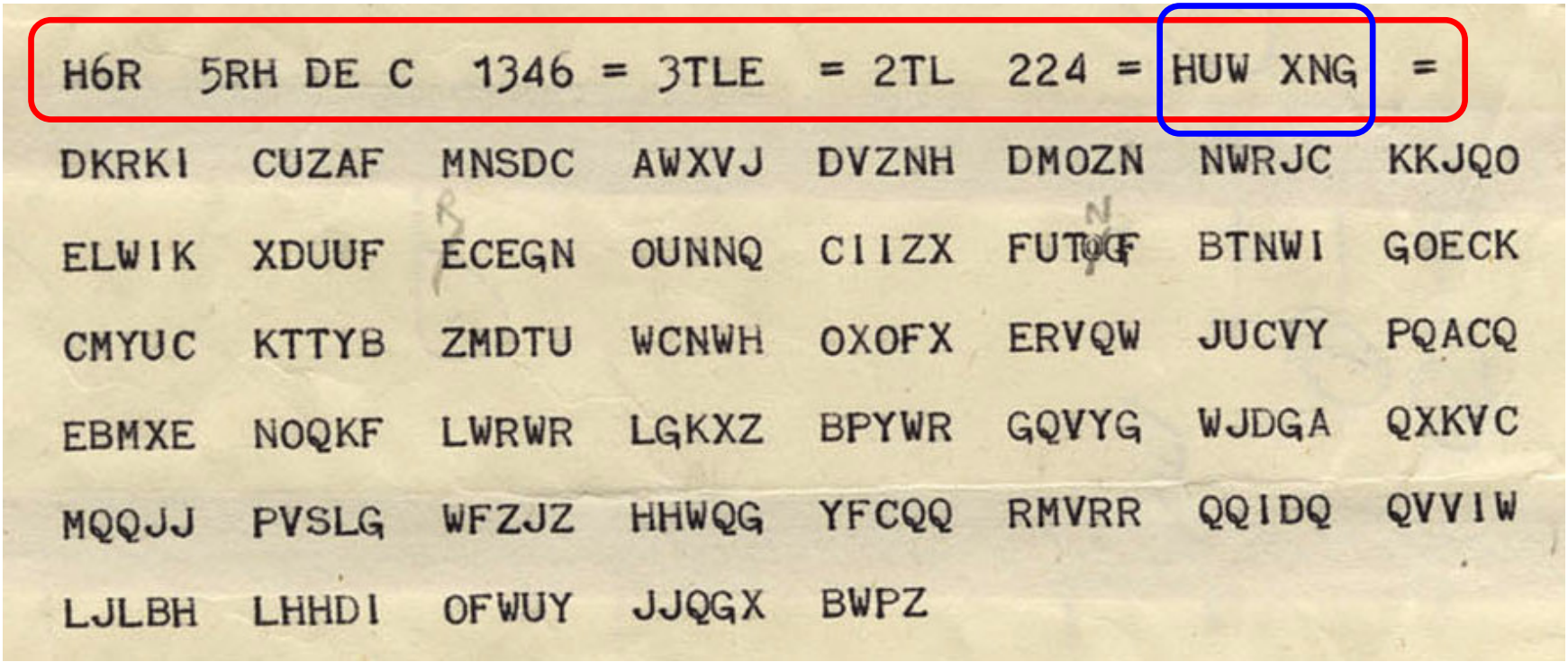
karakterszám



Példa: Egy eredeti rejtjelezett Enigma-üzenet

fejléc

egyedi tárcsa állás



Az Enigma I kulcstere

- A rendelkezésre álló 5 tárcsából 3-at kell a megfelelő helyre beilleszteni: $5 \cdot 4 \cdot 3 = 60$ lehetőség.
- A három tárcsának $26^3 = 17\,576$ állása van.
- A 26 betűből 10 párat összeállítani a kapocstáblán

$$\frac{26!}{2^{10} \cdot 10! \cdot 6!} = 150\,738\,274\,937\,250$$

féleképen lehet.

- Ez összesen

$$158\,962\,555\,217\,826\,360\,000 \approx 1,59 \cdot 10^{20} \approx 2^{67}.$$

- Ez a Kódjátszma c. filmben elhangzó „150 millió millió millió”.
- A kulcstér mérete miatt az Enigmát a szakemberek egybehangzóan **feltörhetetlennek tartották.**

Az Enigma sebezhetőségei

- Titokban akarták tartani a tárcsák drótozását.
- Végig ugyanazt a 8 tárcsát használták.
- A gép minden beállítása a 26 betű egy *fixpontmentes involutórikus permutációját* hozza létre, azaz

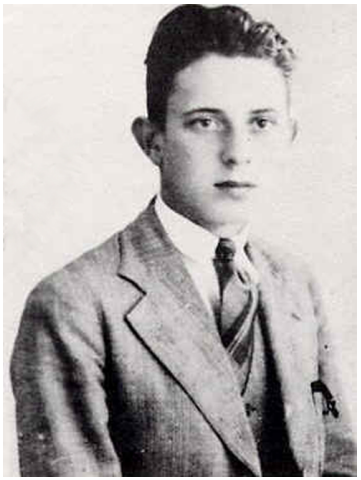
(1) ha pl. az U betű rejtjele a C, akkor a C betűé az U,

(2) és **egyetlen betű sem egyezhet meg a rejtjelével.**

- Az Enigma I változatnál az üzenet egyéni kulcsát (3 tárcsa állása, pl. GTA) duplán megismételve küldték el (pl. UZT PKL).
- Ez azt jelenti, hogy az üzenet 1. és 4., 2. és 5. valamint 3. és 6. betűje ugyanazt a betűt rejtjelezik.
- Ez nagyon durván lecsökkentette a kulcstér méretét.

Az Enigma feltörése: a lengyel matematikusok munkája

Marian Rejewski



Jerzy Różycki

Henryk Zygalski

- Brilliáns absztrakt matematikai módszerekkel, a *véges permutációcsoportok elméletét* használva megfejtették a tárcsák drótozását.
- Rájöttek, hogy amennyiben a rejtjelezett szövegben ismert szó szerepel, azt könnyen be lehet azonosítani felhasználva, hogy *egyetlen betű sem rejtjelezi saját magát.*
- Mechanikus számítógépet építettek a megmaradó (még mindig igen nagy) kulcstér szisztematikus átvizsgálására: **a BOMBA-t.**

Az Enigma feltörése: a brit Bletchley Park

- A lengyel módszereket továbbfejlesztve pár hónap alatt minden **új fejlesztésű tárcsát és kulcsközlő módszert meg tudtak fejteni.**
- Ez azt jelenti, hogy **feltörték a napi kapocstábla állást** és meg tudták határozni az egyes üzenetek egyedi kulcsát.
- Kifinomult *statisztikai és nyelvészeti módszerekkel* a jobb oldali tárcsát meg tudták határozni.
- A lengyel BOMBA-t többszörösen továbbfejlesztve elektromechanikus és programozható elektronikus számítógépeket építettek
- Turing Bomb, US Navy Bomb, Colossus, „Christofer”.
- A brit haderővel együttműködve ismert tartalmú német üzeneteket tudtak generálni.
- Ehhez például adott időpontban adott helyen bombáztak, majd várták az erről szóló rejtjeles üzenetet.

Alan Turing (1912-1954)

- Az egyik legnagyobb **20. századi matematikus zseni**
- Az 1930-as években lefektette a számítógépek elméletének matematikai alapjai *(Turing-gép)*
- A ”Turing Bomb” gép megalkotója
- Az 1950-es években mesterséges intelligencia kutatásokat végzett *(Turing-teszt)*
- Homoszexualitása miatt 1952-ben elítélte az angol bíróság

Szimmetrikus kulcsú kriptográfia

- Ugyanaz a kulcs szolgál rejtjelezésre és visszafejtésre
- Előny: Gyorsaság, kicsi memóriaigény, matematikai módszerekkel jól ellenőrizhető biztonság („keverési” tulajdonságok)
- Hátrány: A kommunikáló feleknek előre meg kell állapodni a közös titkos kulcsban (*key management*)
- 1976: **DES** (Data Encryption Standard)
- 2001: **AES** (Advanced Encryption Standard)

Nyilvános (aszimmetrikus) kulcsú kriptográfia

- Két különböző kulcsot használunk a rejtjelezésre illetve a visszafejtésre
- Az egyik kulcsból a másik kiszámítása **matematikailag bizonyítottan „nehéz”**
- A rejtjelező kulcs nyilvános, a visszafejtő kulcsot csak a címzett ismeri

(1) 1978: **RSA** (Ronald Rivest, Adi Shamir és Len Adleman)
Az RSA biztonsága azon múlik, hogy tudunk-e több száz számjegyből álló számokat prímtényezőkre bontani.

(2) 1976: **Diffie-Hellman kulcscsere**
A biztonság a *diszkrét logaritmus* nehézségére épül.

- Hibrid rendszerek